



Universidade do Minho
Instituto de Ciências Sociais

Sara Margarida da Silva Matos

"Vigiar e/ou proteger?"
Desafios da proteção de dados genéticos
no combate à criminalidade no âmbito do
sistema Prüm

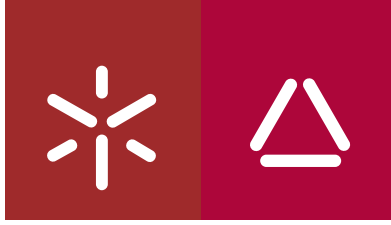
Este trabalho recebeu financiamento do Conselho Europeu de Investigação (ERC) sob o programa de pesquisa e inovação da União Europeia Horizonte 2020 (Contrato N° 648608), no âmbito do projeto «*EXCHANGE* – Geneticistas forenses e a partilha transnacional de informação genética na União Europeia: Relações entre ciência e controlo social, cidadania e democracia» liderado por de Helena Machado e sediado no Centro de Estudos de Comunicação e Sociedade da Universidade do Minho. Entre outubro de 2015 e setembro de 2017 o projeto *EXCHANGE* esteve sediado no Centro de Estudos Sociais da Universidade de Coimbra.



European
Commission

Horizon 2020
European Union funding
for Research & Innovation





Universidade do Minho
Instituto de Ciências Sociais

Sara Margarida da Silva Matos

**"Vigiar e/ou proteger?"
Desafios da proteção de dados genéticos
no combate à criminalidade no âmbito do
sistema Prüm**

Tese de Doutoramento
Ramo do Conhecimento em Sociologia

Trabalho efetuado sob a orientação da
Professora Doutora Helena Machado

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição-NãoComercial-SemDerivações

CC BY-NC-ND

<https://creativecommons.org/licenses/by-nc-nd/4.0/>

AGRADECIMENTOS

À Professora Doutora Helena Cristina Ferreira Machado, orientadora desta tese, quero agradecer a dedicação, disponibilidade e apoio ao longo da investigação. Agradeço também a oportunidade de poder integrar a sua equipa de investigação financiada pelo *European Research Council*, sediada no Centro de Estudos em Comunicação e Sociedade da Universidade do Minho.

Aos participantes desta investigação, pela disponibilidade que demonstraram durante a partilha das suas experiências. Foram fundamentais para a concretização deste estudo.

A todos os elementos que integraram a equipa do projeto Exchange, pela amizade, companheirismo e disponibilidade para me ajudarem a ultrapassar os obstáculos com os quais me deparei ao longo do meu percurso.

À Rafaela Granja e à Filipa Queirós cuja distância e trabalho nunca impediram que fôssemos um tripé de apoio para todas as ocasiões. Apoiamo-nos nos momentos menos bons e festejamos com verdadeiro orgulho as conquistas de cada uma.

À minha família e amigos por todo o apoio transmitido e pelo entusiasmo que demonstraram durante a investigação. Em particular, à Cristiana Pereira, à Diana Amorim, ao Rui Cruz e à Sara Duarte por terem aceite o desafio de lerem a tese. E à Susana Silva que, mesmo longe, sempre encontrou espaço para me presentear com o seu apoio e a sua tão particular boa disposição.

À minha mãe, cuja força e perseverança me inspiram diariamente a ser mais, a ser eu. Que me ensinou que mais importante do que avançar é sermos justos, honestos e fiéis a quem somos. E que me acompanhou em todo este percurso com a curiosidade com que sempre me brindou.

À minha tia Isabel Maria que não me viu começar esta etapa.

E à minha avó que não me viu concluí-la.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

“Vigiar e/ou proteger?” - Desafios da proteção de dados genéticos no combate à criminalidade no âmbito do sistema Prüm

RESUMO

A partilha de perfis genéticos e de dados pessoais com o objetivo de combater a criminalidade transnacional, operacionalizada através do sistema Prüm, tem gerado intenso debate em diferentes esferas da sociedade. Em particular, no que diz respeito à possibilidade de alcançar um equilíbrio entre a proteção de direitos civis e a defesa da segurança coletiva. No epicentro do debate estão desafios éticos e sociais relacionados com a proteção de dados pessoais e a privacidade dos cidadãos, num contexto histórico em que se assiste à intensificação de processos e tecnologias de vigilância a operar no âmbito das políticas da União Europeia.

Este estudo tem como objetivos gerais (1) o mapeamento do debate em torno da proteção de dados pessoais versus intensificação da vigilância e subsequente compressão dos direitos individuais no contexto da União Europeia; (2) a análise das perspetivas de profissionais que operacionalizam a partilha transnacional de perfis de DNA através do sistema de Prüm; e (3) a compreensão de posicionamentos distintos por parte de diferentes grupos profissionais da esfera da ciência genética, da ética e do sistema de justiça, no que diz respeito às suas representações sobre privacidade e proteção de dados, em dois países: Portugal e Reino Unido. Os dois países foram selecionados devido às suas diferenças quanto à inovação ao nível das tecnologias de DNA e utilização no sistema de justiça criminal; ao tipo de sistema de justiça (inquisitorial e adversarial); dimensão, antiguidade e legislação da base de dados nacional forense de perfis de DNA; e postura política quanto à implementação do sistema Prüm ao nível nacional. Para alcançar estes objetivos adotou-se uma metodologia de carácter qualitativo com recurso à análise de entrevistas semiestruturadas e, de modo complementar, à análise documental de regulação e legislação europeia no que diz respeito à proteção de dados na investigação criminal e à cooperação policial transnacional.

Os resultados mostram um consenso relativamente transversal em relação às vantagens do modelo de cooperação policial e judicial operado pelo sistema Prüm. No entanto, as representações relativas aos desafios e riscos que advêm da partilha de dados

genéticos ao nível transnacional demonstram heterogeneidade entre os entrevistados. Tal heterogeneidade evidencia-se ao nível das funções que estes profissionais desempenham na partilha de dados. Não se tratando de divisões estanques, uma parte dos profissionais entrevistados, principalmente os que trabalham em contexto laboratorial, realçam a tecnicidade e a standardização dos procedimentos de cooperação. Por conseguinte, tais narrativas revelam uma escassa reflexão sobre os desafios colocados à proteção de dados na esfera criminal. As narrativas que recaem sobre a neutralização dos desafios à proteção de dados genéticos no combate à criminalidade na Europa apresentam um elevado entusiasmo quanto à automatização e standardização de procedimentos técnicos e científicos. Por sua vez, as perspetivas que aprofundam os desafios e riscos da partilha de dados no âmbito do sistema Prüm são mais recorrentes junto de profissionais da esfera policial. Ainda que mais elaboradas, tais perspetivas incidem, na sua maioria, na reprodução dos discursos que careceram de clarificação acerca do modo como são asseguradas as leis de proteção de dados na cooperação transnacional.

Aprofundar a complexidade da partilha de dados transnacional operacionalizada pelo sistema Prüm através dos estudos de caso revela-se como fundamental para o mapeamento do papel das especificidades nacionais ao nível da sua implementação. No contexto português observa-se que o discurso político e as narrativas dos/as entrevistados/as são consonantes quanto à representação do sistema Prüm como ferramenta tecnocientífica fundamental à cooperação transnacional. Em relação ao contexto britânico, o posicionamento político em relação ao sistema Prüm foi fortemente condicionado pela primazia do interesse nacional. No entanto, a análise das narrativas dos/das entrevistados/as torna visível um discurso que se foca numa análise de custo-benefício para o país com a adesão ao sistema Prüm. As perspetivas veiculadas pela maioria dos/as participantes realçam a importância de um projeto europeu de combate à criminalidade organizada e ao terrorismo. Deste modo, tendo como objeto de estudo o sistema Prüm, esta tese apresenta um contributo original para a exploração das complexidades e das tensões presentes na implementação de sistemas de controlo e gestão da criminalidade na União Europeia.

Palavras-Chave: Dados genéticos; desafios éticos e sociais; proteção de dados; vigilância

**“To surveil and/or to protect?” - Challenges for the protection of genetic data in
the fight against crime within the Prüm system**

ABSTRACT

The transnational automated exchange of genetic profiles and personal data for fighting crime, operationalized through the Prüm system, has generated intense debate in different spheres of society. In particular, regarding the possibility of achieving a balance between the protection of civil rights and the defence of collective security. At the epicentre of the debate are ethical and social challenges related to the protection of personal data and the privacy of citizens, in a historical context marked by the intensification of surveillance processes and technologies operating within the European Union.

This study aims (1) to map the debate around the protection of personal data versus surveillance versus the intensification of surveillance and subsequent compression of individual rights in the context of the European Union; (2) to analyse the perspectives of the professionals operating the transnational exchange of DNA profiles through the Prüm system; and (3) to comprehend the distinct social positions held by different professional groups in the field of genetic science, ethics and the justice system with regard to their representations of privacy and data protection in two countries: Portugal and the United Kingdom. The two countries were selected considering their differences regarding the innovation in terms of DNA technologies and use in the criminal justice system; the type of justice system (inquisitorial and adversarial); size, age and legislation of the national forensic DNA database; and political posture regarding the implementation of the Prüm system at the national level. To achieve these goals, a qualitative methodology was adopted, using semi-structured interviews and, in a complementary way, documentary analysis of European regulation and legislation with regard to data protection in criminal investigations and transnational police cooperation.

The results show relatively transversal consensus regarding the benefits of the police and judicial cooperation model operated by the Prüm system. However, the representations about the challenges and risks that arise from the transnational exchange of DNA profiles demonstrate heterogeneity among respondents. Such heterogeneity is evident in the roles that these professionals have in data exchange. Not being tight divisions, a part of the

interviewed professionals, mainly those who work in a laboratory context, emphasize the technicality and standardization of the cooperation procedures. Consequently, these narratives reveal scarce reflection on the challenges posed to data protection in the criminal sphere. The narratives focused on the neutralization of the challenges of the protection of genetic data in the fight against crime in Europe show significant enthusiasm regarding the automatization and standardization of technical and scientific procedures. The perspectives that deepen the challenges and risks of data exchange within the scope of the Prüm system are more recurrent with police professionals. Although more elaborated, such perspectives focus on the reproduction of discourses that lack clarification about how the data protection laws in transnational cooperation are ensured.

Deepening the complexity of transnational data exchange made operational by the Prüm system through case studies is fundamental to mapping the role of national specificities in terms of implementation. In the Portuguese context, the political discourse and the narratives of the interviewees were consonants regarding the representation of the Prüm system as a fundamental techno-scientific tool for transnational cooperation. Concerning the British context, the political position regarding Prüm system was strongly conditioned by the primacy of national interest. However, the analysis of the interviewees' narratives makes visible a discourse that focuses on a cost-benefit analysis for the country about the adherence to the Prüm system. The perspectives conveyed by the majority of the participants highlight the importance of a European project to combat organized crime and terrorism. Thus, having the Prüm system as its object of study, this thesis presents an original contribution to the exploration of the complexities and tensions present in the implementation of crime control and management systems in the European Union.

Keywords: Data protection; ethical and social challenges; genetic data; surveillance

Índice

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS	ii
AGRADECIMENTOS	iii
DECLARAÇÃO DE INTEGRIDADE.....	iv
RESUMO	v
ABSTRACT	vii
INTRODUÇÃO.....	12
CAPÍTULO 1. ENQUADRAMENTO TEÓRICO	22
1.1. Sistema Prüm	22
1.2. Proteção de dados pessoais na União Europeia	25
Regulação e supervisão na proteção de dados	29
1.3. Cooperação transfronteiriça policial e judiciária	31
1.4. Privacidade – conceito social?	32
Espaço público vs espaço privado	40
1.5. Vigilância <i>hard</i> e vigilância <i>soft</i>	44
Sofisticação da vigilância tecnológica - tecnologias biométricas de vigilância.....	49
1.6. Bases de dados forenses de perfis de DNA	54
1.7. Estandarização, proteção de dados e privacidade.....	59
(D)estandardização dos standards	60
(D)estandardização do perfil forense de DNA.....	81
1.8. Imaginários Sociotécnicos	87
CAPÍTULO 2. METODOLOGIA.....	93
2.1. Enquadramento do projeto Exchange	93
2.1.2 Contributos específicos da tese.....	94
2.2. Entrevistas semiestruturadas - Métodos de amostragem	95
Pontos de Contacto Nacionais (NCPs) do sistema Prüm	98
Geneticistas forenses	100
Stakeholders dos estudos de caso.....	101
2.3. Procedimentos éticos.....	103
2.4. Análise das entrevistas.....	105
CAPÍTULO 3. ANÁLISE EMPÍRICA	106
3.1. Perspetivas de Pontos de Contacto Nacionais do sistema Prüm	106
3.2. Representações dos Pontos de Contacto Nacionais do passo 1 (NCP1)	107
Benefícios e utilidade do sistema Prüm	107
Passo 1 do sistema Prüm.....	110
Desafios e riscos do sistema Prüm	112
Eficácia e futuro do sistema Prüm.....	120

Privacidade e proteção de dados no sistema Prüm	123
Interoperabilidade entre bases de dados com diferentes finalidades.....	126
3.3. Representações dos Pontos de Contacto Nacionais do passo 2 (NCP2)	134
Benefícios e utilidade do sistema Prüm	134
Desafios e riscos do sistema Prüm	136
Eficácia e futuro do sistema Prüm.....	141
Estrutura de dois passos no sistema Prüm.....	144
Privacidade e proteção de dados no sistema Prüm	152
Interoperabilidade entre bases de dados com diferentes finalidades.....	159
CAPÍTULO 4. Análise empírica de dois estudos de caso: Portugal e Reino Unido	162
4.1. Enquadramento sócio-histórico.....	163
4.1.1 Portugal	163
Contexto legal e regulatório – Lei n.º 90/2017.....	167
Lacunas e incertezas sobre a Lei n.º 5/2008 – Lei n.º 90/2017	171
Cooperação internacional e Portugal	174
4.1.2 Reino Unido	175
Base de dados forense nacional – Contextualização da criação e do panorama político	176
Base de dados forense nacional – Funcionamento, supervisão e estatísticas	179
Caso de S. e Marper versus Reino Unido e ‘Protection of Freedoms Act 2012’	181
Cooperação transnacional – Decisões Prüm	185
4.2. Perspetivas de geneticistas forenses e <i>stakeholders</i>	190
4.2.1 Portugal	190
Contexto legal da base de dados forense de perfis DNA	190
Critério de inserção do perfil de DNA na base de dados forense.....	200
Vantagens e desafios do sistema Prüm	205
Privacidade e proteção de dados na base de dados forense	220
Interoperabilidade entre bases de dados forenses e biobancos.....	226
Direito ao apagamento dos dados - Artigo 17.º do Regulamento (EU) 2016/679	233
4.2.2. Reino Unido	239
Desafios éticos da utilização das bases de dados de perfis de DNA para fins forenses	240
Regime de retenção ‘Protection of Freedoms Act 2012’ na base de dados forense nacional	245
Vantagens e desafios do sistema Prüm	251
Envolvimento das entidades de supervisão no sistema Prüm	270
Implicações do contexto político do Brexit no sistema Prüm	271
Interoperabilidade entre bases de dados forenses e biobancos.....	275
4.3. Perspetiva comparativa entre Portugal e o Reino Unido: o papel dos imaginários sociotécnicos	281
4.3.1 Imaginários sociotécnicos dos geneticistas forenses e stakeholders no contexto português	284
4.3.2 Imaginários sociotécnicos dos geneticistas forenses e stakeholders no contexto britânico	287

4.3.3 Comparação ao nível nacional: Portugal e Reino Unido	290
CONCLUSÕES	296
REFERÊNCIAS BIBLIOGRÁFICAS	305
ANEXOS	329
Anexo 1 – Guião de entrevista - Pontos de Contacto Nacionais (NCP)	330
Anexo 2 – Guião de entrevista – Geneticistas forenses	333
Anexo 3 – Guião de entrevista – <i>Stakeholders</i>	335
Anexo 4 – Consentimento informado	338
Anexo 5 – Folheto informativo	339
Anexo 6 - Acordo de confidencialidade para profissionais contratados para a realização das transcrições	341

Índice de Tabelas

Tabela 1-Distribuição dos/as entrevistados/as por país – projeto Exchange	98
Tabela 2-Characterização dos NCPs entrevistados em países operacionais	100
Tabela 3-Characterização dos geneticistas forenses em Portugal e no Reino Unido e organização onde desempenham funções	101
Tabela 4-Número de stakeholders em Portugal e no Reino Unido	103
Tabela 5-Categoria profissional dos stakeholders	103
Tabela 6-Formação educacional dos stakeholders	103
Tabela 7-Comparação entre geneticistas forenses e stakeholders de Portugal e do Reino Unido em relação às bases de dados forenses de DNA, à cooperação transnacional e à interoperabilidade entre bases de dados forenses e biobancos	283
Tabela 8-Comparação entre Portugal e o Reino Unido em relação às bases de dados forenses de DNA e à cooperação transnacional	290

Lista de siglas

CNPD – Comissão Nacional de Proteção de Dados
 EUA – Estados Unidos da América
 INMLCF – Instituto Nacional de Medicina Legal e Ciências Forenses
 ISFG – International Society for Forensic Genetics
 NCP – Ponto de Contacto Nacional
 NGS – *Next Generation Sequencing*
 NSA – *US National Security Agency*
 ONG – Organização Não Governamental
 PoFA – *Protection of Freedoms Act 2012*
 TWGDAM - *Technical Working Group on DNA Methods*
 UE – União Europeia

INTRODUÇÃO

Em junho do ano de 2013 vários órgãos de comunicação social, como o *The Guardian*^{1,2} e o *The New York Times*³, revelaram, sem precedentes, detalhes pormenorizados de atividades de vigilância operadas pela *US National Security Agency* e outros serviços de inteligência dos Estados Unidos da América. Os documentos que serviram de base para as várias notícias e onde constavam todas as informações divulgadas foram cedidos por Edward Snowden, contratado pelo Governo, para trabalhar nos serviços de inteligência do país, um nome até então desconhecido por todos (Dijck, 2014; Lyon, 2015; Wright & Kreissl, 2015). A divulgação destas informações confidenciais colocou sob enorme tensão as relações diplomáticas que os EUA tinham vindo a desenvolver com vários países aliados, a título de exemplo, a Alemanha, o Brasil, o México. A deterioração do diálogo entre os países aliados e os EUA deveu-se às informações contidas nos documentos que originaram a fuga de informação sobre as ações de vigilância massiva levada a cabo durante vários anos. Os documentos revelaram as extensas e intensas atividades de vigilância que incidiram em populações (nos EUA e na UE), bem como em líderes políticos, oficiais das Nações Unidas e empresas como a Google, a Petrobras, entre outras (Wright & Kreissl, 2015).

Em paralelo com as tensões geradas entre os países envolvidos nesta teia de vigilância, também a confiança pública, tanto no Estado como em várias empresas – Verizon, AT&T, Google, Facebook, Apple, YouTube, Skype, Microsoft, PalTalk, entre outras – foi-se deteriorando à medida que se divulgavam os documentos de Snowden, principalmente, devido à falta de segurança e proteção dos dados dos seus utilizadores (Dijck, 2014). O *The Washington Post* revelou ainda que a NSA tinha na sua posse um programa secreto, PRISM, que visava precisamente a recolha de e-mails, chamadas telefónicas (realizadas na Internet), fotos, vídeos, ficheiros transferidos e dados oriundos de redes sociais acedidos através das empresas supramencionadas (Wright & Kreissl, 2015, pp. 6-7). Perante esta situação sem precedentes, é necessário sistematizar os 3 pontos que permitiram esta vigilância massiva no tempo e no espaço operada pelo EUA (Lyon, 2015).

¹ Notícia divulgada no *The Guardian* no seguinte link: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso a 28 de maio de 2017.

² Para uma análise sobre as consequências das divulgações de Edward Snowden na perspetiva do *The guardian* consultar o seguinte link: <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>. Acesso a 28 de maio de 2017.

³ Notícia divulgada no *The New York Times* no seguinte link: <http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html>. Acesso a 12 de maio de 2020.

Primeiro, a NSA contou com o trabalho conjunto dos serviços de inteligência de outros países. Ou seja, houve um contributo ativo dos Governos neste modo de vigilância massiva dos seus cidadãos. Segundo, as empresas, principalmente as ligadas aos serviços de internet, partilharam os dados dos seus utilizadores com os Governos de modo a usufruírem mutuamente dos mesmos. Terceiro, através da pegada digital que o uso das redes sociais e do telemóvel deixam no meio virtual, também os cidadãos contribuíram, ainda que irrefletidamente para este modelo de vigilância. Citando Lyon (2015) a respeito do contributo da população em geral, “without necessarily being aware of it, we all feed data to the NSA and its cognate agencies, just by contacting others electronically” (p. 141).

As revelações de Edward Snowden deixaram todos os lesados e os responsáveis pela vigilância em massa surpreendidos. No entanto, o ponto chave a reter prende-se pela escala megalómana da vigilância e as suas implicações para a privacidade e proteção de dados dos cidadãos. Neste sentido, a vigilância *online* veio mudar o enquadramento da noção de privacidade enquanto conceito restrito aos direitos de um indivíduo identificável (Lyon, 2015). Este grau de acesso a informações pessoais permite a construção de perfis por antecipação onde um cidadão pode ser considerado suspeito, por exemplo, de manter ligações com redes terroristas, sem que tenha ocorrido de facto esta ligação (*idem*). Por este motivo, Snowden é encarado por muitos como um herói que se sacrificou em nome da Humanidade, demonstrando que o seu país não estava a respeitar os restantes parceiros, nem os seus próprios cidadãos. Realce-se que em momento algum foram reveladas informações pessoais que pudessem colocar em perigo os agentes operacionais que estavam responsáveis pela vigilância (Wright & Kreissl, 2015).

Este acontecimento gerou várias respostas institucionais por parte dos países europeus que se viram alvo da vigilância em massa. A União Europeia começou por repensar os acordos realizados com os EUA para a partilha de dados financeiros e de tráfego *online*, bem como redigiu acordos mais restritos em relação à proteção de dados como forma de repúdio pelo comportamento abusivo demonstrado (*idem*). Portanto, as revelações de Edward Snowden foram uma das plataformas que permitiram a reflexão sobre as questões de privacidade, direitos humanos, liberdades civis, liberdade e justiça (Dijck, 2014; Lyon, 2015) num contexto crescente de utilização de tecnologias de informação. Ainda a este respeito, é necessário que se distinga a vigilância massiva da vigilância por *target* e o modo como estas se complementam no aparelho securitário. A

vigilância massiva caracteriza-se pela monitorização e recolha indiscriminada de dados da população em geral, sendo que quanto maior for a infraestrutura em que opera, maior é a possibilidade de ocorrerem falsos positivos quanto aos perfis das pessoas de interesse (Lyon, 2015). Por sua vez, a criação destes perfis pode conduzir à vigilância por *target*, isto é, um indivíduo identificável. O presente estudo foca-se numa infraestrutura transnacional que opera com base na vigilância por *target*, o sistema Prüm (O'Neill & Loftus, 2013). Este é um sistema tecnológico da União Europeia que funciona em rede e permite o acesso mútuo às bases de dados forenses nacionais de perfis genéticos, de impressões digitais e de registos de veículos através dos indicadores de *hit/no hit*. Uma das suas características distintivas em termos de cooperação policial e judicial é o facto de existirem dois passos no processo de partilha de dados pessoais dos cidadãos. Em traços latos, o primeiro passo, automatizado, confirma a correspondência entre um perfil de DNA de uma base de dados forense com a de outros países. O segundo passo ocorre quando é solicitada informação sociodemográfica a respeito do perfil de DNA que gerou a correspondência. Esta fase do processo não é automática e está dependente da lei de Proteção de Dados dos países envolvidos na troca de informações, bem como dos critérios mínimos estabelecidos pela Comissão Europeia para a proteção de dados (Machado & Silva, 2010; Prainsack, 2010).

Ao nível sociológico, entende-se que esta revelação sem precedentes veio contribuir de certo modo para a (re)construção e manutenção de fronteiras entre grupos sociais, como também entre sociedades com valores culturais diferentes. No entanto, esta distinção entre o “nós” e os “outros” é difícil de gerir, pois, encontramos-nos numa era fortemente moldada pela globalização, pelo multiculturalismo e pela cooperação transnacional (Wright & Kreissl, 2015, p. 36). Deste modo, é necessário o questionamento acerca das noções de privacidade e proteção de dados em sistemas de vigilância que operam não só ao nível nacional, mas também numa dimensão transnacional que engloba a partilha de dados pessoais de cidadãos entre diferentes países. Esta discussão deve ser realizada à luz de uma estratégia que envolva a sociedade em geral, de modo a tornar este processo mais transparente, como também de assegurar que a vigilância operada pelo Estado e pelos órgãos institucionais seja equitativa e proporcional (Craig & Búrca, 2008). Com particular ênfase no debate sobre o equilíbrio entre o bem coletivo de segurança e os direitos individuais, como a proteção de dados, privacidade, presunção de inocência, liberdade, entre outros.

O debate em torno da temática da vigilância indiscriminada dos cidadãos demonstra que as novas configurações da vigilância moderna podem apresentar-se como desafios à “privacy, autonomy, dignity, freedom of speech, freedom of association, freedom of movement, non-discrimination, social integration, due process and the presumption of innocence” (Raab, 2015, p. 259). Como resultado, Raab (2015) enuncia três preocupações que advêm dos impactos da vigilância, automatizada, direcionada e voluntária, nas várias esferas da sociedade (p. 261). A primeira remete para a visibilidade, pois a vigilância pode ser visível ou invisível, dado que, muitas vezes, os cidadãos não sabem que estão a ser vigiados. A segunda tem que ver com a legalidade destas atividades. Na medida em que, nem sempre é claro que determinada prática seja legal, a sua legitimidade varia consoante a jurisdição em que ocorre. Acrescente-se que a proporcionalidade de um sistema de vigilância pode ser questionada de acordo com a expectativa razoável de privacidade dos vigiados. A terceira diz respeito às relações de poder presentes na vigilância, pois as relações entre vigiados e vigilantes são bastantes complexas e colocam os primeiros em desvantagem perante os segundos, consequência dos dados previamente recolhidos através do aparato tecnológico, característico das novas configurações de vigilância.

Acrescente-se que, nas últimas décadas, com o desenvolvimento de sistemas tecnológicos que permitem a circulação e partilha de informação em grande escala, tem-se ampliado o debate em torno das implicações sociais, económicas, políticas e éticas decorrentes da recolha massiva, utilização, análise e partilha de dados pessoais. Este debate tem sido balizado, principalmente, em torno da circulação de dados com intuítos comerciais e de âmbito médico (Human Genetics Commission, 2001; Lyon, 2001). No entanto, é necessário aprofundar e sistematizar a discussão no que concerne à privacidade e proteção de dados pessoais em contexto de investigação criminal transnacional (Cabezudo, 2013; Costa & Nunes, 2001; Gonçalves & Jesus, 2013, p. 255; Kierkegaard, 2008; Machado & Prainsack, 2012; McCartney, Williams, & Wilson, 2010).

O presente estudo, de carácter qualitativo, visa compreender quais os desafios da proteção de dados genéticos (DNA⁴) no combate à criminalidade na União Europeia. Configurando-se uma contribuição original para a discussão em torno da proteção de dados pessoais no contexto de partilha transnacional de dados para fins de investigação criminal,

⁴ Apesar da tradução da sigla DNA, correspondente a ácido desoxirribonucleico, para a língua portuguesa ser ADN, no contexto desta tese utilizou-se a formulação em inglês por ser a designação aprovada pela Sociedade Internacional de Bioquímica. Nos excertos empíricos selecionados manteve-se a designação utilizada pelos/as entrevistados/as.

esta tese tem como objetivos: (1) mapear o debate em torno da proteção de dados pessoais *versus* vigilância e compressão dos direitos individuais no contexto da União Europeia; (2) analisar especificamente a partilha transnacional de perfis de DNA, concretamente, o sistema de Prüm, a partir das perspetivas de profissionais que o operacionalizam; e (3) compreender os posicionamentos sociais distintos por parte de diferentes grupos profissionais da esfera da ciência genética, da ética e do sistema de justiça, no que diz respeito às suas conceções sobre privacidade e proteção de dados, em dois países: Portugal e Reino Unido. Deste modo, pretende-se colmatar a escassez de estudos empíricos sobre as consequências da partilha transnacional de informação genética para a privacidade dos indivíduos que constam nestas bases de dados forenses, bem como compreender os imaginários que permeiam a implementação do sistema Prüm. A análise sociológica das dimensões em estudo usufrui dos contributos dos estudos da ciência e da tecnologia, dos estudos da vigilância e dos estudos sociais da genética forense permitindo alcançar a panóplia de desafios que são elencados na reflexão acerca das implicações da partilha transnacional de dados pessoais para a proteção da privacidade dos indivíduos. Para investigar o fenómeno em estudo – o sistema Prüm – é necessário equacionar a sua dimensão tecnológica, pois a partilha é realizada através de sistemas interoperáveis e ligados em rede, onde a standardização e o avanço tecnológico são essenciais; a sua dimensão biométrica/genética, pois sem os desenvolvimentos operados ao nível do conhecimento do genoma humano, as tecnologias biométricas não abarcavam a identificação através do perfil de DNA dos indivíduos; e a sua dimensão da vigilância, na medida em que, esta recorre às novas tecnologias de informação com o objetivo de facilitar um maior acesso a dados sobre os indivíduos vigiados.

De modo a alcançar os objetivos enunciados esta tese mobiliza, num primeiro momento, uma análise de conteúdo de entrevistas aplicadas a Pontos de Contacto Nacionais do sistema Prüm. O estudo das narrativas destes atores permitirá, de modo geral, a compreensão das práticas e expectativas a respeito do sistema Prüm, da cooperação transnacional e das perceções sobre proteção de dados ao nível da União Europeia. Num segundo momento, será realizada uma análise de conteúdo de entrevistas conduzidas a atores sociais do sistema de justiça, a membros de comissões de ética e a peritos forenses em Portugal e no Reino Unido. O enfoque nos países referidos permitirá o aprofundamento da compreensão das tensões, dinâmicas e processos de (d)standardização por se

encontrarem desalinhados das práticas e expectativas gerais a respeito do processo de implementação do sistema Prüm.

Portugal é um dos estudos de caso da tese por ser um país que tem ambicionado a modernização do sistema de justiça através da tecnologia de modo a acompanhar os países mais desenvolvidos ao nível da investigação criminal (Amelung, Granja, & Machado, 2020; Machado & Silva, 2010). A recente criação da base de dados forense de perfis de DNA, em 2008, e a partilha transnacional de informações de DNA podem ser elencadas como exemplos desta postura. Posto isto, o contexto cultural, social e económico português tem influenciado o modo como estas infraestruturas são projetadas, principalmente, devido à escassez de recursos económicos, aos baixos índices de criminalidade grave e aos baixos níveis de confiança pública no sistema de justiça em geral. A estrutura do sistema justiça caracterizada pelo sistema inquisitorial e por uma das legislações sobre a base de dados forenses de perfis de DNA mais restritivas da União Europeia conferem a Portugal um contexto particular para o aprofundamento das temáticas em estudo (*idem*; Machado & Silva, 2008b).

Por sua vez, o Reino Unido, foi selecionado como estudo de caso por ser um dos países impulsionadores da inovação ao nível das tecnologias de DNA, com uma longa tradição na utilização destas tecnologias no sistema de justiça criminal (sistema adversarial). A sua base de dados é a mais antiga do mundo e possui, proporcionalmente, o maior número de população inserida (Downey, Stephens, & Flaherty, 2012; Johnson & Williams, 2007). A sua postura política quanto ao sistema Prüm tem sido caracterizada por vários avanços e recuos face à decisão de implementar este sistema de cooperação. Deste modo, em 2014, a vontade política ditou que o Reino Unido não iria fazer parte da cooperação transnacional operada pelo sistema Prüm. Mais tarde, em 2015, após a realização de testes com outros países, o Governo britânico decidiu proceder à sua implementação. No entanto, a votação do referendo para o *Brexit*, em 2016, condicionou o andamento do processo de implementação do sistema Prüm e o país só ficou operacional em 2019 (Council of the European Union, 2019a). Neste cenário e com a saída oficial do país da União Europeia a sua permanência no sistema Prüm encontra-se mais uma vez em causa. No contexto britânico, o discurso político a respeito do sistema Prüm tem sido o de o instrumentalizar para a redução da criminalidade levada a cabo por estrangeiros no país, fazendo-se acompanhar por tentativas de limitação na partilha de informações de cidadãos britânicos com outros

países. O avanço ao nível das tecnologias de DNA, as especificidades da base de dados forense de perfis de DNA e o tipo de sistema legal que caracteriza o Reino Unido constituem elementos que permitem o aprofundamento das dinâmicas e dos processos de (d)estandardização na implementação do sistema Prüm.

O presente estudo visa o mapeamento das condições de determinado fenómeno ou acontecimento (Law, 2009), sendo precisamente o reconhecimento das suas interconexões que permite discernir sobre os potenciais desafios e dilemas da proteção de dados num contexto de investigação criminal. Da análise da operacionalização do sistema Prüm é possível a identificação dos atores que mobilizam as tecnologias de DNA, que operam a rede de partilha de dados e que contribuem para a co-construção de poder. Em concreto, os atores que contribuem para o funcionamento do sistema Prüm são os peritos forenses, os Pontos de Contacto Nacionais e outros *stakeholders*, respetivamente, a comunidade de geneticistas forenses que desenvolvem investigação académica e tecnológica com potencial de aplicação na investigação criminal, as comissões de ética que monitorizam e regulam a utilização das bases de dados genéticos forenses e os agentes do sistema de justiça criminal. Acrescente-se que esta infraestrutura de partilha de dados com dimensão europeia depende igualmente de *softwares* – como a rede sTESTA⁵ e o CODIS – que permitem eletronicamente a partilha de informações, bem como do próprio perfil de DNA e das Diretivas e regulações Europeias a este respeito (Machado & Costa, 2013). Posto isto, o sistema Prüm, enquanto rede tecnológica, pode ser entendido como um “centro de cálculo” (Latour, 1987a) ou “ponto de passagem obrigatória” (Callon, 1991).

A análise do sistema Prüm permitirá compreender de que modo as decisões tomadas pela União Europeia face ao desenvolvimento tecnológico (biotecnologia) e proteção de dados pessoais têm gerado diferentes respostas por parte dos Estados democráticos liberais, onde a ciência e a tecnologia devem servir o interesse público. A existência de diferentes iniciativas legislativas, por parte dos países da União Europeia, no que concerne à regulação da utilização de tecnologias forenses no combate à criminalidade e com respeito ao direito à proteção de dados pessoais é exemplo de que apesar de existirem normas europeias, os contextos nacionais têm seguido caminhos dissemelhantes na proteção dos dados pessoais dos seus cidadãos (Jasanoff, 2005; Machado & Santos,

⁵ Disponível em https://ec.europa.eu/isa/ready-to-use-solutions/stesta_en.htm. Acesso a 6 de junho de 2017

2016). Os mecanismos de participação pública, os níveis de confiança nas tecnologias e a noção de direitos cívicos variam de acordo com o tipo de práticas envolvidas na utilização das tecnologias de vigilância forenses por parte dos Estados, bem como com a aceitação pública da ciência e da tecnologia no que concerne às tecnologias genéticas.

Em particular, o estudo mobiliza o conceito de (d)estandardização (Lampland & Star, 2009; Timmermans & Epstein, 2010) da privacidade e o conceito de imaginários sociotécnicos (Jasanoff & Kim, 2009) para a análise das narrativas dos participantes. O recurso ao conceito de (d)estandardização permitiu analisar as perspectivas a respeito do sistema Prüm, por parte dos Pontos de Contacto Nacionais, por se considerar que este empreendimento europeu se apoiou em noções de estandardização tecnocientíficas pretenderam neutralizar as diferenças legais, culturais e políticas dos países (Lampland & Star, 2009, pp. 4-5; Prainsack & Toom, 2010, 2013). Porém, as divergências encontradas, ao nível dos enquadramentos legais, têm colocado tensões à sua implementação atuando enquanto agentes de destandardização do próprio sistema. Deste modo, a desconstrução da *black box* da privacidade no sistema Prüm permite apreender a performatividade da proteção de dados nas redes tecnológicas em que as informações genéticas circulam (Barad, 2003; Law, 2008; Tsekeris, 2007). Portanto, analisar as consequências para a vida social dos cidadãos que advêm da implementação do sistema Prüm permite compreender os modos de apropriação local e nacional dos *standards* de proteção de dados definidos no âmbito da União Europeia.

A respeito do estudo de duas realidades nacionais, Portugal e o Reino Unido, a reflexão realizada apoiou-se concretamente no mapeamento dos ‘imaginários sociotécnicos’ (Jasanoff & Kim, 2009) destes países, pois pretendeu-se compreender o posicionamento, face ao fenómeno da partilha transnacional de dados genéticos e pessoais, dos atores de diversas áreas (ética, direito, ciência forense) que têm contribuído para o debate sobre as controvérsias levantadas pelo uso da biotecnologia no sistema de justiça. A concretização deste objetivo passou por tornar visível o que tem sido fechado em *black boxes* trazendo à discussão a privacidade e a forma como esta é apreendida pelos atores nas suas práticas mundanas “with the same attention as has been paid to the abstract ethics principles guiding existing policy work” (Hoeyer, Tupasela, & Rasmussen, 2016, p. 19). A “viagem” de informação genética entre Estados-Membros é realizada através de “infraestruturas sociomateriais” que vão além do objetivo de armazenamento e partilha,

“[t]here is a morality built into the ties between people, and these ties restrict the flows” (*idem*, p. 13). Esta dimensão moral da partilha transnacional de dados foi captada através dos imaginários sociotécnicos observados nas narrativas dos entrevistados.

A presente tese encontra-se dividida em quatro capítulos de teor teórico, metodológico e empírico. No primeiro capítulo é realizado o enquadramento teórico do estudo através do aprofundamento das temáticas relevantes para a análise dos dados empíricos recolhidos. Neste sentido, são apresentados os temas respeitantes ao debate atual da proteção de dados na União Europeia, à cooperação policial e judiciária transnacional operada através do sistema Prüm, à reflexão sobre o conceito de privacidade quanto à sua dimensão social, aos tipos de vigilância e respetivos modos de operar, às bases de dados forenses de DNA, à (d)estandardização da utilização de perfis forenses de DNA no seio da esfera científica e legal e ao aprofundamento do contributo do conceito de imaginários sociotécnicos para a análise de duas realidades nacionais. Dito isto, os contributos teóricos que constam neste capítulo permitem a concretização do primeiro objetivo da tese que remete para o mapeamento do debate em torno da proteção de dados e da privacidade na União Europeia. Primeiro, devido à especificidade do debate e da regulação em relação a dados para investigação criminal face à proteção de dados em geral. Segundo, devido à identificação das tensões e controvérsias em torno da proteção de dados pessoais *versus* vigilância e segurança das sociedades. O segundo capítulo é o da metodologia onde se clarifica o enquadramento da tese no âmbito do projeto de investigação Exchange e são justificadas as opções metodológicas tomadas para a recolha e análise dos dados empíricos. Em particular, explicaram-se os métodos de amostragem dos entrevistados, o modo de recolha dos dados e os procedimentos éticos tidos em consideração no decorrer do estudo.

Os últimos capítulos da tese são de caráter empírico. No capítulo três é realizada a análise das perspetivas dos Pontos de Contacto Nacionais para o passo 1 e o passo 2 do sistema Prüm. Em concreto, a análise foca-se nos benefícios e utilidade deste sistema de partilha de dados, na sua estrutura de partilha de informação em dois passos, nos riscos e desafios da sua implementação, no seu futuro e eficácia enquanto ferramenta de cooperação policial e judicial e nos seus desafios quanto à privacidade e proteção dos dados partilhados entre Estados-Membros. Num último ponto são também analisadas as suas perspetivas a respeito da possível interoperabilidade entre bases de dados forenses e

biobancos médicos. As temáticas exploradas vertem diretamente da análise das entrevistas semiestruturadas realizadas aos Pontos de Contacto Nacionais e pretendem concretizar de modo complementar dois dos objetivos da tese. Primeiro, permitem mapear os dilemas éticos e sociais que decorrem da partilha transnacional de dados genéticos forenses entre países europeus, concretamente, através do sistema de Prüm. Incluindo-se as perspetivas dos/as entrevistados/as relativamente à possível compressão de direitos civis e humanos e a possibilidade de criminalização de grupos socialmente mais vulneráveis. Segundo, permitem discernir as narrativas veiculadas por estes profissionais no que concerne às representações e sentidos atribuídos à proteção de dados e à privacidade.

No capítulo quatro é realizada a análise empírica das narrativas de geneticistas forenses e *stakeholders* de Portugal e do Reino Unido. As dimensões de análise apresentadas neste capítulo procuram respeitar as particularidades dos contextos nacionais em estudo. Deste modo, são exploradas temáticas coincidentes entre os dois países, como também características específicas ao nível nacional que desempenham ou desempenharam um papel no decorrer da implementação do sistema Prüm. Genericamente, as dimensões em estudo remetem para as suas perceções a respeito das bases de dados forenses nacionais, sobre a implementação do sistema Prüm ao nível local e, por fim, sobre as expectativas acerca da hipotética interoperabilidade entre bases de dados forenses e biobancos médicos. Com a análise das narrativas de vários perfis de participantes em dois países diferentes pretende-se a concretização de dois dos objetivos da presente tese. Primeiro, ambiciona-se a compreensão e a identificação dos imaginários sociotécnicos de Portugal e do Reino Unido quanto ao posicionamento de atores de diversas áreas no que concerne à partilha transnacional de informações pessoais e as controvérsias levantadas pela utilização da biotecnologia pelos sistemas de justiça. Segundo, e de modo complementar, pretende-se explorar e identificar as narrativas destes atores quanto ao sentido que atribuem ao conceito de proteção de dados e de privacidade. Portanto, neste capítulo, a mobilização do conceito de imaginários sociotécnicos, dos estudos da ciência e da tecnologia, pretendeu tornar o estudo comparativo dos dois contextos nacionais mais completo para que se consiga compreender quais os processos sociais de co-construção entre ciência e ordem social.

CAPÍTULO 1. ENQUADRAMENTO TEÓRICO

1.1. Sistema Prüm

Nos últimos anos, tem-se assistido a cenários renovados relativamente à partilha transnacional de dados no âmbito forense. Contextualizando, o Tratado de Schengen (1997)⁶ visou a promoção da livre circulação de indivíduos entre países europeus. Porém, com a abertura de fronteiras, os Estados-Membros foram alvo de novos desafios no que concerne à segurança nacional e, com eles, surgiu a “demanda contra o terrorismo e o crime organizado” (Hert, 2005). Numa tentativa de colmatar estes desafios, o desenvolvimento tecnológico e a potencialidade da utilização das bases de dados genéticos para identificação atravessaram fronteiras com o Tratado de Prüm, celebrado em 2005, por um grupo de países, nomeadamente, Alemanha, Áustria, Espanha, França, Bélgica, Holanda e Luxemburgo, ao qual mais tarde se juntaram França, Itália e Portugal (Kierkegaard, 2008; Machado & Granja, 2019a; Matos, 2019; O’Neill, 2010).

A cooperação com base no Tratado de Prüm é realizada através da partilha de dados sociodemográficos associados a perfis genéticos, registos de veículos automóveis e impressões digitais, através de um sistema de *hit/no hit*. Esta tese, em particular, debruça-se sobre a partilha de perfis genéticos. A partilha de dados é operacionalizada através de uma estrutura de dois passos (*steps*). O primeiro passo é automatizado e tem como objetivo verificar as correspondências entre perfis de DNA de diferentes Estados-Membros. Se a correspondência se confirmar, os países envolvidos podem avançar para o segundo passo. Isto é, a solicitação da informação sociodemográfica associada ao perfil genético que gerou a correspondência. Esta partilha deve decorrer de acordo com a lei de Proteção de Dados dos países envolvidos, bem como os critérios mínimos estabelecidos pela Comissão Europeia para a proteção de dados (Machado & Silva, 2010; Prainsack, 2010). Saliente-se que este processo permite avaliar a legislação nacional e perceber se a troca se encontra de acordo com os parâmetros de legalidade, como também verificar se as medidas de proteção de dados vigoram em relação à troca de dados pessoais (McCartney et al., 2011, p. 316; Prainsack & Toom, 2010). Importa realçar que o segundo passo não é automático, nem obrigatório, pelo que são os Estados-Membros envolvidos que decidem se procedem ao pedido ou ao envio da informação solicitada. Só em 2008 surge a decisão 2008/977/JAI do

⁶ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:l33020>. Acesso a 12 de maio de 2020.

Conselho da União Europeia⁷ que remete para a proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (Gonçalves & Jesus, 2012, p. 123; O'Neill, 2010). A argumentação em torno da legitimação deste sistema de vigilância genética segue os mesmos contornos dos restantes aparelhos tecnológicos, pois recorre ao discurso político sobre a necessidade de combater o terrorismo como forma de justificar o (re)equilíbrio da liberdade e da privacidade com a segurança coletiva (Bigo, 2008, p. 92). No entanto, certos autores alertam para as críticas que têm sido tecidas a esta iniciativa, sendo uma das mais recorrentes a que remete para o facto de esta decisão não abranger o processamento de informações pessoais realizado ao nível nacional, isto é, cinge-se à regulação do plano transnacional da sua partilha (Gonçalves & Jesus, 2012, p. 123).

A transposição do Tratado de Prüm para a lei da União Europeia – sistema Prüm⁸, em 2008, gerou intenso debate em torno da proteção de dados (Decisão 2008/615/JHA⁹ de 23 de junho) (Kierkegaard, 2008, pp. 243-244; Maciel & Machado, 2014, p. 149). Estima-se que com o sucesso deste aparelho de vigilância genética, sejam partilhados cerca de 10 milhões de perfis de indivíduos entre os países da União Europeia (Prainsack & Toom, 2010, 2013; Santos, Machado, & Silva, 2013). O sistema Prüm é obrigatório para todos os países pertencentes à União Europeia e opera em rede, permitindo o acesso mútuo à bases de dados forenses nacionais de perfis genéticos. Não obstante este sistema procurar a uniformização tecnológica, são visíveis diferenças sociais, culturais, tecnológicas e políticas em diferentes fases da sua implementação e operacionalidade. Por exemplo, enquanto alguns Estados-Membros já possuíam bases de dados genéticas operacionais em 2008, outros países foram obrigados a proceder à sua criação. Atualmente, existem 26 países operacionais, incluindo-se neste número o Reino Unido. Outro exemplo das diferenças elencadas remete para o número de conexões entre os países, enquanto Portugal se encontra a trocar dados com 19 países, o Reino Unido apenas o faz com 6 Estados-Membros. [citar DAPIX]

Peter Hustinx, da Autoridade Europeia para a Proteção de Dados, emitiu, a este respeito, um parecer onde expressava a sua preocupação com a inexistência de uma estrutura geral que garantisse a proteção de dados quando a sua partilha é realizada em

⁷ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32008F0977&from=PT>. Acesso 12 de maio de 2020.

⁸ No âmbito desta tese, o passo 2 é considerado enquanto parte integrante do sistema Prüm.

⁹ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32008D0615&from=PT>. Acesso 12 de maio de 2020.

grande escala, como se verifica com o sistema Prüm. Para Hustinx, a ausência desta estrutura poderia incorrer numa supressão de direitos civis dos cidadãos, bem como comprometer a eficácia das autoridades na aplicação da lei devido à possibilidade do aumento da taxa de falsos positivos entre perfis de DNA e nas comparações entre impressões digitais (Kierkegaard, 2008, p. 245; Prainsack & Toom, 2010, p. 1124). No entanto, apesar das lacunas descritas pela Autoridade Europeia para a Proteção de Dados, deve salientar-se, novamente, que a partilha de informação realizada no âmbito de Prüm só resulta na transferência de dados pessoais dos cidadãos entre os Estados-Membros quando se verifica a ocorrência de um *hit*, sendo esta concretizada através de canais mútuos de assistência jurídica (McCartney et al., p. 316).

Pensando no enquadramento social e legal do sistema Prüm, Bellanova (2008), refere que é necessário que este mecanismo de vigilância seja avaliado de forma a compreender as implicações que pode ter, parafraseando, na transparência, legitimidade e direitos fundamentais devido à partilha de dados pessoais e custos associados à sua implementação (p. 204). O autor aponta também uma fragilidade do sistema quanto à proteção de dados, esta prende-se com o facto de que as negociações iniciais sobre Prüm carecerem do envolvimento das autoridades nacionais de proteção de dados, bem como da presença da Autoridade Europeia para a Proteção de Dados (*idem*, p. 205). Também a implementação da partilha de dados pessoais tem enfrentado problemas, por um lado, devido à falta de confiança entre as autoridades dos Estados-Membros (Hijmans, 2006, pp. 2-3; Hufnagel, 2012; Hufnagel & McCartney, 2015), por outro, devido à propriedade dos dados (Bigo, Bruggeman, Burgess, & Mitsilegas, 2007). Outra crítica remete para a obrigação legal da criação de bases de dados de DNA, por parte dos Estados-Membros, sendo que esta disposição político-legal permite a implementação destas bases de dados sem que o tema seja debatido no plano nacional, quer por parte da opinião pública, quer pelo próprio parlamento (Bellanova, 2008, p. 212). Por fim, o sistema Prüm baseia-se na dicotomia DNA codificante e não-codificante como forma de salvaguarda dos dados genéticos dos indivíduos que constam nas bases de dados de perfis de DNA (*idem*, p. 213). Porém, face ao estado do desenvolvimento das tecnologias de DNA, como as NGS, esta dicotomia encontra-se cada vez mais diluída. Por fim, Bellanova (2008) realça um aspeto crucial sobre a avaliação da implementação de Prüm que coloca a tónica nas diferentes relações de poder que os sistemas de vigilância têm vindo a denotar. Em particular, de que forma é que se

pode avaliar a proporcionalidade das medidas aplicadas à supressão da privacidade, se os atores mais relevantes no processo “are marginalized in the field of struggle” (*idem*, p. 217).

Sob este pano de fundo levantam-se desafios relativos ao controlo social, à cidadania e à democracia no espaço da União Europeia. Em particular: 1) a perceção nacional e internacional em relação ‘ao que é boa governação’ e o ‘que é boa ciência’ pode não coincidir; 2) a prevalência da falta de transparência e de prestação de contas relativas às Decisões Prüm; 3) a potencial emergência da categoria de ‘populações suspeitas’ ao nível transnacional, pois certos países permitem a retenção de perfis de indivíduos que nunca foram condenados ou formalmente acusados como suspeitos de um crime; e, por fim, 4) a existência de diferenças socioeconómicas entre os países da União Europeia (Balzacq et al., 2006; Balzacq, 2005; Brown, 2009; Kietz & Maurer, 2006; Liu, 2013; McCartney et al., 2011). Por um lado, o sistema Prüm veio salvaguardar direitos coletivos, como a segurança e o bem-estar, e individuais como a satisfação da necessidade de justiça das vítimas de crime. Por outro lado, veio colocar em causa a capacidade de harmonização europeia tão ambicionada, pois os obstáculos ao enquadramento global legal da proteção de dados podem estar relacionados, num contexto nacional, com a falta de recursos e especialistas em questões de privacidade e de formas de assegurar a proteção de dados (Costa & Nunes, 2001; Fiodorova, 2014, p. 130; Prainsack & Toom, 2013).

1.2. Proteção de dados pessoais na União Europeia

O exponencial desenvolvimento tecnológico ao nível dos sistemas de informação tem potenciado várias mudanças estruturais no acesso, processamento e troca de dados pessoais dos cidadãos. Considera-se que na era da economia da informação os dados pessoais dos cidadãos passam a ser equacionados enquanto moeda de troca de modo a garantir o acesso ‘gratuito’ (Dijck, 2014, p. 197). Na medida em que não incluem o pagamento de uma taxa de utilização, a vários serviços sejam eles do foro público, como os balcões *online* das finanças, ou de âmbito privado, como a subscrição de serviços de email da Google.

Neste pano de fundo, as autoras Gonçalves e Jesus (2013) identificaram que a relevância dada, por parte das organizações públicas e privadas, aos dados pessoais dos cidadãos encontra-se, geralmente, em rota de colisão com o que é esperado pelos mesmos

em questões de privacidade. Esta discrepância de expectativas sobre a recolha, processamento e possível partilha de dados pessoais deve-se, por um lado, ao facto de as empresas procurarem alcançar a máxima eficiência sem obstáculos e sem custos elevados, nomeadamente, através do recurso à “informatização de dados e à comunicação eletrónica” (p. 155). Por outro lado, prende-se com o facto de os indivíduos se posicionarem no sentido de ambicionarem o uso legítimo, adequado e proporcional dos seus dados pessoais por parte das organizações que os recolheram. Nas palavras das autoras, estes cidadãos esperam a “salvaguarda da sua privacidade e da sua intimidade” (*idem*, p. 255). Dito isto, o conceito de proteção de dados, central para a presente discussão, remete para a criação de normas que visam, genericamente, a proteção dos direitos e liberdades dos indivíduos que têm os seus dados pessoais “recolhidos, armazenados, processados, disseminados, destruídos, etc.” de modo a permitir que estes exerçam o controlo autónomo sobre os mesmos, com o objetivo de prevenir intrusões abusivas na sua privacidade que podem, em última análise, produzir consequências insanáveis (Thorogood & Zawati, 2015, p. 693). Neste sentido, a União Europeia tem vindo a desenvolver um conjunto de instrumentos legislativos (nem sempre vinculativos) para que os cidadãos tenham o seu direito à proteção de dados e à privacidade protegidos.

A Declaração Universal dos Direitos Humanos¹⁰ consagra no artigo 12.º o direito à privacidade e ressalva também que intrusões injustificáveis e ilegais não podem, ou não devem ocorrer, assumindo-se que esta interferência só é aceitável por questões relacionadas com moralidade, ordem pública e bem-estar geral (Liu, 2013; Prainsack & Aronson, 2015; Thorogood & Zawati, 2015, p. 692). Brevemente, no plano europeu tem-se a Carta dos Direitos Fundamentais da União Europeia¹¹ que estipula nos artigos 7.º e 8.º o respeito pela vida privada e a proteção dos dados pessoais como direitos fundamentais. Esta Carta integra-se no Tratado de Lisboa¹² e é juridicamente vinculativa nas instituições e órgãos da União e nos Estados-Membros quando estes aplicam legislação da UE. A Convenção 108 de 1981 do Conselho da Europa¹³ para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais foi o primeiro instrumento

¹⁰ Disponível em <https://dre.pt/web/guest/pesquisa-avancada/-/asearch/446107/details/maximized?order=whenSearchable&search=Pesquisar&sortOrder=ASC&numeroDR=57&types=SERIEI&dataPublicacaoInicio=1978-03-09>. Acesso a 12 de maio de 2020.

¹¹ Disponível em http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso a 12 de maio de 2020.

¹² Para mais informações consultar o Tratado de Lisboa em <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=PT>.

¹³ Disponível em <https://rm.coe.int/1680078b37>. Acesso a 12 de maio de 2020.

internacional juridicamente vinculativo em matéria de proteção de dados pessoais. Esta Convenção pretendeu «garantir (...) a todas as pessoas singulares (...) o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal». A Convenção Europeia dos Direitos Humanos¹⁴ reconhece no artigo 8.º o direito ao respeito pela vida privada e familiar, onde se ressalva, mais uma vez, que “não pode haver ingerência da autoridade pública no exercício deste direito senão quando (...) seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros”.

Mais recentemente, tem-se ainda a Diretiva Europeia de Proteção de Dados Pessoais que remete para o processamento e partilha de dados, redigida pela primeira vez em 1995 (Brown, 2009; Human Genetics Commission, 2001; Hustinx, 2010). Em particular, a Diretiva 95/46/CE¹⁵ regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos, que foi revogada em maio de 2018. Estabeleceram-se, neste documento, vários princípios que devem ser cumpridos pelas entidades/organizações públicas e privadas que controlam e processam dados pessoais. Nomeadamente, a (1) limitação da finalidade (*purpose limitation*), onde se reitera que os dados pessoais apenas devem ser recolhidos para “finalidades específicas, explícitas e legítimas”, sendo que estes não devem ser utilizados para fins diferentes dos que motivaram a sua recolha. A (2) minimização de dados (*data minimization*), que tem por objetivo que não seja recolhida informação pessoal para além da necessária para um fim específico. A (3) proporcionalidade (*proportionality*), onde os dados recolhidos devem ser “adequados, relevantes e não excessivos” no que concerne aos fins para que serão utilizados. Por fim, o (4) controlo de dados (*data control*), que tem que ver com a responsabilização do Estados-Membros da UE quanto à supervisão da recolha, análise e do processamento dos dados pessoais (Brown, 2009; European Data Protection Supervisor, 2006; Gamero et al., 2008; Gonçalves, 2018; Gonçalves & Jesus, 2012, 2013; Harbo, 2010; Hert, 2005; IRISS, 2012). Pretendeu-se com a redação deste instrumento legislativo a criação de um critério mínimo de proteção de dados pessoais entre todos os países da União

¹⁴ Disponível em http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso a 12 de maio de 2020.

¹⁵ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=pt>. Acesso 12 de maio de 2020.

Europeia. É de salientar que este documento não é passível de ser aplicado em dados anónimos, pois como pode ler-se no artigo 2.º, alínea a, que os dados são pessoais, na medida em que remetem para um indivíduo identificado ou identificável. No entanto, a Diretiva não abrangeu a esfera da aplicação e cumprimento da lei penal (artigo 3.º, n.º 2). Neste contexto, a União Europeia tem vindo a desenvolver políticas de segurança cada vez mais expansivas, que têm categoricamente permitido o aumento de informação dos cidadãos que é recolhida, armazenada, processada e partilhada (Aas, 2006, 2009, 2013; Gilbert, 2007; Lyon, 2014).

No entanto, com a evolução tecnológica, a crescente globalização dos mercados (Lyon, 2004) e as diferentes apropriações, por parte dos Estados-Membros, das normas previstas na Diretiva supramencionada, o Parlamento e o Conselho Europeu apresentaram, em 2012, um novo pacote legislativo que visou reformar a legislação relativa à proteção de dados da UE. Pretendeu-se com esta solução a criação de uma legislação única de forma a evitar a fragmentação entre Estados e a diminuição dos dispendiosos encargos administrativos. Pode ler-se no *website* do Parlamento Europeu¹⁶ que o sucesso desta reforma “ajudará a reforçar a confiança dos consumidores nos serviços em linha, proporcionando o tão necessário impulso para o crescimento, o emprego e a inovação na Europa”. Neste sentido, foi apresentada a proposta para o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho¹⁷, de 27 de abril de 2016, que remete para a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revogou a Diretiva 95/46/CE.

Relativamente à proteção de dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal tem-se a Decisão-Quadro 2008/977/JAI do Conselho¹⁸, de 27 de novembro de 2008, revogada em maio de 2018. Este documento abrange apenas os dados policiais e judiciários partilhados entre os Estados-Membros, as autoridades e os sistemas associados da União Europeia, não abrangendo, deste modo, os dados tratados no âmbito nacional. De forma a modernizar os pressupostos presentes no documento, o novo pacote legislativo também possui uma proposta para a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho¹⁹, de 27 de abril de 2016, relativa à proteção das

¹⁶ Disponível em http://www.europarl.europa.eu/atyourservice/pt/displayFtu.html?ftuid=FTU_5.12.8.html. Acesso a 12 de maio de 2020.

¹⁷ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso a 12 de maio de 2020.

¹⁸ Disponível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:pt:PDF>. Acesso a 12 de maio de 2020.

¹⁹ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT>. Acesso a 12 de maio de 2020.

peças singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

Regulação e supervisão na proteção de dados

A supervisão do (in)cumprimento dos instrumentos legislativos enunciados é realizada em diferentes níveis por várias instituições europeias. A Autoridade Europeia para a Proteção de Dados (AEPD)²⁰ é a entidade supervisora independente que assegura que as instituições e os órgãos da UE respeitam as suas obrigações em matéria de proteção de dados dos cidadãos. Em particular, (1) pode prestar aconselhamento a instituições e órgãos da UE sobre questões relacionadas com o processamento de informações pessoais, sendo consultada pelo legislador da UE para propostas de legislação e novas políticas que podem afetar a privacidade. (2) É responsável pela monitorização de novas tecnologias que possam afetar a proteção de informações pessoais. (3) Intervém perante o Tribunal de Justiça da UE através da redação de pareceres especializados sobre a interpretação da legislação em matéria de proteção de dados. E, por fim, (4) coopera com as autoridades nacionais de supervisão com o objetivo de trazer maior consistência à proteção de dados pessoais no plano nacional. O Grupo de Trabalho do Artigo 29.⁹²¹ é também um órgão de consulta independente sobre a proteção de dados e privacidade, criado pelo artigo 29.º da Diretiva 95/46/CE. Tem como membros os representantes das autoridades nacionais de proteção de dados dos Estados-Membros da União Europeia, da AEPD e da Comissão. Este órgão emite recomendações, pareceres e documentos de trabalho, sendo futuramente substituído, devido ao novo pacote legislativo, pelo Comité Europeu para a Proteção de Dados.

A União Europeia possui na sua constituição outras instituições que não supervisionando diretamente o processamento da proteção de dados e privacidade, são também importantes para a garantia e proteção destes direitos. A Agência dos Direitos Fundamentais (FRA) da União Europeia posiciona-se ao lado das Nações Unidas e do Conselho da Europa, assumindo que a União Europeia se depara com desafios específicos relativos à crescente utilização de tecnologias. Exacerbando-se a necessidade de garantir e promover os direitos fundamentais dos cidadãos em contexto virtual. Neste sentido, a

²⁰ Disponível em https://edps.europa.eu/edps-homepage_en?lang=pt. Acesso a 12 de maio de 2020.

²¹ Disponível em http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083. Acesso a 12 de maio de 2020.

agência FRA presta aconselhamento independente a responsáveis políticos ao nível nacional e da UE, em particular, sobre discriminação, acesso à justiça, racismo e xenofobia, proteção de dados, direitos das vítimas e direitos das crianças. Deste modo, pretende tornar mais eficazes as políticas, a legislação e as ações de promoção em matéria de direitos humanos fundamentais. A concretização deste objetivo é realizada através da recolha e análise de informações no âmbito de trabalhos de investigação de cariz sociojurídico, garantindo um aconselhamento fundamentado. A Confederação das Organizações Europeias de Proteção de Dados, foi fundada em 2011, e é uma organização que pretende reunir todos os órgãos nacionais de proteção de dados dos Estados-Membros da UE. A sua fundação deveu-se, essencialmente, à adoção e implementação do Regulamento Geral de Proteção de Dados (GDPR), tornando-se pró-ativa na apresentação de propostas concretas para ajudar a definir o pacote de legislação atual, bem como na publicação de vários documentos sobre o mesmo. Por fim, tem-se a Comissão Europeia, que não sendo o seu enfoque especificamente, também se dedica à proteção de dados e privacidade dos cidadãos europeus. O seu objetivo é o de “simplificar a vida dos europeus que estudam, trabalham ou constituem família noutros países da UE (...). Só um espaço europeu de justiça sem descontinuidades nem fronteiras dará a certeza aos cidadãos de que beneficiam do mesmo conjunto de direitos em toda a Europa”. Desta forma, pretende garantir que os europeus partilham os valores consagrados nos Tratados da UE e na Carta dos Direitos Fundamentais, onde consta o direito à proteção de dados.

Apesar de todos os esforços e instituições responsáveis pela salvaguarda de direitos civis e humanos, nomeadamente, o direito à privacidade e à proteção de dados, Charles Raab (2008) enumera seis fragilidades que podem ser encontradas no enquadramento legal da privacidade e da vigilância tecnológica. Primeiro, revela-se tendencialmente reativa, na medida em que a legislação para a utilização de certas tecnologias é criada posteriormente ao seu desenvolvimento e aplicação. Segundo, carece de abordagens híbridas e inovadoras, sendo que se tem focado maioritariamente em aspetos de ordem técnica e administrativa. Terceiro, não tem equacionado de modo adequado o que é considerado ‘interesse público’, na maioria das vezes, este reflete apenas a ideologia do legislador que possui uma conceção demasiado restrita sobre privacidade. Quarto, a aplicação e criação de leis tem sido realizada à margem do debate público, exceto o que ocorre entre especialistas da área. Quinto, a regulação que incide sobre a salvaguarda da privacidade e a proteção de dados é,

com frequência, em termos políticos, encarada como um obstáculo para o mercado e a para o Estado, pois pode inibir o fluxo de informação. Sexto, e último, a reflexão sobre enquadramento legal tem sido influenciada pelos discursos polarizados reproduzidos nos meios de comunicação social. Por um lado, centram-se em histórias de terror sobre a invasão de privacidade, por outro, passam narrativas exageradas acerca das potencialidades das novas tecnologias, invisibilizando as complexas questões éticas, políticas e sociais que a vigilância envolve (pp. 257-258).

1.3. Cooperação transfronteiriça policial e judiciária

Os ataques terroristas em várias cidades europeias, como em Madrid (2004) e Londres (2005) e, mais recentemente, em Paris (2015) e Bruxelas (2016), reacenderam nas agendas políticas de vários Estados-Membros a necessidade de aprofundar a cooperação transfronteiriça de natureza policial e judiciária. Neste cenário, ganharam renovada legitimidade no espaço público e político a implementação de redes e sistemas tecnológicos sofisticados que visam a identificação e o controlo de indivíduos e populações “suspeitas” (Cole & Lynch, 2006; Haggerty & Ericson, 2000; Maciel & Machado, 2014). Exemplo destes sistemas tecnológicos são o *European Dactyloscopy* (Eurodac) que entrou funcionamento em 2003 enquanto base de dados que tem por finalidade a comparação de impressões digitais de requerentes de asilo; o *Visa Information System* (VIS), a funcionar desde 2011, com o objetivo de partilhar dados sobre vistos entre os Estados-Membros da área Schengen; e as ‘Decisões Prüm’ (Decisão 2008/615/JAI, 2008 e Decisão 2008/616/JAI, 2008) que visam a partilha de dados genéticos, registo de veículos e impressões digitais com o objetivo de combater o terrorismo e a criminalidade organizada.

Como estratégia de combate à criminalidade, a União Europeia implementou a criação de bases de dados de perfis genéticos e a sequente partilha transnacional de perfis de DNA para fins de investigação criminal (McCartney, Wilson, & Williams, 2011; McCartney, 2013, 2014a; Prainsack & Toom, 2010, 2013). A implementação destas bases de dados tem gerado debate sobre os desafios éticos, sociais e políticos, em particular, em matéria de privacidade e proteção de dados. Acresce o facto de vários autores argumentarem que a expansão generalizada destas bases de dados aliada ao aumento do controlo e vigilância sobre os indivíduos tem levado à criminalização e vulnerabilização de determinadas populações (Chow-White & Duster, 2011; Duster, 2004, 2006; Machado, Silva,

& Amorim, 2010) e, conseqüentemente, tem potenciado a sua estigmatização (Aas, 2011; Ball, Di Domenico, & Nunan, 2016; Williams & Johnson, 2004a, 2004b). Um ponto fundamental que tem estado na origem da falta de legitimação destas bases de dados tem que ver com a ausência de um suporte legal que sirva os princípios da proteção de dados no campo criminal penal e de investigação criminal (Gonçalves & Jesus, 2013, pp. 255-256), sendo este um dos obstáculos que se pretende ultrapassar com o novo pacote legislativo da União Europeia em matéria de proteção de dados²².

O presente estudo irá apoiar-se no chamado Sistema Prüm como exemplo desta realidade no espaço da União Europeia. O Tratado de Prüm foi assinado em 2005, por vários Estados-Membros da UE, de forma a garantir o acesso mútuo às bases de dados forenses nacionais de perfis genéticos, tal como de impressões digitais e de registo de veículos. A análise deste sistema tecnológico de dimensão considerável pretende abarcar todos os Estados-Membros, será realizada com base sociológica e numa perspetiva interdisciplinar que procura contributos dos Estudos da Ciência e da Tecnologia, em particular, os estudos da genética forense, da biocidadania e da genetização da sociedade, bem como dos estudos da vigilância. Desta forma, pretende-se, com o cruzamento de disciplinas, alcançar e compreender a multiplicidade de desafios desencadeados por este fenómeno que comporta em si componentes da área tecnológica, pois é um sistema tecnológico que funciona em rede; verte parte do conhecimento da área da genética, através do trabalho desenvolvido nos perfis e nas amostras de DNA; e, por fim, dos estudos da vigilância, na medida em que as novas tecnologias vieram facilitar e permitir um maior acesso a dados sobre os indivíduos vigiados.

1.4. Privacidade – conceito social?

O novo pacote legislativo proposto pelo Parlamento Europeu e o Conselho vem reforçar a necessidade de debate sobre as conseqüências que o desenvolvimento tecnológico aliado às novas formas de vigilância pode ter para a privacidade e proteção de dados dos cidadãos no espaço Schengen. Nesta secção pretende-se refletir sobre o conceito de privacidade quando este se encontra embebido no contexto tecnológico e político atual,

²² Neste pacote incluem-se os seguintes documentos: Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados; bem como o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

tentando, desta forma, ultrapassar a concepção de privacidade enquanto direito que se esgota na sua dimensão individual à luz de definições menos contemporâneas.

O galopante crescimento das tecnologias de informação tem-se apresentado como um dos potenciais perigos para a proteção da privacidade, pois este permite a vigilância generalizada dos indivíduos culminando numa capacidade de os monitorizar até então fora do alcance tecnológico das instituições. Hoje é possível observar, recolher e analisar informação sobre as pessoas permitindo segui-las através do tempo e do espaço. Os desenvolvimentos no conhecimento que permitem este tipo de práticas de vigilância ocorreram em três grandes áreas científicas. Nas bases de dados computadorizadas, na medida em que o progresso científico veio permitir uma maior capacidade de processamento (Goos, Friedewald, William, Webster, & Leleux, 2015, p. 56) que aliada à oferta abundante de dispositivos de armazenamento com custos inferiores aos praticados anteriormente contribuiu de forma substancial para o aumento das “capacities for storing, organizing, and retrieving great quantities of information” (Nissenbaum, 2010, p. 36). O avanço da ciência e da engenharia das redes de comunicação digitais, como a Internet, proporcionou a possibilidade do fluxo de informações de forma confiável e eficiente a velocidades muito elevadas, ou seja, começou a ser possível aceder a informação a partir de qualquer lugar do mundo (*idem*). Por fim, teve-se o desenvolvimento das técnicas de análise de dados, operadas através da informática computacional, da análise matemática e estatística, da criptografia e da inteligência artificial (*idem*). O *data mining* é uma das técnicas utilizadas para o efeito mencionado e tem como objetivo a “transformation of raw data into information that can be utilized as strategic intelligence within the context of an organisation’s identifiable goals” (Gandy, 2007, p. 364). Portanto, esta técnica permite uma maior capacidade de transformação de dados aleatórios em conhecimento útil devido às novas e mais eficazes capacidades de compressão, ordenação, manipulação, interpretação e partilha desses mesmos dados (Nissenbaum, 2010, p. 37). Estes avanços foram também sistematizados, com base na mesma argumentação, por Solove (2006), citando o autor:

“But aggregation’s power and scope are different in the Information Age; the data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyze it are more sophisticated and powerful” (p. 506).

Tendo como pano de fundo os avanços científicos supramencionados, existem várias posições no que concerne à proteção da privacidade. Por um lado, vários autores defendem que a sua proteção assenta, essencialmente, na limitação e no controlo do fluxo de informação que os indivíduos têm sobre os seus dados, baseando-se em conceções estritamente descritivas, normativas e legais (Raab, 2015, pp. 262-264). Por outro lado, num tom crítico, Nissenbaum (2010), defende através do conceito de integridade contextual, que os indivíduos não estão apenas preocupados em restringir o fluxo unidirecional de informação. Encontram-se, de facto, mais interessados em assegurar o uso adequado dos seus dados pessoais (*idem*). Parafraseando a autora, os indivíduos ambicionam que os seus dados fluam de forma apropriada e transparente através da prestação de contas, não pretendem necessariamente terminar ou inibir o fluxo dos mesmos (*idem*, p. 2).

Nesta fase será importante fazer um parêntesis, de modo a refletir sobre o fluxo de dados (pessoais) num momento em que se verifica o aumento da colaboração transnacional em várias esferas sociais (Hoeyer et al., 2016), nomeadamente, no plano forense. Colaboração essa regularmente operada sobre a forma de bases de dados (pessoais) partilhadas transnacionalmente. O contexto atual de partilha de informações pessoais dos cidadãos que constam nas bases de dados forenses de perfis de DNA levou à necessidade de se (re)pensarem políticas éticas e legais que controlem e restrinjam os fluxos de dados (*data flows*), bem como protejam a privacidade, a confidencialidade e a autonomia dos indivíduos. Hoeyer e colegas (2016) teorizam o fluxo de dados com base em várias questões: o que é que se move? Como se move? É legítimo esse movimento? Prosseguem realçando que esse fluxo de informações é operado através de uma infraestrutura, sendo este um conceito relacional, a infraestrutura é encarada como uma atividade e não como um objeto fixo e estanque. Onde, citando os autores, “[e]veryone and everything are simultaneously engaged in many different relations, hence there is not one infrastructure, but multiple interrelated infrastructures enacted through different practices” (*idem*, p. 7).

O trabalho de Hoeyer e colegas (2016) debruçou-se na partilha de dados na esfera médica, no entanto, podem verter-se vários pontos da sua investigação para o campo forense, de modo a facilitar a compreensão da tensão entre o que está legislado e o que é a prática da investigação criminal e do trabalho laboratorial envolvido no processo. Primeiro, a partilha transnacional de dados para fins de investigação médica, comercial ou forense exige um trabalho socialmente incorporado, onde se devem compreender os mecanismos

sociais envolvidos na mesma. O fluxo de materiais e informações sensíveis que se movem numa rede pode ser condicionado por mecanismos sociais relacionados com a expectativa de obrigações sociais mútuas. Não se trata apenas da disponibilidade de dados numa infraestrutura, mas sim das relações que existem, a título de exemplo, entre Estados-Membros da União Europeia. A exigência da criação de bases de dados nacionais forenses segue o princípio da mutualidade no sentido em que todos os países devem contribuir para um ambiente de maior segurança quer nacional quer internacional.

Em relação à privacidade e proteção de dados, a confiança que os indivíduos possuem nas instituições ou organizações que recolham, armazenem e partilham os seus dados, pode condicionar os fluxos de informação. Este condicionamento pode ser desencadeado devido a práticas policiais corruptas ou devido a fugas negligentes de informação. Segundo, as relações sociais são um fator importante para o sucesso da partilha de dados. O tipo de rede de partilha, também condiciona os 'fluxos', 'não fluxos' e o 'transbordamento de informação'. Se se analisarem as funções dos atores responsáveis por operar a partilha, conseguem mapear-se as restrições ou a inexistência das mesmas nos fluxos de partilha de informações pessoais, bem como as implicações desta prática na privacidade dos cidadãos. Ainda que exista uma regulação Europeia para esse efeito, são estes indivíduos que têm que se deparar com as tensões entre as normas formais e informais presentes na troca. Por exemplo, no âmbito do sistema Prüm, são estes indivíduos os responsáveis por decidir se todos os crimes motivam a partilha de dados pessoais, ou se apenas certos tipos de crimes podem motivar esse fluxo. Não se trata de não existir uma infraestrutura que permita o movimento dos dados, como referem os autores, há um grande volume de trabalho que é feito para que esse fluxo seja possível.

O *ethics work* (Hoeyer et al., 2016, p. 387), que os autores se propuseram a desenvolver, permite compreender a ética tácita que se encontra fora das regulações formais, mas que faz parte do dia-a-dia de quem trabalha com estas bases de dados. O conceito mostra também que apesar do entusiasmo no desenvolvimento tecnológico em relação às tecnologias forenses é necessário que este desenvolvimento esteja perto das pessoas que irão ser, em primeira instância, afetadas pela sua existência, com o objetivo de criar relações de confiança entre atores. Numa era em que o *Big Data* e o *data mining* são uma realidade, a vigilância de todos os cidadãos é também ela uma realidade. Onde a confiança nas polícias e nos órgãos que procedem às análises dos dados recolhidos é

essencial para legitimar a tecnologia e descansar as pessoas que têm os seus dados armazenados, ou seja, a garantia de que a sua privacidade e autonomia será salvaguardada neste cenário. O *ethics work* revela-se uma ferramenta relevante para a compreensão das tensões entre o plano local e o global. Sendo que a tentativa de harmonização dos *standards* científicos e de políticas de ética deve considerar o acesso que os países têm a recursos que lhe permitam fazer essas mudanças. O sistema Prüm enquanto agente de standardização da vigilância genética na União Europeia tem encontrado vários desafios. Isto porque a cooperação transnacional está embebida num contexto de diversidade política e legal, de diferentes tradições em relação às tecnologias biométricas forenses, bem como diferentes expectativas e perceções em relação ao impacto societal que esta vigilância pode operar. Entendendo-se que tem sido mais fácil atender aos critérios técnicos e científicos deste Tratado, do que às salvaguardas éticas, por exemplo, sobre privacidade e proteção de dados na partilha transnacional. Desta forma, o *ethics work*, permite perceber quais os sentidos dados às noções de privacidade e de proteção de dados no âmbito da partilha transnacional de dados num contexto de carácter securitário.

Considerando os diferentes posicionamentos face aos entendimentos sobre as dimensões de privacidade, importa fazer uma breve referência às definições avançadas por vários autores. Desta forma, Westin (1967) define privacidade enquanto “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicate to others” (p. 7). Neste seguimento, apresenta uma categorização que remete para os ‘estados de privacidade’, respetivamente, solidão, reserva, intimidade e anonimidade (Westin, 1967 *apud* Raab, 2015, p. 262), encontrando-se no grupo de autores que defendem a privacidade enquanto conceito descritivo e normativo. Na mesma linha de pensamento, Reiman (1976) defende que a privacidade é, parafraseando, uma condição que priva as outras pessoas do acesso à informação, a uma situação ou experiência sobre determinado indivíduo (p. 30). No entanto, Gavison (1980) tenta apresentar uma definição neutral do conceito, na medida em que o encara como uma forma de medir o acesso que as pessoas têm a um indivíduo através da proximidade física, bem como da informação acedida (Gavison *apud* Nissenbaum, 2010, p. 68).

Finn, Wright e Friedewald (2013) também apresentaram o seu contributo para a definição de privacidade com base em sete categorias, nomeadamente, privacidade da

pessoa, privacidade do comportamento e da ação, privacidade da comunicação pessoal, privacidade dos dados e da imagem, privacidade dos pensamentos e dos sentimentos, privacidade da localização e do espaço e, por fim, privacidade de associação que remete para a privacidade de grupo (pp. 4-6). As categorias supramencionadas verteram do trabalho de investigação que os autores realizaram face aos possíveis efeitos que vários tipos de tecnologias podem apresentar para o indivíduo. As tecnologias em estudo foram as seguintes: *whole-body image scanning*, RFID, *enabled travel documents*, *unmanned aircraft systems*, *second-generation DNA sequencing technologies*, *human enhancement*, and *second-generation biometrics* (*idem*, pp. 6-17). A título de exemplo, Finn e colegas (2013) referem que as tecnologias de sequenciação de DNA podem produzir efeitos na categoria privacidade da pessoa. Pois, as informações recolhidas pelas tecnologias de DNA podem ser de carácter sensível (sexo, etnia, saúde, entre outros) e afetar a dignidade do indivíduo, sendo que o acesso a estas informações por terceiros pode acarretar prejuízos sociais para o mesmo em matéria de autoimagem e autorrespeito. O estudo levado a cabo por estes investigadores revela-se de elevada importância para a discussão na temática da privacidade, pois o facto de desconstruírem a tecnologia nas suas várias aplicações (genética, *chip*, documentação) permitem que se discuta com maior precisão as políticas de proteção de dados e de privacidade. Sendo que objetivo último é o de equilibrar a necessidade coletiva de segurança e o direito individual à privacidade.

De forma mais genérica e também complementar às categorizações acima explanadas, Allen-Castellitto (1999) defende que a privacidade pode ser entendida sob três dimensões, nomeadamente, a privacidade física que se caracteriza pelas “special seclusions and solitude”, a privacidade informacional que remete para a “confidentiality, secrecy, data protection and control over personal information” e, por último, privacidade proprietária que diz respeito ao “control over names, likenesses and repositories of personal information” (p. 713). As dimensões apresentadas pelo autor revelam-se instrumentos de reflexão que possibilitam o aprofundamento de uma discussão fundamentada sobre os riscos que o desenvolvimento das tecnologias de informação pode trazer para a proteção da privacidade. Neste sentido, mapear e diluir os riscos que uma tecnologia pode acarretar para o indivíduo, seja de armazenamento de perfis de DNA ou de informação sobre navegação na Internet, implica que as equipas de investigadores, as instituições Europeias e as instituições nacionais estejam munidas, não só do conhecimento científico e técnico,

como também das ferramentas teóricas que auxiliem na (des)construção das dimensões e da escala de intrusão que esta opera na privacidade do indivíduo.

Não se pretende com a apresentação dos vários posicionamentos em relação à privacidade encontrar uma definição estanque da mesma, o relevante é a compreensão de que esta abarca em si diversas dimensões e fragmentos da vida social do indivíduo. Sendo que, para Nissenbaum (2010), a privacidade tem como objetivo último o da proteção da diversidade de escolhas. Porém, não implica de forma alguma a salvaguarda da liberdade de prejudicar outros indivíduos ou de praticar atos criminosos (*idem*, p. 77; Marx, 2008, p. 95). Equacionando as várias esferas da vida social dos indivíduos em que este conceito se revela de grande importância, deve ter-se em mente que a par da privacidade, também noções como autonomia, dignidade, liberdade, personalidade e autodeterminação são essenciais ao desenvolvimento individual e social do ser humano, devendo ser protegidas de igual modo (Raab, 2015, p. 262). A necessidade de proteção não só da privacidade, como também das restantes noções mencionadas, encontra a sua fundamentação em valores de ordem moral, Hoven (2001) avança com quatro tipos de proteção a ter em consideração. Primeiro, *information-based harm*, neste caso pode ocorrer que informações pessoais sobre determinado indivíduo sejam acedidas por indivíduos mal-intencionadas. A título de exemplo, pode dar-se um roubo de identidade, crime que tem vindo a aumentar com o desenvolvimento das tecnologias de informação. Segundo, *informational inequality*, neste ponto o autor refere que as desigualdades podem estar relacionadas com o facto de os indivíduos não terem conhecimento do verdadeiro valor que os seus dados podem ter para o mercado. Desta forma, a cedência de informações pode significar uma maior perda para o sujeito do que um ganho adquirido ao ceder os seus dados pessoais. Terceiro, *informational injustice*, esta categoria está relacionada, de certa forma, com o princípio da limitação da finalidade. Explicando, verifica-se injustiça informacional quando os dados pessoais recolhidos dos indivíduos servem fins de processamento e análise diferentes dos que motivaram a sua recolha. O exemplo prático deste enviesamento decorre do acesso forense para fins de investigação criminal a biobancos médicos. Por último, a quarta categoria remete para *encroachment on moral autonomy*, nesta situação a falta de proteção da privacidade e, por conseguinte, das informações pessoais de um indivíduo, pode conduzir a perdas significativas na autonomia dos indivíduos que veem a sua privacidade alvo de intrusão (p. 433).

Retomando a ideia inicial desta secção, importa relevar que a privacidade deve ser perentoriamente protegida. Neste sentido existem mecanismos legais nacionais e europeus que sustentam esta convicção devendo esta ser extrapolada da sua componente individual e equacionada de igual modo na sua dimensão social. Nesta linha de pensamento, vários autores que se debruçam sobre esta temática defendem que a privacidade “is a value inherent in a liberal society” (Raab, 2015, p. 264), sendo esse o principal motivo que justifica a sua proteção contra ameaças externas. Assim, é expectável que numa sociedade liberal os indivíduos estejam sujeitos ao controlo social e a constrangimentos implementados pelo Estado. No entanto, é também esperado que estes indivíduos consigam manter as suas vidas com um grau de autonomia satisfatório que lhes permita tomar decisões e escolher os caminhos que pretendem percorrer dentro dos limites estatalmente impostos. Pensar a privacidade em termos de dignidade, remete para o respeito, termo intrinsecamente associado a aspetos da vida social, pois, quando inseridos em sociedade, os indivíduos devem gozar do respeito dos restantes membros que, em diferentes graus, partilham os mesmos ou valores semelhantes entre si (Post, 2001). Seguindo este raciocínio o autor considera que é o sucesso das normas sociais que permite que os indivíduos se encontrem integrados na sociedade, mantendo, desta forma, uma identidade coerente e consistente. Portanto, a componente social da dignidade prevê a existência de uma estrutura social onde os atores sociais se agregam com base em normas comuns assentes na interação social, sendo que “these norms constitute the decencies of civilization” (Raab, 2015, p. 293).

Movendo a discussão da tónica no indivíduo para a sociedade em geral, retém-se que a privacidade deve ser encarada como um valor individual, social e político, sendo considerada por muitos autores como a “foundation stone of political democracy and of a panoply of human or civil rights” (*idem*; consultar também Regan, 1995; Schoeman, 1992; Bygrave, 2002; Goold, 2009). Reforçando a conceção de que uma intrusão à privacidade enquanto forma de dignidade desloca este conceito para aspetos da vida social, na medida em que, citando Post (2001), “[i]nvading privacy causes injury because we are socialized to experience common norms as essential prerequisites of our own identity and self-respect (p. 2094).

Espaço público vs espaço privado

A discussão em torno do conceito de privacidade e das suas dimensões sociais deve ser ainda enquadrada no debate entre a dicotomia espaço público *versus* espaço privado. Este debate vem, de algum modo, ajudar a refletir sobre as tensões já apresentadas na representação da privacidade enquanto direito individual, mas também enquanto conceito social e necessário ao funcionamento de uma sociedade liberal. O debate aqui proposto irá ser considerado à luz do conceito de integridade contextual de Nissenbaum (2010), na medida em que se tem revelado uma ferramenta bastante útil para a avaliação da panóplia de novos sistemas tecnológicos que têm vindo a ser desenvolvidos nas esferas sociais, como na área da saúde e na área da genética forense; bem como nas práticas que afetam o fluxo de informação que essas tecnologias têm proporcionado, nomeadamente, através da prática de *Big Data*.

Em matéria de privacidade e de proteção de dados pessoais a ideia de dicotomia entre meio público e espaço privado está a tornar-se cada vez mais obsoleta. Isto porque devido às novas formas de obtenção de informação pessoal dos indivíduos por via do desenvolvimento de sistemas tecnológicos é possível uma maior vigilância e recolha de dados em grande escala. Desta forma, o melhoramento do armazenamento, processamento e análise dos dados recolhidos tem vindo, cada vez mais, a levantar questões sobre a necessidade de garantia e proteção da privacidade em público (Nissenbaum, 1997, 1998). Na mesma linha de pensamento, Gary Marx (2007) alerta que as novas tecnologias têm vindo a diluir as fronteiras entre o *self* e o *other*, bem como a separação entre o público e o privado (p. 86). Contrariando a tese de Regan (1995), onde a autora reitera que o benefício coletivo de segurança sacrifica a privacidade, sendo esta um valor caracterizado como *selfish* (*apud* Nissenbaum 2010).

A dicotomia tem sido utilizada como enquadramento teórico para a compreensão de questões sobre o direito à privacidade, essencialmente, em três pontos identificados por Nissenbaum (2010), nomeadamente, reivindicações específicas, por parte dos indivíduos, contra a intrusão da privacidade operada por atores estatais, contra a intrusão que pode ocorrer através de empresas privadas e, por fim, contra a recolha e disseminação de informações pessoais a terceiros (p. 114). No entanto, interpretar a privacidade no enquadramento público *versus* privado não abarca todas as situações em que esta pode sofrer supressões. Esta dificuldade prende-se em grande medida com as rápidas mudanças

e desenvolvimentos que têm vindo a ser operados no meio social através dos avanços nos sistemas tecnológicos. Metcalf e Crawford (2016) contribuem para esta discussão com o seu trabalho sobre a necessidade de atualizar o enquadramento ético nas investigações científicas que se servem do *Big Data* para a recolha de dados. No seu estudo é notória a tentativa de deslocar os dados publicamente acessíveis para o domínio da privacidade (p. 1). Em particular, defendem que as investigações se têm escudado do questionamento ético sobre privacidade ao utilizarem apenas dados publicamente acessíveis. Neste sentido, os autores argumentam que um dado sozinho que até então não era passível de originar a identificação do sujeito, quando conjugado com dados provenientes de outras bases de dados (mesmo que sejam públicas) pode gerar um potencial de identificação muito superior graças à recolha de informação de fontes diversificadas, característica do *Big Data*. As investigações levadas a cabo têm-se debruçado, por exemplo, no *profiling geográfico* (técnica de inferência estatística) e legitimam-se com base em argumentos presentes no discurso sobre o risco, onde os investigadores alegam que este tipo de técnicas pode ser extremamente útil na identificação precoce de terroristas (Hauge, Stevenson, Rossmo, & Le Comber, 2016, p. 5). Os autores concluem defendendo que este tipo de investigação pode apresentar sérios riscos para os direitos civis dos indivíduos e das comunidades em matéria de proteção de privacidade (*idem*, p. 2). Riscos que têm sido ignorados e contornados no debate em relação à ética dos Estudos do *Big Data*, cujos dados vertem do avanço tecnológico (*idem*).

No entanto, mesmo reconhecendo a escassez de debate e atualização do enquadramento ético para investigações que processam e analisam dados ‘públicos’ é importante compreender o contexto que tem motivado a aprovação deste tipo de investigação por parte dos comités de ética. Em particular, os *standards* da regulamentação ética estão obsoletos, pois a dualidade entre público e privado, como observam os autores, em linha com Nissenbaum (2010), já não é suficiente para inibir ou permitir uma investigação (Metcalf & Crawford, 2016, p. 2). Neste sentido, a discussão em torno do *Big Data* move o conceito de investigação ética para outras dimensões, extrapolando o plano dos danos tradicionalmente equacionados pelos comités (por exemplo, dor física), para se debruçar também em conceitos como o impacto sobre a privacidade da informação e *data discrimination*. Isto deve-se ao facto de, historicamente, existir um distanciamento entre os sujeitos em estudo e a investigação levada a cabo por campos não biomédicos (como por

exemplo, ciência computacional, estatística, matemática), ou seja, têm recorrido a um referencial ético diferente do que é seguido no campo biomédico. Uma das diferenças enunciadas é o tipo de consentimento informado que é aplicado nos dois campos, onde afirmam que as investigações não biomédicas carecem de rigor, na medida em que apresentam consentimentos com termos de difícil compreensão e políticas de privacidade demasiado vagas (*idem*, p. 2). A par do desenvolvimento das tecnologias de informação, também as tecnologias genéticas, para uso médico ou forense, têm acompanhado esse avanço. Neste caso em particular, a dicotomia entre região codificante e não-codificante do DNA está ultrapassada e o desenvolvimento das tecnologias NGS permite uma maior obtenção de informação conduzindo a discussão para a necessidade de se (re)pensar o enquadramento ético de determinadas técnicas de análise de modo a proteger do escrutínio os cidadãos que possuem os seus dados pessoais nas bases de dados.

Krista Boa (2007), apresenta um contributo para este debate, tendo como pano de fundo o avanço tecnológico e a consequente facilidade de vigilância dos cidadãos por parte da polícia, remetendo a sua análise para o conceito de expectativa razoável de privacidade (p. 330). A autora refere que o desenvolvimento tecnológico veio tornar as práticas de vigilância policial mais sofisticadas, porém considera que se deve questionar o seu carácter potencialmente invasivo para a privacidade dos indivíduos que são alvo dessa vigilância. Neste sentido, a sua questão de partida é a seguinte: “is the use of newer surveillance technologies and practices qualitatively different from what was done before, or it is a matter of law enforcement have better tools to conduct surveillance as they have always done?” (*idem*, p. 329). A delineação do que é entendido como ‘expectativa razoável de privacidade’ não tem sido consensual. Deste modo, a diversidade de entendimentos nesta matéria deve-se, essencialmente, ao facto de que o processo de determinação da expectativa razoável de privacidade é subjetivo, este depende “on a given judge’s understanding of the implications of the facts of a given case, and the relationship of those facts to his or her understanding of the nature and value of privacy” (*idem*, p. 330). Para além do seu carácter subjetivo, Elizabeth Paton-Simpson (2000) argumenta que este conceito não consegue abarcar as situações em que as invasões de privacidade ocorrem em locais tipicamente públicos, ou quando a informação é considerada pública (*apud* p. 330), reiterando que os tribunais se têm servido desta dicotomia (público/privado) como justificação para as suas decisões. Desta forma, Paton-Simpson (2000) desloca a esfera da

privacidade tradicional do âmbito local para o âmbito pessoal, ou seja, devem proteger-se as pessoas e não os locais (p. 330). Austin (2003) segue a mesma linha de pensamento e defende que “paying attention to the distinctive features of information technology can help highlight what is at stake” (p. 164). Esta estratégia vai para além de se procurar perceber onde foi a informação recolhida (público ou privado) e coloca em evidência as características da tecnologia que podem potencialmente invadir a privacidade dos cidadãos.

Face ao contexto tecnológico presente e à massiva recolha generalizada de dados pessoais sobre os cidadãos, importa realçar que estes sistemas são muitas vezes pouco transparentes (Cohen, 2000; Gandy, 1993; Lyon, 2007; Solove, 2004; Solove & Rotenberg, 2003), apresentando-se como potenciais ameaças à privacidade dos indivíduos. O escasso questionamento sobre os pontos que têm vindo a ser enunciados nesta secção podem estar relacionadas, num primeiro momento, com o facto de que ciências como a ciência computacional, a estatística e a matemática descurarem a dimensão social, ética e política dos dados que analisam, encarando-os enquanto numéricos e neutros. Esta posição não permitiu que o desenvolvimento e criação da tecnologia e dos *softwares* fosse realizado com base nos princípios de *privacy by design* (Jones & Raab, 2015; Schaar, 2010). Sendo que o seu objetivo se pauta pela avaliação de riscos previamente à conclusão do sistema, com o objetivo último de evitar consequências, como a discriminação social, para os indivíduos que estão à sua mercê. Através de um maior recurso à construção de tecnologias através dos princípios de *privacy by design* e de uma avaliação sistemática de todos os atores, tipos de informação, formas de recolha e princípios de transmissão da mesma será, em princípio, mais fácil de assegurar a proteção da privacidade dos indivíduos num contexto que vai além da dicotomia entre público e privado. Terminando-se esta secção com a tese defendida por Nissenbaum (2010) a respeito do direito à privacidade que sistematiza o debate em torno do conceito, citando:

“We have a right to privacy, but it is neither a right control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones. This is the right I have called contextual integrity, achieved through the

harmonious balance of social rules, or norms, with both local and general values, ends, and purposes” (p. 231).

1.5. Vigilância *hard* e vigilância *soft*

Vários autores defendem que o combate à criminalidade, seja na sua dimensão nacional seja na transnacional, veio mudar o paradigma das sociedades europeias. Em particular, assiste-se à transformação de sociedades tipicamente ‘disciplinares’ para sociedades de ‘segurança’ (Cunha, 2008, p. 75; Maciel & Machado, 2014, p. 141). As primeiras tinham como ambição a eliminação do crime através da disciplina dos indivíduos que cometiam práticas criminosas. As segundas têm optado por políticas neoliberais centradas na preocupação com a ‘segurança nacional’ e com a gestão do risco e da ameaça criminal pela previsão, mais do que enveredar em tentativas de procura das causas da criminalidade ou da sua erradicação (Garland, 2001; Lyon, 2014, p. 11). Seguindo este raciocínio, Lyon (2001), refere que o aumento da preocupação com questões de ‘segurança nacional’, logo o aumento da vigilância, verte, em grande medida, do crescimento de alguns tipos de criminalidade, nomeadamente o terrorismo e o roubo de identidade. Situação que, consequentemente, conduziu a um interesse gradual no desenvolvimento e aplicação de novas ‘tecnologias de vigilância’ (Bygrave, 2002; Lyon 2001). Monahan (2010) defende, nesta lógica de pensamento, que a vigilância se tornou um símbolo poderoso de segurança nacional (p. 8). Dito isto, Lyon (2001) define, genericamente, o conceito de vigilância enquanto “collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been collected” (p. 2). De modo complementar pode acrescentar-se a esta conceptualização que os aparelhos de vigilância são responsáveis pelo controlo dos indivíduos através da “identification, tracking, monitoring, or analysis of individuals, data, or systems” (Monahan, 2010, p. 8) baseando-se em categorias fixadas de forma universal (Kreissl, Norris, Krlic, Groves, & Amicelle, 2015, p. 161).

Neste contexto, os mecanismos de vigilância têm encontrado novas modalidades que tendem a distanciar-se das formas tradicionais. Sob este pano de fundo, pode entender-se que as modalidades de vigilância se encontram, ainda que genericamente, divididas em vigilância *hard* e vigilância *soft*. A primeira remete para as formas tradicionais de controlo, caracterizadas, essencialmente, pelo seu carácter invasivo, como na revista

corporal realizada por agentes policiais. A segunda distingue-se por não ser invasiva, por exemplo, a zaragatoa bucal (ou esfregaço bucal) para obtenção de DNA; pautando-se ainda pela recolha invisível de informações, como é o caso dos *softwares* de reconhecimento facial, que não exigem um contacto físico com o “corpo” vigiado (Marx, 2006, pp. 1-2). Este tipo de controlo possui a particularidade de procurar a voluntariedade dos cidadãos, muitas vezes através de narrativas sobre o bom-cidadão que tem o dever de contribuir individualmente para o bem-comum, o altruísmo, a responsabilidade social, entre outros (Machado & Silva, 2008b, p. 161; Marx, 2006, pp. 1-2, 2008, p. 95; Rose, 2008). A voluntariedade dos cidadãos nos mecanismos de vigilância levanta algumas preocupações, nomeadamente, quando se verifica a recusa na cedência de informações pessoais por parte do indivíduo vigiado. Nesta situação, a negação da participação voluntária pode gerar perdas morais para o mesmo, pois pode incorrer na pena de ser categorizado enquanto “mau” cidadão, podendo ainda verificar-se a erosão de direitos como a presunção de inocência (Kreissl et al., 2015, p. 161; Marx, 2006, p. 5) e a dúvida razoável (Lyon, 2014, p. 10). Contribuindo, deste modo, para o reforço da ideia “nothing to hide, nothing to fear” onde a “privacidade e a criminalidade são sinónimos” (Crossman, 2008, p. 116).

No entanto, se um indivíduo ceder, voluntariamente, uma amostra de DNA, não está apenas a permitir o acesso a informação pessoal, este oferece de igual modo informação sobre os seus familiares que, possivelmente, não tiveram oportunidade de dar o seu consentimento para tal (Marx, 2008, p. 90). A vigilância *soft* não tem encontrado resistência pública significativa, pois serve-se da difusão de tecnologias que são utilizadas pelos cidadãos de forma regular e diária (Monahan, 2010, p. 99, 111). A título de exemplo, telemóveis, GPS, câmaras de vídeo e outros dispositivos com capacidade de armazenamento de dados padronizados, sendo por isso necessário equacionar a invisibilidade na recolha dos dados como um tópico de interesse (*idem*). Esta característica possibilita métodos de vigia não invasivos, mas impossibilita o consentimento informado do indivíduo no que concerne à recolha dos seus dados, alterando-se, assim, o modo de criação de suspeitos de um crime (Aas, 2006, p. 148, 2013; Cole & Lynch, 2006; Lynch & McNally, 2009; Marx, 2008, p. 92).

Considerando que neste estudo a vigilância é discutida no plano da investigação criminal importa explorar, ainda que brevemente, o contributo de Williams e Johnson (2004a) sobre a observação criminal. Os autores distinguem duas categorias sobre a mesma,

respetivamente, a observação ‘preconstrutiva’ e a observação ‘reconstrutiva’ (p. 4). A primeira remete para a visibilidade do corpo, onde é possível ver/observar com exatidão os comportamentos do indivíduo que pratica atos criminosos, neste caso a vigilância CCTV é uma das tecnologias que pode ser elencada para suprir esta necessidade. A segunda remete para o que se encontra invisível aos olhos do investigador criminal. Nesta situação a investigação decorre em modo retrospectivo servindo-se da procura de impressões digitais e/ou de amostras biológicas de DNA (ou outros vestígios) com a finalidade de, como a própria designação indica, reconstruir o crime (*idem*, p. 4). Os tipos de observação criminal supramencionados operam no âmbito dos sistemas de vigilância denominados de sistema aberto de vigilância e sistema fechado de vigilância (Hindmarsh, 2010; Williams & Johnson, 2004a). O primeiro diz respeito ao tipo de investigação que não tem disponíveis gravações que possam ser pesquisadas em arquivo. Por oposição, o segundo, caracteriza-se pela disponibilidade de arquivos para pesquisa, onde as bases de dados de perfis de DNA para fins forenses se encontram inseridas (Williams & Johnson, 2004a, p. 5).

Antes de refletir sobre a vigilância apoiada nas novas tecnologias de informação deve ter-se em consideração que esta só é passível de ser expandida se responder a certos requisitos (Goos et al., 2015, p. 62). Primeiro, é necessário que existam bases de dados capazes de armazenar e que possibilitem a pesquisa de grandes quantidades de informação. Segundo, é crucial que se criem redes de partilha entre bases de dados que permitam a conexão entre arquivos diferentes. Terceiro, é essencial que se adotem medidas de standardização para classificação e identificação dos dados pessoais de modo a facilitar a coerência dos mesmos nos processos de recolha (*idem*). Neste sentido, a era digital e o desenvolvimento tecnológico vieram permitir a criação de redes de vigilância tecnológica em massa cada vez mais interoperáveis e interconectadas em torno das sociedades contemporâneas (Gilliom, 2007, p. 114). A partilha de informações pessoais sobre potenciais suspeitos de um crime, com recurso a bases de perfis de DNA para fins forenses, foi facilitada pela possibilidade do armazenamento digital dos perfis genéticos. Esta capacitação veio agilizar, mobilizar e reconfigurar o papel dos vários atores envolvidos no sistema judicial (Thorogood & Zawati, 2015, p. 690).

As mudanças tecnológicas operadas ao nível societal vieram acompanhadas de novas formas de vigilância (Poster, 1990) e de controlo de populações e indivíduos “suspeitos” (ver também Lyon, 2007 e Marx, 1988 sobre categorias de suspeição),

nomeadamente, o “policiamento preditivo” (Kreissl et al., 2015, p. 150) com recurso a tecnologias que visam controlar, prever e identificar possíveis comportamentos e atos criminosos, através da “quantificação do «perigo»” (Machado & Santos, 2016). Seguindo o pensamento de Mark Poster (1990), o desenvolvimento tecnológico permitiu a existência de “system[s] of surveillance without walls, windows, towers or guards” (p. 93) que, consequentemente, têm gerado novas formas de (bio)poder (Foucault, 1994 [1976]) que emergiu nos finais do século XVIII e inícios do século XIX. A sua principal preocupação pautase pelo corpo e a sua consequente relação com as estruturas de poder (Pugliese, 2012, p. 7). Cimentando desta forma a ideia de que o “panóptico tecnológico” não pretende atuar através da disciplina, mas antes salvaguardar o estado de segurança máxima como refere Ivone Cunha (2008, p. 71) a par da transformação societal acima referida. A utilização de videovigilância em espaços públicos e privados e a prática de *Big Data* podem ser elencados como exemplos práticos do desenvolvimento e inovação tecnológica da vigilância (Brown, 2009; Lyon, 2014, p. 1). A dimensão preditiva da vigilância como forma de salvaguarda da segurança nacional pode gerar o que Lyon (2003) denomina de discriminação digital. Este tipo de discriminação com base em dados informáticos remete para os modos como o fluxo dos dados pessoais engrenam os processos de gestão do risco. Estes processos definem, através da análise dessas informações, os indivíduos legítimos e os que apresentam riscos de comportamento desviante (*idem*, p. 81), promovendo a categorização de indivíduos enquanto suspeitos sem que estes tenham efetivamente cometido um delito.

Portanto, a prática de vigilância tem estado intrinsecamente interligada com as “subjetividades modernas” e com o desenvolvimento das tecnologias de governação (Foucault, 1977, 1991 *apud* Haggerty & Ericson, 2007, p. 4). Neste seguimento, a *dataveillance* (Garfinkel, 2000), operada através dos dados digitais recolhidos em diversas fontes (Raab, 2015, p. 261), tem permitido uma integração estrutural da vigilância nas instituições sociais das sociedades contemporâneas. Tenner (1996) e Winner (1986) alertaram que estas novas formas de operar a “nova” vigilância através da tecnologia podem conduzir à alteração das “social structures, practices, and opportunities in ways not envisioned” (*apud* Haggerty & Ericson, 2007, p. 6) pelos atores responsáveis pela sua implementação. Hoje, as instituições e outros agentes responsáveis pela vigilância têm como estratégia garantir a segurança através de modalidades de visibilidade (*idem*, p. 7), sendo que esta premissa dá azo a alterações significativas sobre a forma como os indivíduos

experimentam a sua privacidade (*idem*, p. 11). As alterações que estes autores referem têm que ver com o facto de as tecnologias serem cada vez mais intrusivas para os indivíduos, sob o pretexto de que só assim conseguem maximizar a sua eficácia (*idem*, p. 13).

As transformações operadas pelas tecnologias nas várias dimensões sociais que têm vindo a ser descritas estão em linha com uma das teses defendidas por Durkheim na sua obra “Da divisão do trabalho social” de 1893 (Durkheim, 1999). Na medida em que, como referiu, as sociedades contemporâneas estão dependentes da diferenciação entre os indivíduos, onde as tecnologias podem ser enquadradas enquanto ferramentas com capacidade para potenciar a diferenciação social. O recurso às ferramentas tecnológicas permite, com maior facilidade, agregar e colocar os indivíduos nas posições mais adequadas com base nas suas diferenças, bem como pressiona esses mesmos indivíduos a manterem-se nas categorias que lhes foram conferidas (Monahan, 2010, pp. 9-10). Ainda nesta ótica, e demonstrando a atualidade do pensamento Durkheimiano, outros autores demonstram que a identidade/especialidade de um sujeito faz parte da malha da vigilância em duas dimensões. A primeira tem que ver, parafraseando, com a monitorização e o controlo de grupo sociais já previamente formados, muitas vezes com base em critérios discriminatórios (Lyon, 2007, p. 49). A segunda remete para a criação de novas formas de identidade com base no alcance tecnológico e no consequente aumento da recolha de dados destes indivíduos (Gandy, 2007, p. 367; Haggerty & Ericson, 2007, p. 14). Os regimes modernos de vigilância tendem a reduzir os indivíduos e as suas práticas sociais a dados supostamente analisados e processados de acordo com critérios objetivos, invisibilizando a “classificação sociotécnica do mundo” (Monahan, 2010, p. 117). Portanto, regressando a Durkheim, a classificação social (*social sorting*) operada através do aparato tecnológico contemporâneo “mascara a discriminação” social, pois estes sistemas tendem a ser pensados com base na sua neutralidade e imparcialidade no que concerne às práticas sociais que daí advêm (Lyon, 2007, p. 55; Monahan, 2010, p. 10). A ideia de neutralidade tecnológica encontra-se implicitamente contrariada no pensamento de Richard Dyer (1997) onde o autor refere que entende a tecnologia consoante a sua componente técnica, que abarca os seus aspetos materiais e funcionais, mas também na sua dimensão social, condicionada pelos fatores económicos, culturais e ideológicos da mesma (p. 83).

Tendo a discriminação como pano de fundo, percebe-se que a vigilância pode ter um papel relevante no reforço das desigualdades sociais, pois os seus sistemas podem ser

aplicados de forma desproporcional consoante o grupo social de pertença dos vigiados que podem, à priori, já estar em situação de vulnerabilidade. Neste sentido, Monahan (2010) toca num ponto crucial quando se discute a temática da vigilância e do direito à privacidade e proteção de dados dos indivíduos. O autor considera que as sociedades não têm dado a atenção merecida aos problemas e desafios que os sistemas de informação podem trazer para os atores sociais, nomeadamente, o facto de estes poderem proporcionar o aumento da vulnerabilidade de certos indivíduos ou populações devido a abusos na vigilância estatal e/ou privada (*idem*, p. 60). Vigilância que com o desenvolvimento das tecnologias e sistemas de informação moveu a coerção no plano material, para o plano imaterial, sem necessidade de contacto físico, como já foi referido anteriormente (Bogard, 2007, p. 59). Neste panorama, a prática da vigilância é vista pelo Estado como um meio de obtenção de “safety, security and social order” (Goos et al., 2015, p. 52).

Sofisticação da vigilância tecnológica - tecnologias biométricas de vigilância

Uma das questões que deve ser respondida de forma a compreender as dinâmicas imprimidas pelas tecnologias de vigilância nas práticas sociais é, nomeadamente, o que é que mantém a vigilância a operar nos dias de hoje (Lawrence, 1999). Passando por perceber quais são os argumentos utilizados para legitimar a sua aplicação generalizada ao “corpo” dos cidadãos. Retomando uma ideia já referida no decurso da secção anterior, a expansão dos sistemas de vigilância encontra a sua justificação na necessidade de gestão do risco. Como refere Bogard (2007), o sucesso de um sistema de vigilância não passa apenas pela sua eficiência, está intimamente relacionado com a sua capacidade de, citando, “eliminates problems before they merge, absolutely, before they even have the chance to become problems” (p. 60). Através dos discursos que incidem sobre o risco tem-se verificado o desenvolvimento do pânico moral (Cohen, 2002; Garland, 2008; Goode & Ben-Yehuda, 1994) nas sociedades contemporâneas como resposta à possível deterioração da estrutura de valores das mesmas. A este respeito alguns autores teorizam que o medo é socialmente construído, tendo como objetivo último proporcionar um maior controlo sobre as vidas dos atores sociais, por parte dos Governos (Altheide, 2006; Amoore, 2006, 2007 *apud* Frois, 2008, p. 127).

Os processos culturais que permitem a disseminação do sentimento de insegurança encontram-se em grande medida relacionados com os vários ataques terroristas que

ocorreram na Europa entre 2004 e 2017, sendo estes a imagem da “insegurança moderna”. O pânico e insegurança gerados em torno dos atentados deve-se em grande medida ao facto de estes atos se enquadrarem fora do âmbito dos riscos calculáveis e previsíveis, logo controláveis (Monahan, 2010, p. 4). Estes atos distanciam-se desta categorização, na medida em que ocorrem, aparentemente, de modo a que não seja possível prever, nem tampouco controlar quando e onde vão acontecer, colocando-os no plano do irracional (*idem*, p. 6). A fluidez e imprevisibilidade deste tipo de crime provoca a maximização do sentimento de medo experimentado por parte dos indivíduos e das sociedades. O que, por sua vez, conduz à criação de narrativas do medo que são amplamente disseminadas pelos meios de comunicação social contagiando os indivíduos com este tipo de percepção (*idem*). Considerando que o crime é a fonte de eleição para a legitimação dos discursos sobre o risco e sobre a necessidade de aprofundar a vigilância (Kreissl et al., 2015, p. 154), os Governos têm criado uma panóplia de respostas que pretendem erradicar qualquer ato desviante, estas medidas incluem “zero-tolerance laws, private security forces, gated communities, and technological surveillance” (*idem*, p. 1).

No pacote de medidas adotado pode incluir-se a expansão das tecnologias de identificação biométrica humana, também conhecidas como biotecnologias, sendo que estas ganharam maior relevância com os ataques terroristas de 11 de setembro 2001. A ênfase no seu desenvolvimento foi de tal modo que Woodward Jr., Orleans e Higgins (2003) alegam que com o aparecimento e desenvolvimento destas biotecnologias o mundo irá transformar-se (p. xxiii). Importará, portanto, perceber quais os seus contributos para o aparelho de vigilância, de que modo se encontram relacionadas com formas de biopoder e quais as questões levantadas quanto à possível ameaça de direitos civis. A biometria tem como finalidade o estudo das características do comportamento humano, para o efeito recorre a técnicas de análise de atributos físicos e comportamentais com o objetivo de verificar a identidade dos indivíduos (Anil, Ross, & Prabhakar, 2004; Liu, 2013, p. 29). Segundo Bateman (1998) as tecnologias biométricas podem ser encaradas de acordo com três grupos genéricos. Para fins de aplicação comercial, como o controlo do acesso físico a um edifício, a segurança eletrónica de dados, o comércio eletrónico, serviços financeiros, dispositivos pessoais de segurança eletrónica, ligação de computadores em rede, entre outros. Para fins de aplicação governamental, como os sistemas de controlo de fronteiras, os passaportes biométricos, cartões de identificação nacional, cartas de condução, vigilância

em áreas públicas, entre outros. E, por fim, para fins de aplicação forense como a investigação criminal e a identificação de terroristas (Liu, 2013, p. 49). O presente estudo debruça-se exclusivamente nas aplicações governamentais e forenses.

Pugliese (2012), no seu livro, apreende as tecnologias biométricas através do conceito de ‘situated knowledges’, cunhado por Haraway (1991, p. 188), pretendendo analisar as dimensões sociais e políticas inscritas nas mesmas (Pugliese, 2012, p. 5). Prossegue argumentando que estas tecnologias são “instrumentos contemporâneos da biopolítica” (*idem*, p. 2) e, como tal, encontram-se inscritas e enquadradas nas infraestruturas das relações de poder. Podem ainda observar-se características da sociedade disciplinar na medida em que a autenticação e verificação da identidade dos indivíduos dá-se através de categorias normativas pré-definidas, como o género, a raça, a classe social, entre outros (*idem*). Nas palavras do autor estes aparelhos operam no sentido da “individuating, identifying, classifying and distributing the templates of biometrically enrolled subjects” (*idem*, p. 2) através de redes de infraestruturas políticas, legais e sociais, sendo esta a sua relação com o biopoder. Neste sentido, as biotecnologias têm-se desenvolvido a par dos restantes sistemas tecnológicos de vigilância e é necessário refletir sobre a capacidade que estas possuem para ameaçar e suprimir a autonomia e privacidade – valores democráticos – dos indivíduos (Wayman & Nuger, 2005). A reflexão deve ser empreendida sobre diversos pontos da biometria, nomeadamente, sobre a forma como as informações biométricas pessoais são “created, stored, compared, linked, and shared” (Liu, 2013, p. 36).

A biovigilância é o resultado do desenvolvimento das tecnologias biométricas aliado às práticas de vigilância, sendo que, visando a procura da diferença, esta pode incidir perigosamente em populações ou indivíduos que já se encontram em situação de vulnerabilidade. Considerando que existe o risco de se criminalizarem estas populações mesmo sem a ocorrência de um crime, com base na lógica implícita da prevenção de delitos (Pugliese, 2012, p. 81). Neste sentido, o debate em torno dos perigos da tecnologia biométrica para a privacidade e certos valores democráticos pode ser equacionado sob duas posições algo distintas. Para certos autores, como Clarke (2001), as tecnologias biométricas, entre as que fazem parte do aparelho de vigilância, apresentam-se como as que mais riscos acarretam para as liberdades dos indivíduos e das sociedades. No entanto, autores como Woodward (1997), defendem que as tecnologias biométricas podem ser encaradas como

uma solução para a salvaguarda da privacidade. Sendo que quando combinadas com técnicas criptográficas, estas podem, inclusivamente, preservar e proteger a identidade e integridade dos indivíduos (Liu, 2013, p. 5).

O debate supramencionado abarca ainda a necessidade do equilíbrio entre os direitos civis e humanos, como a privacidade e a proteção de dados, e a supressão destes mesmos direitos sob pretextos de segurança pública (Heinemann, Lemke, & Prainsack, 2012; Toom et al., 2016). Sendo que Cavoukian (2001) argumenta que o equilíbrio em discussão possui uma componente fortemente flexível e parcial, na medida em que, quando colocado sob pressão a decisão foi quase sempre no sentido de favorecer a segurança em detrimento da privacidade (p. 1). Nesta linha de pensamento, entende-se que as limitações que têm vindo a ser impostas à privacidade dos indivíduos podem conduzir ao reforço e/ou desenvolvimento de problemas/desigualdades sociais. Podem enunciar-se, segundo Liu (2013), o aumento do estigma social, da discriminação no emprego e dos obstáculos à obtenção de serviços, como seguros de saúde, entre outros (p. 64). Uma outra fragilidade que pode estar na origem de situações que degradem os direitos humanos e civis dos vigiados tem que ver com a possibilidade de ocorrer *function creep* (Dahl & Sætnan, 2009). Por outras palavras, pode verificar-se a perda de anonimidade e o uso inadequado dos dados biométricos recolhidos por estas tecnologias que, em última instância, podem ficar na posse de indivíduos ou instituições com intenções maliciosas (Liu, 2013, pp. 66, 87). A digitalização das informações e a focalização nas componentes biológicas do ser humano revelam-se outro aspeto sobre o qual se deve refletir. Isto porque a priorização dos fatores biológicos relega por completo aspetos que não são passíveis de ser medidos por estas tecnologias, como por exemplo, os traços de personalidade dos indivíduos vigiados (Feldman, 2003, p. 666). A tendência tem sido a de uma sociedade que cada vez mais reduz os seus atores sociais a uma panóplia de características biológicas e objetivas que passam a determinar a “nova” identidade com base no corpo do cidadão, excluindo muitas vezes os aspetos subjetivos do ser humano. Citando, Catarina Frois (2008):

“[o] que existe por parte dos organismos estatais e comerciais é uma cada vez maior indiferenciação da pessoa enquanto ser com laços sociais, efectivos e relacionais à medida que se dá cada vez mais primazia a uma identidade que possa ser traduzida numa linguagem composta por símbolo (...), algoritmos, que têm um determinado propósito” (p. 130).

O grande desafio apontado às tecnologias biométricas tem que ver com a perda do controlo dos dados pessoais, por parte dos indivíduos, que está diretamente relacionado com a dimensão informacional da privacidade²³ (Liu, 2013, p. 72). Tal como foi referido na secção sobre o conceito de privacidade. Esta situação prende-se com o enviesamento do princípio de finalidade na recolha de informação, pois como denota Liu (2013), o uso massivo das tecnologias biométricas potencia a recolha de dados pessoais dos indivíduos para além do necessário e relevante para os fins que motivaram a sua recolha (*idem*, p. 73). Nesta linha, a autora defende que uma das formas de evitar a recolha abusiva de dados biométricos passa pelo estabelecimento de normas legais estandardizadas que possam assegurar que a recolha de informações pessoais não sacrifica de modo desproporcionado a privacidade dos indivíduos vigiados (*idem*, p. 74). Pois, quando utilizadas num contexto público estas tecnologias tendem a operar a recolha generalizada e compulsória de informações sobre todos os indivíduos, colocando o consentimento informado do cidadão num plano inferior (*idem*, p. 105). O facto de as tecnologias biométricas também poderem usufruir da dimensão invisível na recolha de dados e de estarem sob o chapéu dos discursos de gestão do risco e do medo do terrorismo, por si só, não é explicativo da aparente falta de debate público sobre a sua eficácia. O debate a este respeito cinge-se, com frequência, a questões de privacidade e de integridade do indivíduo. Wayman (2000) avança com outro ponto que deve ser tomado em consideração quando se abarca o tema do avanço tecnológico, este relaciona-se com o facto de que os cidadãos atribuem muita credibilidade às tecnologias que vertem do avanço científico, sem que haja um grande questionamento a este respeito.

Liu (2013), no seu livro sobre bio-privacidade e a regulação da biotecnologia biométrica, aponta, como possível abordagem a esta problemática, uma solução híbrida que abarque, por um lado, uma legislação geral sobre a privacidade e, por outro lado, a criação de diretrizes mais específicas que englobem os contextos específicos em que esta pode estar ameaçada (p. 258). De modo implícito, a autora, à semelhança de Nissenbaum (2010), pretende que a privacidade e a proteção de dados sejam equacionadas à luz da integridade contextual numa situação que pode demonstrar-se como uma ameaça para os direitos civis e humanos dos cidadãos. Quanto à solução elencada por Liu (2013), pode observar-se, na

²³ Liu (2013) distingue, no seu livro, duas dimensões de privacidade, nomeadamente, privacidade física e privacidade informacional.

UE, esta tentativa de solução/alternativa no novo pacote de medidas protetoras das informações pessoais. Medidas que incluem a redação de um Regulamento de proteção de dados vinculativo para todos os Estados-Membros e a apresentação de Diretivas na mesma temática em esferas como a da investigação criminal.

1.6. Bases de dados forenses de perfis de DNA

Aprofundando a exposição desta secção ao tema em estudo, importa voltar a realçar que grande parte do desenvolvimento em matéria de biometria foi legitimado sob o pretexto de segurança nacional, segurança pública e prevenção do crime e veio suprir a necessidade de garantir maior segurança nas fronteiras e de facilitar a aplicação da lei (Hert, 2005 *apud* Liu 2013, p. 103). Dito isto, apesar das transformações sociais a que se tem assistido, a utilização de sistemas de classificação, monitorização, vigilância e disciplina de determinadas populações e indivíduos não pode ser balizada apenas no passado. Atualmente, os Governos continuam a verter da ciência sistemas mais sofisticados que permitem a continuação deste tipo de práticas numa escala até então impossível (Miranda, 2015, p. 430; Pugliese, 2012, p. 17). Citando Anthony Burke (2001), o conceito de segurança deve ser teorizado enquanto “political technology” que encerra em si um conjunto de “network of practices and techniques which produce and manipulate identities, societies, spaces and flows” (p. xxxiv).

Portanto, com o desenvolvimento de tecnologias biométricas de vigilância assiste-se à intensificação da vigilância digital do corpo dos cidadãos (Aas, 2006, p. 144) através de técnicas e procedimentos de instrumentalização (Pugliese, 2012, p. 55). Isto deve-se a novas conceções de identidade e de identificação do corpo humano que têm vindo a ser transcritas em padrões digitais processáveis num curto espaço de tempo e a uma escala global (Aas, 2006, p. 144; Campbell & Van Brakel, 2015; Pugliese, 2012, p. 55). Neste contexto, a leitura de informação biométrica do corpo – por exemplo, o perfil de DNA ou a impressão digital – é hoje uma das ferramentas tecnológicas utilizadas na identificação humana e possui infraestruturas capazes de armazenar os biodados recolhidos. A partilha transnacional de perfis genéticos (e/ou de impressões digitais) e a subsequente partilha de dados pessoais é possível devido à criação de estruturas tecnológicas que podem funcionar em rede. Sendo que a partilha transnacional das informações pessoais dos indivíduos vem

trazer visibilidade ao papel simbólico das fronteiras, que possibilitam o mapeamento dos métodos de vigilância dos vários países (Marx & Muschert, 2007, p. 381).

A utilização de informações genéticas como ferramenta de identificação de indivíduos suspeitos conduziu à criação de bases de dados forenses de perfis genéticos de DNA para fins de investigação criminal. Neste sentido, o recurso a dados pessoais para fins de investigação criminal releva o caráter crucial de estruturas que estejam preparadas para armazenar esses dados, sejam eles digitais ou biológicos. Os biobancos têm-se destacado enquanto estruturas de armazenamento de tecidos humanos, tanto para utilização médica, como criminal, sendo que estes armazenam o material biológico humano, mas também os dados relativos ao tutor dos mesmos (Machado, Alves, & Silva, 2015, p. 57). A par do exponencial aumento na recolha de informações pessoais dos indivíduos, o desenvolvimento e expansão dos biobancos deveu-se ao facto de usufruírem do “desenvolvimento da bioinformática”, de “destacarem os dados genéticos” e, por fim, por se verificar que a partilha transnacional de dados, supramencionada, tem vindo a aumentar em volume (*idem*). Neste sentido, Machado e colegas (2015) referem que as decisões do Conselho Europeu em matéria de proteção de dados têm sido interpretadas à luz dos diferentes enquadramentos legais, culturais, políticos e sociais dos Estados-Membros. A divergência interpretativa tem, citando os autores, “gerado insegurança jurídica e fragmentações na execução da proteção de dados pessoais entre diferentes países, com implicações nos níveis de confiança pública e na perceção dos riscos associados aos biobancos [e/ou bases de dados forenses]” (*idem*, p. 62). A proteção de dados e privacidade ao nível dos repositórios de material biológico humano deve ser equacionada com o objetivo último de proporcionar um enquadramento estável e coeso ao direito que os cidadãos possuem quanto à proteção e privacidade dos seus dados (*idem*, p. 62). Complementando-se pelo estímulo à confiança pública relativamente à transparência das leis e utilização de dados pessoais (European Data Protection Supervisor, 2006; Williams, Johnson, & Martin, 2004, p. 63) para fins de investigação criminal.

Relativamente às bases de dados forenses de perfis de DNA, a Interpol elenca as vantagens da sua aplicação em contexto nacional. Neste sentido, as bases de dados forenses (1) permitem encontrar conexões com casos arquivados e entre diferentes cenas de crime; (2) identificar através de *hits* delinquentes e perpetradores de crimes; (3) garantir a identificação mais rápida de ofensores, prevenindo atividades criminosas; (4) o DNA pode

oferecer pistas que ajudem na identificação de um indivíduo; (5) têm um efeito dissuasor, sendo esta premissa bastante discutida; e, (6) permitem, através de pesquisa familiar a identificação de um suspeito com base nos dados genéticos que partilha com os seus familiares biológicos (INTERPOL, 2009). Com base nestas alegações, o recurso ao DNA como ferramenta para identificação de indivíduos ‘suspeitos’ tem sido uma das tecnologias empregues na vigilância e no controlo de populações. A sua utilização tem gerado debate sobre os desafios legais e éticos que advêm da incorporação da genética forense no sistema de justiça criminal, nomeadamente, no que concerne a questões de proteção de dados e privacidade (Lazer, 2004; Liu, 2013; Pratt, Gaffney, Lovrich, & Johnson, 2006; Pugliese, 2012; Schroeder & White, 2009; Williams et al., 2004). Neste sentido, colocando em retrospectiva as questões éticas levantadas pela implementação de bases de dados forenses de DNA, identificam-se vários direitos que podem estar potencialmente ameaçados, respetivamente, o direito à integridade física e moral, à autodeterminação informacional, à privacidade familiar, à liberdade, à autonomia, ao consentimento informado, à igualdade, à dignidade humana e à presunção de inocência (Guillén, Lareu, Pestoni, Salas, & Carracedo, 2000; Hindmarsh & Prainsack, 2010; Krimsky & Simoncelli, 2011; Lazer, 2004; Machado & Silva, 2016; Machado, Silva, & Santos, 2008, pp. 135-137; McCartney, 2006a, 2006b; Toom, 2012; Van Camp & Dierickx, 2008). Os direitos enunciados podem ser limitados ou suprimidos de acordo com o princípio da proporcionalidade (Harbo, 2010; Prainsack & Aronson, 2015; Williams & Johnson, 2004a; Williams & Wienroth, 2014). A utilização do DNA tem sido legitimada por argumentos que remetem para a necessidade de assegurar o bem-coletivo e uma maior segurança, bem como pelo ideário de neutralidade onde a ciência e a tecnologia são essenciais para a “procura da verdade”, com potencial para condenar culpados e ilibar inocentes (Costa & Nunes, 2001; Heinemann et al., 2012; Lynch, Cole, McNally, & Jordan, 2008; Maciel & Machado, 2014, p. 143; Schwartz-Marín & Wade, 2015). De forma complementar, os frequentes discursos em torno de casos de sucesso, onde as tecnologias operaram um lugar de destaque na sua resolução (para exemplos de casos de sucesso ver House of Lords, 2007; McCartney et al., 2011; Prainsack & Toom, 2013) têm desempenhado um papel importante na consolidação destas mesmas tecnologias ao nível da investigação criminal.

O Tribunal Europeu dos Direitos Humanos (TEDH) tem sido chamado a intervir em processos que envolvem o não respeito pela privacidade, como é exemplo o processo de S

*and Marper vs United Kingdom*²⁴, onde na decisão constou que a retenção ilimitada de perfis de DNA não é justificável, constituindo-se como uma violação do direito à privacidade (Amankwaa, 2018; Amankwaa & McCartney, 2019; Annas, 2009; Tseloni & Pease, 2010). A par desta decisão Liu (2013) atesta ainda que a retenção de um perfil ou amostra de DNA apresenta-se como uma ameaça à privacidade de um indivíduo pelo facto de que este pode revelar relações genéticas entre indivíduos (p. 110). Neste sentido, vários autores refletem sobre a complexidade das questões éticas que devem ser (re)pensadas no que concerne à retenção de amostras biológicas humanas. Uma amostra biológica possui um potencial informativo muito mais amplo do que um perfil de DNA, pois através desta é possível obter informação que vai além da mera identificação de um indivíduo, é possível realizar análises adicionais que podem revelar informação sensível como doenças genéticas ou informação fenotípica (Annas, 2009; Dierickx, 2008; Duster, 2004, 2006; Machado, Alves & Silva, 2015, p. 69; Machado, Silva & Santos, 2008, p. 136; Maras, 2012; McCartney, 2006a, 2012; Soletto, 2014, pp. 92-94; Thorogood & Zawati, 2015, p. 695; Van Camp & Dierickx, 2008). A partilha transnacional de perfis de DNA veio agravar os receios relativos à possível perda ou supressão dos direitos enunciados (Balzacq, Bigo, Carrera, & Guild, 2006; Johnson & Williams, 2007; McCartney et al., 2010, 2011), bem como tem vindo a fazer pressão no sentido da harmonização tecnológica e científica, sendo um dos desafios a diversidade legislativa dos países da União Europeia (Prainsack, 2010, p. 22; Prainsack & Toom, 2013). Importa referir que as questões relacionadas com os direitos humanos, com os riscos éticos das bases de dados forenses de DNA e os potenciais benefícios públicos desta tecnologia têm sido encarados como um dado adquirido, carecendo de uma discussão mais ampla quanto à natureza e aos significados destas assunções (Jasanoff, 2011; Nuffield Council on Bioethics, 2007). Em particular, a natureza sensível dos dados genéticos, a perda ou uso inadequado de dados por incompetência ou corrupção das entidades responsáveis e o receio de acusações falsas (através de vestígios biológicos) (Gamero et al., 2008; Liu, 2013, p. 13; Wallace, Jackson, Gruber, & Thibedeau, 2014, p. 58). Pensando no equilíbrio entre as liberdades individuais e o interesse público são de realçar dois pontos em relação ao uso da genética forense no campo criminal (Tseloni & Pease, 2010). O primeiro tem que ver com a noção de risco-benefício do uso nacional e da partilha transnacional de dados genéticos

²⁴ Explicado em maior profundidade no capítulo empírico sobre o caso de estudo do Reino Unido.

para fins forenses. O segundo está relacionado com a anonimização do perfil de DNA quando inserido na base de dados e os seus limites, onde este deve ser separado dos dados pessoais do indivíduo.

Face à discussão no âmbito da utilização das bases de dados forenses de DNA, vários investigadores têm realizado estudos relacionados com as perspetivas de diferentes grupos sociais relevantes em relação às tecnologias de DNA. Williams e Johnson (2004b) mapearam as distintas representações sobre os desafios éticos e sociais da utilização de bases de dados de perfis de DNA de vários grupos profissionais, distinguindo três tipologias, nomeadamente, o (1) “excecionalismo genético”, que salienta a natureza sensível da informação genética e é frequente entre membros de organizações civis de proteção de direitos humanos e comissões de ética; o (2) “minimalismo genómico”, que é caracterizado por sustentar o caráter “inofensivo” da análise do DNA não-codificante, permitindo apenas a identificação dos indivíduos, e é frequente entre os peritos forenses; e o (3) “pragmatismo biométrico” onde se distinguem as diferentes fontes de obtenção do DNA e se avalia a legitimidade da extração do mesmo de acordo com distintas avaliações de integridade física por associação a diferentes partes do corpo humano, e é frequente em operadores judiciais e legisladores (Machado & Silva, 2008b, pp. 155-161; Williams & Johnson, 2004b, pp. 211-219).

No contexto português, respeitante às perspetivas do cidadão comum em relação às tecnologias de DNA enquanto mecanismo de vigilância têm-se os estudos de Machado e Silva (2014a, 2014b, 2015a, 2015b, 2016). Relativamente ao mapeamento de atitudes de profissionais e académicos da área forense e de reclusos face à tecnologia de DNA tem-se o contributo de Machado, Silva e Cunha (2012). Quanto às perspetivas de reclusos em relação às bases de dados de DNA tem-se o estudo de Machado, Santos e Silva (2011), Machado e Prainsack (2012, 2014) e Machado (2012). Numa outra investigação realizada por Machado, Martins e Matos (2013) observaram-se as representações sociais dos estudantes das Ciências Sociais e Humanas e dos estudantes das Ciências Naturais e Exatas em torno da criação e utilização de uma base de dados genéticos forense em Portugal. Outra investigação foi levada a cabo por Machado e Costa (2013) e pretendeu analisar as configurações locais das representações e usos sociais da tecnologia de DNA na investigação criminal em Portugal. As opiniões sobre a criação e a utilização das bases de dados forenses de perfis de DNA podem ser entendidas, por um lado, mediante uma noção otimista, na

medida em que se acredita que estas potenciam o combate e a prevenção da criminalidade (Gilbert, 2007), posição tendencialmente seguida por políticos e cientistas forenses (Machado, 2011; Maciel & Machado, 2014, p. 143). Por outro lado, mediante uma noção mais crítica, como tem sido, geralmente, a dos cientistas sociais, das comissões de bioética e de ONGs. As críticas levantadas têm que ver com a sobrevalorização da ciência e da tecnologia relativamente aos meios tradicionais de investigação criminal e a consequente suavização dos seus riscos (Maciel & Machado, 2014, p. 143). No entanto, é de salientar a escassez de estudos empíricos em Portugal e nos restantes países sobre as questões de privacidade que podem ser suscitadas não só pela criação de bases de dados forenses nacionais, como também pela partilha transnacional de informação genética. Sendo este o contributo que o presente estudo pretende facultar.

1.7. Estandardização, proteção de dados e privacidade

A estandardização e os *standards*, tal como a tecnologia, fazem parte da vida moderna, sendo essenciais nas operações de diversas tecnologias de vigilância. O processo de estandardização torna o mundo “equivalente entre culturas, tempo e espaço” (Bowker & Star, 1999) através da construção de regras uniformizadas. Os *standards* permitem agregar diferentes comunidades e diferentes práticas numa rede comum, tornando possível que estas funcionem em conjunto, ainda que estejam separadas pela distância e pela heterogeneidade de atores (Bowker & Star, 1999; Timmermans & Epstein, 2010, p. 71).

O Tratado de Prüm, ao implementar no Espaço da União Europeia a partilha transnacional, automatizada, de perfis genéticos, apoia-se na ideia de harmonização e estandardização técnico-científica neutralizando, deste modo, as diferenças legais, culturais e políticas entre os diferentes países (Lampland & Star, 2009, pp. 4-5; Prainsack & Toom, 2010, 2013). A partilha e a circulação de dados no contexto do sistema Prüm deve-se também à criação de *standards* que visam garantir a interoperabilidade (Balzacq et al., 2006; Bigo, 2008, p. 105; De Hert & Gutwirth, 2006; McCartney 2014a, 2014b) tecnológica das bases de dados dos países signatários. Concretamente, a harmonização da cooperação policial e judiciária no sistema Prüm tem-se deparado com divergências nas práticas dos países da União Europeia. A título de exemplo, ao nível dos dados pessoais que são partilhados no step 2 e da custódia das bases de dados forenses de DNA. Sendo que estas

bases de dados forenses podem encontrar-se sobre a alçada do Ministério da Justiça ou do Ministério do Interior.

Todo o processo de criação de *standards* significa, segundo Lampland e Star (2009), “*codify, embody, or prescribe ethics and values*” (pp. 4-5), que suporta uma componente fortemente normativa permitindo e justificando a necessidade de correção dos indivíduos considerados desviantes (Gilbert, 2007). Do mesmo modo, os *standards* de privacidade são definidos num mínimo exigível a partir do *standard* do homem médio. Neste estudo pretende-se desconstruir a caixa negra da privacidade de forma a apreender a performatividade da proteção de dados (Barad, 2003; Law, 2008; Tsekeris, 2007) nas várias redes em que circula. Almeja-se, ainda, compreender de que forma a não conformidade com outros *standards* prevalecentes, por exemplo, de conduta, expressão cultural ou pertença étnica, podem resultar na supressão de *standards* de privacidade. A estandardização mais do que uma homogeneização pode significar modalidades heterogêneas de (d)estandardização da privacidade. Neste trabalho, um dos objetivos consiste em compreender os modos de apropriação local/nacional dos *standards* de proteção de dados definidos e regulados por instâncias da União Europeia.

(D)estandardização dos standards

O mundo é hoje um ambiente vincado pelo seu carácter transnacional e, para tal, recorre a processos de estandardização de vários produtos e certificados. A amplitude e o âmbito da regulação e da governação está a aumentar exponencialmente e estende-se por vários setores e atividades (Djelic & Sahlin-Andersson, 2006; Hallström & Boström, 2010; Timmermans & Epstein, 2010), por exemplo, na área da tecnologia, mais concretamente, nas tecnologias de vigilância. Neste panorama, a governação contemporânea caracteriza-se pela proliferação de regulações e pela sua articulação com atividades de monitorização e de organização (Djelic e Sahlin-Andersson, 2006, p. 1). A governação nestes trâmites vem reiterar a ideia de que as fronteiras físicas de um país não se circunscrevem necessariamente às fronteiras regulatórias, citando, “[n]ational regulatory patterns can quickly get transnationalized and transnational initiatives are having a local impact” (*idem*, p. 2). Neste contexto, é possível que o Estado tenha as suas ações limitadas, pois as interações entre os diversos atores que intervêm direta ou indiretamente em atividades de

governança e de regulação entendem-se bastante complexas e multidirecionais, sendo que a separação entre o setor público e privado é cada vez mais fluída (*idem*, p. 2; Marx, 2007).

À luz da corrente neo-institucionalista, os processos de standardização são entendidos enquanto ferramenta essencial à configuração de regras/normas, bem como à sua adoção por parte dos indivíduos que são afetados pelos mesmos. Noutra linha de pensamento, o interacionismo simbólico coloca a standardização no plano da categorização e classificação através da naturalização desses processos tornando os *standards* invisíveis, sendo esta característica a que lhes confere poder no meio social. Timmermans e Epstein (2010), refletem sobre *standards* e a standardização com recurso ao referencial teórico do interacionismo simbólico, tendo como objetivo a análise e a compreensão tanto das consequências positivas como negativas que advêm da adoção destes processos para a vida social dos indivíduos. Neste sentido, apesar do desenvolvimento de trabalhos sociológicos sobre os processos de standardização, os aspetos relacionados com a modernidade cada vez mais imprimida na standardização carecem de atenção. Esta premissa é concretizada com a ideia de que a gestão da vida na modernidade se caracteriza pela crescente “creation, institutionalization, use and dissemination of diverse kinds of standards” (*idem*, p. 70).

A fixação de uma regra enquanto *standard* permite que os atores envolvidos usufruam dos benefícios que a harmonização lhes confere (Botzem & Dobusch, 2012, p. 23). No entanto, é necessário compreender a falsa neutralidade que tende a revestir os discursos em torno destes processos que têm vindo a ser encarados como não sendo inerentemente bons ou maus (Timmermans & Epstein, 2010, p. 70). A retórica do argumento da neutralidade relega para um plano inferior o possível enviesamento das práticas quando se utiliza determinado *standard* em determinada circunstância, consequência das relações de poder existentes na standardização. Por outras palavras, confrontar os atores com os possíveis enviesamentos e constrangimentos que têm origem a montante da sua difusão (Botzem & Dobusch, 2012, p. 23) permite dar conta das mudanças que podem ocorrer durante o processo de standardização. Esta estratégia possibilita a identificação dos atores relevantes e o modo como estes contribuem para as transferências de poder (*idem*). Em última instância, estas práticas podem apresentar-se nocivas para o exercício da democracia. Timmermans e Epstein (2010) avançam com um conjunto de questões estratégicas que podem ajudar a mitigar o enviesamento que pode decorrer do

processo de criação de um *standard*, respetivamente, 1) “[h]ow do we hold the standard makers accountable?”; 2) “Whose benefits are served by standards?”; 3) “When standards conflict, which ones should prevail?” (*idem*, p. 70).

Rose e Miller (1992) consideram que para enquadrar os *standards* no âmbito da governação é necessário que estes sejam responsivos e passíveis de serem corrigidos. Nesta linha, Brunsson e Jacobsson (2005) reforçam o papel dos *standards* na construção de uma ‘forma de regulação social’ que pode atuar enquanto substituta de uma opção mais autoritária (p. 12). Já no patamar da transnacionalidade, permite que se “encourage actors to behave in a similar fashion, producing uniformity across time and space” (*idem*, p. 14; ver também Ahrne & Brunsson, 2006). Seguindo o mesmo vetor, Kerwer (2005) realça que estes possuem implicitamente um carácter voluntário que está imprimido na escolha pelas melhores práticas (p. 611). No entanto, Botzem e Dobusch (2012) alertam para o facto de que a voluntariedade que lhes é característica poder ser contornada por terceiros, na medida em que os indivíduos podem ser compelidos a cumprir um *standard* por falta de opção que satisfaça as suas necessidades, tornando-se num custo agravado para o próprio (p. 5). Raymond Williams (1983) teoriza o *standard* numa linha mais otimista, pois considera que este é visto como uma meta desejável a alcançar por parte dos atores sociais, nas suas palavras, um *standard* é uma “source of authority” e um “level of achievement” (*idem*, pp. 296-299). Timmermans e Epstein (2010) contribuem para a sua caracterização avançando com quatro categorias que podem ser úteis para uma análise mais detalhada dos mesmos. Realce-se, no entanto, que a tipificação apresentada não deve ser entendida de forma rígida e estanque. Portanto, têm-se os *design standards* (especificações estruturais), os *terminological standards* (estabilidade de conceitos), os *performance standards* (especificações dos resultados) e os *procedural standards* (como devem ser performados os processos) (*idem*, p. 72). Os *standards* são, metaforicamente, o cimento que permite que diferentes métricas e práticas consigam ser interoperáveis entre si, acrescentando-se o facto de permitirem a possibilidade do trabalho em rede a grandes distâncias, característico da vida moderna (*idem*, p. 71).

Os *standards* encontram-se interrelacionados com outros *standards* (Lampland & Star, 2009), podendo ser representados visualmente como uma teia (ou rede) que depende de todos os pontos para se manter estável. Estes, por sua vez, são distribuídos de forma desigual nas várias esferas da sociedade, pois a sua criação pressupõe que estejam

embebidos na ética e em valores que afetam de forma diferente os diferentes atores sociais das diferentes classes sociais (Timmermans & Epstein, 2010, p. 71). A distribuição assimétrica de poderes na sua criação pode encontrar a sua retórica na própria forma de categorizar os grupos de atores sociais. Por outras palavras, a construção destas categorias pode beneficiar certos indivíduos em detrimento dos restantes o que conduz a impactos diferenciados no grau de agência que estes possuem nos processos de standardização (Hallström e Boström, 2010, p. 118, 138). Reforçando que a categorização do mundo social não é neutra, pelo contrário, tem origem num conjunto variado de circunstâncias históricas e contextos sociais (Hacking, 1999).

Os processos de standardização (transnacional) podem ser definidos enquanto “process[es] in which the formation of standards and their subsequent diffusion are shaped by actors and closely interrelated” (Botzem e Dobusch, 2012, p. 2). O carácter transnacional destes processos remete para a criação de normas ao nível das fronteiras nacionais que produzem efeito num espaço não materializado geograficamente, sendo que estas regras são desenhadas por uma panóplia de atores estatais e não estatais (Böstrom & Garsten, 2008; Djelic & Sahlin-Andersson, 2006; Mason, 2005; Rosenau, 2003). Neste tipo de teorização pretende-se enfatizar o papel do ator que se encontra inserido numa rede e que contribui para a ordem social, mas que se encontra fora da malha organizacional. Pretende-se também dar conta da relevância que os recursos específicos possuem em determinadas circunstâncias. Na dimensão transnacional da formação de *standards* também se verifica o acesso desigual a recursos económicos, sociais e políticos, pelo que nem todos os atores sociais conseguem aceder a oportunidades de participação nos processos de formação de *standards* (Schmidt & Werle, 1998; Cochoy, 2004; Hallström, 2004; Werle & Iversen, 2006). Nesta linha de pensamento, Smith (2005) refere que no plano transnacional é necessária uma maior alocação de recursos, por parte dos atores e das organizações do que na dimensão nacional (*idem*, p. 235; Smith, 2008). Depreende-se que as oportunidades de participação dos atores sociais na construção de *standards* encontram-se condicionadas pela distribuição assimétrica do poder pelos vários grupos sociais. Este constrangimento afeta o acesso aos recursos disponíveis e, conseqüentemente, afeta também a própria eficácia das estruturas organizacionais erigidas em torno de poderes desiguais (Hallström & Boström, 2010, p. 81; Kekk & Sikkink, 1998; Scholte, 2005; Smith, 2005)

Bowker e Star (1999), discernem um sentido mais neutro para os processos de standardização, estes são entendidos como processos que tornam o “modern world equivalent across cultures, time, and geography” (Timmermans & Epstein, 2010, p. 70) através da construção de regras uniformizadas e globalmente reconhecidas. Dito isto, analisar um *standard* ou um processo de standardização passa por compreender a sua natureza dual, em última instância dicotômica, pois este pode permitir e/ou constranger as interações sociais concomitantemente. Portanto, o seu processo de criação passa por limitar de alguma forma a escolha dos indivíduos, pelo que se torna pertinente pensar na participação dos *stakeholders* e na relevância da negociação destas regras (Botzem & Dobusch, 2012, p. 5).

A globalização e a modernização abarcam implícita e explicitamente processos de criação de *standards*. A aparente inércia na reflexão sobre os processos de standardização pode encontrar justificação numa das dimensões do *standard*, nomeadamente, a da invisibilidade, pois este é encarado enquanto uma “infraestrutura técnica e moral da modernidade” (Lampland & Star, 2009, p. 11). Um *standard* só é equacionado enquanto regra, ainda que goze de maior voluntariedade do que as regras formais (Brunsson & Jacobson, 2005, p. 36), quando um indivíduo tenta, de algum modo, ignorá-lo, contrariá-lo ou modificá-lo, sendo que este comportamento pode representar custos demasiado elevados para o indivíduo em particular (Thévenot, 2009, p. 795). Os processos associados à standardização ocupam um papel relevante na cimentação da autoridade simbólica de várias instituições ou modos de agir, a título de exemplo, os cientistas reafirmam a sua legitimidade e autoridade através de *standards* que os próprios criaram ou participaram na sua criação (Porter, 1995; Shapin & Shaffer, 1985). No entanto, certas organizações transnacionais de criação de *standards* têm muita dificuldade em demonstrar o seu poder simbólico, situação que pode colocar em causa a existência da própria infraestrutura (Hallström e Boström, 2010, p. 83).

A coordenação da vida social pelo Estado tem sido influenciada pelos *standards* e os seus respetivos processos de criação como tem vindo a ser descrito. A globalização, principalmente a que tem ocorrido ao nível económico, contribuiu e continua a contribuir em larga medida para a mudança dos papéis desempenhados pelas organizações transnacionais de standardização. Estas são responsáveis pela diluição das fronteiras nacionais, bem como do próprio estado regulatório (*idem*, p. 1). Seguindo a mesma retórica,

Beck (2005) argumenta que, de forma semelhante, também a política se deparou com novos cenários de governação, citando, “politics is no longer subject to the same boundaries as before, and it is no longer tied solely to state actors and institutions. The result being that additional players, new roles, new resources, unfamiliar rules and new contradictions and conflicts appear on the scene” (pp. 3-4).

Um dos aspetos relevantes a ser elencado na utilização dos *standards* tem que ver com o facto de os seus processos de criação serem, geralmente, mais transparentes permitindo uma maior capacidade de prestação de contas por parte dos órgãos institucionais dos Governos (Timmermans & Epstein, 2010, p. 82). Portanto, para avaliar e analisar as consequências dos processos de estandardização e dos *standards* deve ter-se em consideração diversos aspetos. Primeiro, os *standards* e os processos a eles subjacentes permitem uma maior coordenação e coerência no meio social e transnacional (Botzem & Dobusch, 2012, p. 1), na medida em que operam enquanto tradutores de práticas e símbolos entre sistemas *a priori* incompatíveis. Sendo que podem ainda “create specific kinds of mobility, uniformity, precision, objectivity, universality, and calculability” (Timmermans & Epstein, 2010, p. 83). Segundo, apesar de os *standards* serem enquadrados no plano da voluntariedade, os processos de estandardização implicam necessariamente a visibilidade de certas características (ou valores e grupos sociais) em detrimento de outras remetendo-as para a dimensão do invisível, podendo mesmo conduzir a processos de exclusão e discriminação social (Baines, 2006; Bowker & Star 1999). Terceiro, apesar de serem considerados regulação *soft* são acompanhados por mecanismos de coerção para o seu cumprimento, no caso de serem universais pode verificar-se a deterioração de certos *standards* locais/nacionais em prol da sua transnacionalidade (Timmermans & Epstein, 2010, p. 83). Ou seja, o plano local que recebe o *standard* numa relação de simbiose perde e recebe determinadas características durante o seu processo de implementação. Neste sentido, ao nível nacional pode verificar-se uma pressão para o seguimento de convenções e acordos transnacionais sob o argumento de que todos os países devem seguir as mesmas diretrizes em determinado assunto (Hallström & Boström, 2010, p. 3).

Através da noção de ‘viagem de ideias’ enquanto processo social ativo de tradução entre mundos compreende-se que estas ‘ideias’ (ou *standards*) são escolhidas pelos diversos atores que, por sua vez, as transmitem a outros atores contribuindo para a sua disseminação e utilização (Djelic & Sahlin-Andersson, 2006, p. 20). No entanto, não são

necessariamente as características de uma ideia (ou *standard*) que a torna adequada para ser utilizada pelo resto da rede, mas antes os atores e o seu poder/autoridade na rede que as tornam a norma a ser seguida (Czarniawska & Sevón, 1996; Hallström & Boström, 2010, p. 11; Røvik, 2002; Tolbert & Zucker, 1983), como já foi explorado. Neste sentido, assumir que um *standard* possui *a priori* um carácter neutro pode acarretar várias consequências para os seus utilizadores. Os seus processos de criação, difusão e implementação podem ter origem em processos políticos enviesados, citando, “standards’ objectivity, universality, and optimality are hard won victories that can be heavily contested by third parties lobbying accusations of bias and politicization” (Timmermans & Epstein, 2010, p. 74).

Outro aspeto a ser desconstruído tem que ver com a elevada tendência em se associar a estandardização à homogeneização massiva da sociedade e da vida moderna. A visão holística deste tipo de concepções sobre a estandardização relega para um patamar inferior a influência das contingências locais nos processos de estandardização, sejam elas económicas, sociais ou culturais (*idem*), o que pode enviesar a reflexão sobre o tema. Vários autores defendem que o aumento da estandardização encontra-se intimamente relacionada com o aumento da globalização nas sociedades contemporâneas (Brunsson & Jacobson 2005; Krislov, 1997; Hallström 2004). Nesta linha de pensamento, a definição de nichos de estandardização pode ser uma das estratégias a adotar para a compreensão das consequências que decorrem da adoção de determinado *standard*, sendo que só com a lente das ‘contingências históricas’ é possível percecionar os seus contextos de criação, seja ele de carácter conservador ou inovador (Timmermans & Epstein, 2010, p. 75).

A estandardização encontra-se também associada ao capitalismo e à industrialização, no entanto, está presente nas mais variadas esferas da sociedade, como por exemplo, nos tribunais. Neste tipo de instituições para além da estandardização de instrumentos, como os formulários, assiste-se também à estandardização do comportamento humano (*idem*, p. 76). Este tipo de prática pode, num momento inicial, reproduzir e perpetuar situações de exclusão e estratificação social em populações mais vulneráveis. Pois, ainda que a criação de *standards* pretenda ser do interesse do público, os indivíduos que irão ser diretamente afetados pelos mesmos nem sempre se encontram representados no seu processo de criação. Neste sentido, existem grupos de ativistas e movimentos anti estandardização que se propõem a debater e a desconstruir a invisibilidade de poderes nos processos de criação e implementação dos *standards* através

de pressões políticas (Czerniawski, 2007; Epstein, 2007, 2009; Igo, 2007; Lengwiler, 2009). A título de exemplo, ao nível de tecnologias controversas de análise de DNA e ao nível da estandardização do comportamento humano. Os movimentos e as discussões geradas pelos grupos supramencionados têm sido de particular relevância, pois permitem ajustar os processos de estandardização a vários contextos, deixando de parte o ideário de *standard* humano, para equacionar a estandardização do comportamento à luz do nicho de estandardização, ou seja, da criação de subtipos de um *standard* humano. Os nichos de estandardização são entendidos como, citando, “a way of transforming human populations into standardized objects available for (...) purposes that eschews both universalism and individualism and instead standardizes at the level of the social group (...). In place of a standard human, niche standardization substitutes an intersecting set of standard human subtypes” (Epstein, 2007, pp. 135–54).

O processo de estandardização e, em particular, a implementação de *standards*, encontra-se condicionado pela existência de infraestruturas físicas e culturais que permitam a sua aceitação generalizada. Nesta linha, também a implementação internacional de um *standard* pode ser alvo de vários obstáculos, na medida em que no plano local/nacional podem observar-se diferentes práticas, ferramentas e legislações. Desta premissa decorre a importância da dimensão flexível de um *standard* que vem permitir a compatibilidade entre contextos dissemelhantes (Timmermans & Berg, 1997). Pode entender-se com os contributos de Latour (1988) e de O’Connell (1993) que a universalidade dos *standards* é operada através de uma “rede massiva (a sociedade) de circulação de medidas” (Timmermans & Epstein, 2010, p. 80). Ainda a este respeito, mesmo quando um *standard* se encontra já determinado, quer na sua dimensão rígida quer global, permanece sempre incompleto (*idem*, p. 81), esta condição está diretamente relacionada com a sua adaptação às diferentes epistemologias locais/nacionais.

Os *standards* encontram-se, por um lado, como já foi referido, amplamente disseminados nas diversas esferas da vida social dos indivíduos. Por outro lado, são muito “voláteis e contestados”, dependendo de um conjunto de condições específicas e favoráveis para serem enquadrados no plano das regras autoritárias (Botzem & Dobusch, 2012, p. 2). Portanto, depreende-se que o carácter flexível do *standard* é a característica que permite sustentar o funcionamento dos processos de estandardização ao nível transnacional. Recorrendo ao Sistema Prüm como exemplo, percebe-se que todo o processo de partilha de

dados pessoais genéticos se baseia tanto em regras rígidas, como os formulários que são preenchidos ou os procedimentos de comparação de perfis de DNA, como em regras mais flexíveis, como se observa, particularmente, no passo dois (*step 2*) que está inteiramente dependente da interpretação da legislação dos países envolvidos. Dito isto, uma das formas de garantir a continuação de um processo de standardização pauta-se por encontrar o equilíbrio entre a rigidez e a flexibilidade de um *standard*, de modo a permitir, em simultâneo, a sua adaptação aos vários contextos sociais e às suas especificações (Timmermans & Epstein, 2010, p. 81).

Num plano mais abrangente, o estudo multidisciplinar dos processos de standardização permite apreender um outro aspeto fundamental à coordenação de espaços e pessoas. Estudar os *standards* e os processos de standardização que lhes são inerentes vem tornar visíveis os formatos de ordem transnacional e os seus impactos gerados sem a existência da figura de uma autoridade pública (Cutler, Haufler, & Porter, 1999; Hall, Rodney & Biersteker, 2002; Djelic & Sahlin-Andersson, 2006; Pattberg, 2007; Higgott, Underhill, & Bieler, 2000). Rosenau (2003) dá conta das diferentes fontes de obtenção de poder num contexto de fronteiras diluídas e ‘novas autoridades’, sendo relevante equacionar os acordos bilaterais e os arranjos híbridos entre entidades estatais e não estatais. Neste sentido, Hallström e Boström (2010) argumentam que os novos cenários regulatórios da standardização transnacional definidos apenas por organizações não estatais podem enfrentar maiores dificuldades ao nível estrutural (p. 23), na medida em que a governação está sempre dependente do seu grau de legitimidade (Weber 1919/1977 apud Hallström & Boström, 2010).

Um outro aspeto que deve ser equacionado é o facto de que a criação de um *standard* não se cinge exclusivamente à sequenciação linear de fases, característica que nem sempre se encontra explícita nos contributos ao tema. Por outras palavras, devem entender-se os seus mecanismos de criação e de difusão à luz dos ciclos recursivos de standardização transnacional, onde estes se encontram interligados e se reforçam mutuamente (Botzem & Dobusch, 2012, p. 3). Citando, “[i]n such cycles, different actors may be involved in different phases, or the same actors may contribute to several phases of standardization” (*idem*, p. 9). Aliado ao hibridismo característico da implementação e difusão de um *standard*, ou seja, ao equilíbrio entre caráter flexível e rígido, também a legitimidade

influencia diretamente o sucesso da sua implementação ao nível transnacional (Hallström & Boström, 2010; Mayntz, 2010; Quack, 2010).

No contexto transnacional, como já foi referido, os *standards* atuam na ausência de organizações formais, relevando-se o papel desempenhado pelos atores nas várias esferas sociais não-estatais. No entanto, a sua criação pode, e costuma, estar associada a um certo grau de autoridade pública, na medida em que é este envolvimento que lhe confere um certo grau de legitimação aquando da sua criação, implementação e difusão (Botzem & Dobusch, 2012, p. 4). Portanto, no que concerne à legitimidade dos *standards*, têm-se, por um lado, as correntes funcionais que se focam nos efeitos da coordenação dos *standards*, onde estes são encarados como uma ferramenta para resolver problemas. As críticas às correntes funcionais passam pela constatação de que estas relegam para segundo plano os “aspectos culturais e organizacionais da estandardização”, não conseguindo captar a multiplicidade de contextos e de diferenças de poder na construção e difusão dos *standards* (*idem*, p. 6). Por outro lado, têm-se as perspetivas sociais que se debruçam na sua criação e normatividade, neste caso, os *standards* são entendidos enquanto “negociações sociais” (*idem*).

À semelhança do que se verifica no plano nacional, a ordem social no panorama transnacional encontra-se de certo modo dependente do sucesso e da legitimidade do processo de estandardização, na medida em que é necessário preencher o vazio regulatório presente neste contexto. Torna-se crucial que os *standards* correspondam a regras justas, necessárias e proporcionais às necessidades das sociedades em que atuam, de outra forma a sua autoridade será questionada e todo o processo de difusão pode ser colocado em causa (Botzem & Dobusch, 2012, p. 7). Uma das formas de reforçar a legitimidade de uma entidade transnacional não estatal pode passar pela criação de “systems of accountability and effective governance mechanisms” (Waddell & Khagram, 2007, p. 281). Dito isto, verifica-se a existência da *input legitimacy* quando os indivíduos que são afetados pelos *standards* contribuem para a sua construção de modo a terem os seus interesses representados no processo (Hallström & Boström, 2010, p. 140; Mayntz, 2010, p. 10). A *procedural legitimacy* que remete para questões relacionadas com uma maior transparência de procedimentos, tomadas de decisão e participação dos vários grupos sociais (Hallström & Boström, 2010, p. 25). Por fim, assiste-se à *output legitimacy* quando esta advém de decisões racionais de terceiros que visam a resolução objetiva de um problema técnico

tendo em vista a minimização dos custos de transação (*idem*, p. 140; Mayntz, 2010, p. 10), bem como a estabilidade do *standard* a longo prazo. Mais uma vez, os tipos de legitimidade supramencionados não são estanques nos seus limites, pelo que existem em complementaridade no seu processo de criação, sendo que os conflitos que podem advir desta formulação passam pelas relações de poder entre atores e pela disponibilidade de recursos (Botzem & Dobusch, 2012, p. 8).

Neste sentido, denotam-se três dimensões na criação de *standards*, nomeadamente, (1) a distinção entre a sua formação inclusiva e exclusiva; (2) a sua difusão; e (3) a distinção entre os quatro ideal-tipos de *standards*. Relativamente à primeira dimensão, na formação exclusiva, como o próprio nome indica, o *standard* é desenvolvido por uma única entidade; já na formação inclusiva observa-se maior abertura para um processo de negociação entre os vários atores envolvidos na sua criação (*input legitimacy*) (*idem*, p. 9). A segunda dimensão remete para a importância da disseminação das regras enquanto garante da aceitação do *standard* a longo prazo, onde um elevado grau de aceitação do mesmo gera *output legitimacy*, citando, “[h]igh adoption rates increase the coordination power of standards, which lies at the heart of output legitimacy” (*idem*, p. 10). Clarifique-se que quando um *standard* é sujeito às condições locais do meio em que é transposto, retorna novamente à fase de (re)formação onde é “adaptado, reformulado e reinterpretado”, também aqui ocorre uma nova redistribuição de poder entre os atores (*idem*). Por fim, na terceira dimensão, têm-se os (1) *competing standards* que se caracterizam pela mútua incompatibilidade, onde um tem de dominar sobre o outro; os (2) *de-facto standards* que são amplamente aceites e adotados pelos atores; os (3) *coexisting standards* que remetem para um conjunto de *standards* que coexistem, pelo que não lutam pelo domínio; e os (4) *collective standards* onde constam os que são criados de forma inclusiva e, como tal, largamente adotados. Realçando-se que um mesmo *standard* pode migrar entre categorias consoante o contexto e a fase em que se encontra (*idem*, pp. 10-11).

A *output legitimacy* pode, até certo grau, substituir a *input legitimacy*, na medida em que o conhecimento dos especialistas tem vindo a ganhar relevância em detrimento da prestação de contas democrática. Realce-se, uma vez mais, que a “standard diffusion causes changes in the power distribution between standard adopters and standard developers” (*idem*, p. 25). Neste sentido, os ciclos de estandardização transnacional permitem observar a existência de uma relação de mutualidade entre os diferentes tipos de legitimidade e

efeitos de distribuição entre os atores envolvidos (*idem*, p. 26). Num primeiro plano, tem-se que a legitimação através da participação de vários atores na sua formação é importante para a adoção alargada dos *standards*. Porém, a inclusividade pode condicionar os consensos quanto à elaboração das normas e prescrições (*idem*). Desta forma, as taxas de adoção de um *standard* são também um fator importante de legitimidade (*output legitimacy*) para perpetuar a ordem social (*idem*). Dito isto, as redes responsáveis pela disseminação dos *standards* podem ser pensadas enquanto ferramentas de governação que vão “além do Estado” (*idem*, p. 27), onde a participação de *stakeholders* é um dos elementos chave para a obtenção de *input legitimacy*, na medida em que vem permitir uma maior transparência e prestação de contas ao público.

A procura pela estabilização da legitimidade de uma organização de standardização não é uma atividade balizada no tempo (Hallström & Boström, 2010, p. 160). Pelo contrário, estas organizações encaram a legitimidade como um conceito relacional, na medida em que, têm de estar em constante (re)construção da mesma. Por outras palavras, as organizações transnacionais de standardização encontram-se em permanente negociação com os grupos sociais que podem demonstrar diferentes interpretações dos *standards*. Hallström e Boström (2010) enunciam no seu livro, sete estratégias que as organizações desenvolveram para alcançar legitimidade junto dos atores sociais (p. 141). (1) Criação de categorias sociais representativamente equilibradas. (2) Inclusão de *stakeholders* nessas mesmas categorias. (3) Referência recorrente a conhecimento especializado. (4) Transparência e prestação de contas dos vários processos. (5) Procura de vocabulário compreensível para permitir uma participação efetiva. (6) Procura de tomada de decisões através de consenso entre os membros. (7) Equilíbrio entre os impactos do mercado e a necessidade de auditorias rigorosas aos *standards*.

Um dos obstáculos encontrados na prossecução de estudos aprofundados sobre a (re)organização das regulações ao nível transnacional tem que ver com o facto de os campos teóricos se encontrarem desadequados ao contexto atual. Esta desadequação teórica tem que ver com o facto de que as teorias utilizadas para compreender a criação, implementação e difusão de *standards*, bem como a sua monitorização se basearem em sistemas westfalianos que tendem a colocar a regulação transnacional em segundo plano (Cutler, 2002; Kobrin, 2002). Importa também referir que o entendimento sobre o que é a soberania de um Estado, bem como quais as estruturas preferenciais para o

desenvolvimento de uma organização correspondem, grosso modo, ao discurso dominante apresentado pelos modelos de governação ocidentais (Meyer & Jepperson, 2000, p. 106). Sob este pano de fundo urge criar e adaptar os instrumentos analíticos de modo a que seja possível enquadrar a regulação enquanto complexa, multidimensional e composta por uma panóplia de atividades que fazem a ponte entre o contexto global e o local. Neste domínio, certas atividades podem desenrolar-se em simultâneo “dentro, entre e através das fronteiras nacionais” (Djelic e Sahlin-Andersson, 2006, p. 3). Neste sentido, o enquadramento teórico da teoria de campo deve permitir a compreensão das dimensões macro, meso e micro dos processos institucionais presentes na governação transnacional (*idem*, p. 23). Lewin (1951) define campo (*field*) como “totality of coexisting facts which are conceived of as mutually interdependent” (*idem*, p. 240).

Na mesma linha, Bourdieu (1977, 1984) considera que os campos se apoiam em crenças comuns entre os atores, onde a coerência e a conformidade são desenvolvidas através de padrões de ação e significados que perduram no tempo e no espaço. No entanto, ressalve-se que nestes ‘campos’ dá-se a luta por recursos, relações e posições centrais que oferecem um papel dominante de alguns atores sobre os restantes. Como resposta às lacunas das correntes neo-institucionalistas e institucionalistas, nomeadamente, na apreensão de todas as dimensões espaciais e relacionais da construção de novas estruturas e atividades, Djelic e Sahlin-Andersson (2006) avançam com uma definição da noção de ‘campos’. Citando, “we understand fields as complex combinations of spatial and relational topographies with powerful structuring forces in the form of cultural frames or patterns of meaning” (*idem*, p. 27), integrando neste conceito três dimensões, nomeadamente, a espacial, a relacional e a de significação (Böstrom & Klintman, 2008).

Desta forma, pretende-se observar a governação transnacional através de lentes mais precisas, pois as topografias espaciais tradicionais entre local, nacional e transnacional estão cada vez mais ultrapassadas e diluídas (Djelic & Sahlin-Andersson, 2006, p. 27). Neste sentido, a governação é apresentada sob a ótica de uma topografia relacional sendo que as redes se conectam com indivíduos, organizações, grupos e outras redes. Neste ponto, realce-se novamente Bourdieu, que salienta que o carácter relacional deste termo continua a conter em si o poder e a luta entre atores como dimensões constitutivas. Neste sentido, as organizações tentam adequar-se às normas e culturas regulatórias, em vez de darem primazia à ‘escolha racional’ (Powell & DiMaggio, 1991). Ainda, a governação transnacional

pode ser vista como um ‘campo de forças’, na medida em que esses campos são estruturados por instituições dominantes que constituem a “transnational culture or meaning system” (Djelic & Sahlin-Andersson, 2006, p. 28).

Em linha com os autores supramencionados, Katzenstein e colegas (1999) salvaguardam que o caráter transnacional da regulação não significa a anulação completa dos Estados, pelo contrário, estes encarnam o papel de atores como os demais, sendo que nem todas as interações passam sempre pelos mesmos canais de comunicação nem pelos mesmos atores. A compreensão daquilo que é a (re)governança do mundo não toma como garantida a centralidade do Estado, mas também não pretende negligenciar o papel que o mesmo detém nos vários processos de criação de regras e regulações (Djelic & Sahlin-Andersson, 2006, p. 4). Parafraseando, na governança transnacional contemporânea a soberania nacional e a autonomia associadas aos estados westfalianos não são uma garantia absoluta. Neste contexto, a governança transnacional é operada através de forças institucionais embebidas em diversas redes de atores que possuem estruturas geopolíticas e valores culturais diversos (*idem*, p. 5). Negligenciar os interesses comuns entre atores, bem como as relações de poder entre os mesmos, num plano transnacional, pode invisibilizar os conflitos que existem entre as políticas locais e globais dos países (Hallström & Boström, 2010, p. 7). Desta forma, a organização de determinados processos tem dois objetivos basilares, por um lado, adequar a organização ao contexto nacional, por outro lado, exercer poder sobre o mesmo (*idem*). Nesta linha de pensamento, olhar além do centralismo associado ao Estado permite assimilar o grau de autoridade que algumas instituições não governamentais possuem no meio social. Cutler, Haufler e Porter (1999), entendem que estamos perante uma situação de autoridade “when an individual or organization has decision-making power over a particular issue and is regarded as exercising that power legitimately” (*idem*, p. 5). Do mesmo modo, Weber (1947) encara a autoridade enquanto um conjunto de regras que são cumpridas por um conjunto de atores sociais que para além de as cumprirem também têm vontade de lhes obedecer (*idem*, p. 144). Neste sentido, Hallström e Boström (2010) chamam a atenção para a literatura relacionada com a autoridade privada, na medida em que vem reconhecer a ‘autoridade política e reguladora’ enquanto característica de meios não estatais (*idem*, p. 15).

Inicialmente entendida como parte integrante do contexto económico, a regulação transnacional, tem migrado para a esfera social das sociedades contemporâneas (Jordana &

Levi-Faur, 2004). Esta incursão gradual na esfera social gerou mudanças que conduziram a novos modos de governação com características ímpares. A abordagem sobre o espaço regulatório transnacional vem realçar as tensões entre a concorrência e a legitimidade (Botzem & Quack, 2006), colocando a descoberto a dificuldade sentida no estabelecimento da autoridade na criação de regras por parte das organizações de standardização. Neste campo de forças que é o plano transnacional, apenas as organizações e os atores com elevados níveis de legitimidade e de recursos conseguem produzir impactos na (re)governança (Hancher & Moran, 1989; Young, 1994). O carácter transnacional trazido pela regulamentação permitiu a criação de estruturas de controlo não só do meio económico como também do meio social numa dimensão geográfica que até então se encontrava balizada apenas no contexto intrafronteiriço (Djelic & Sahlin-Andersson, 2006, p. 8). Neste sentido, entende-se que o conceito de governação não se esgota na regulação, este possui uma dimensão mais macro da criação e implementação de regras, citando, “dense organizing, discursive and monitoring activities that embed, frame, stabilize and reproduce rules and regulations” (*idem*). Segundo Baldwin e colegas (1998), a regulação pode ser enquadrada em três categorias, respetivamente, (1) regulação enquanto regras autoritárias, (2) regulação como forma de orientação da economia (por parte das agências) e (3) regulação como mecanismo de controlo social (*idem*, pp. 3-4). De forma complementar, Djelic e Sahlin-Andersson (2006), destringem quatro dimensões que decorrem da categorização apresentada (*idem*, p. 6).

A primeira dimensão remete para o agente de regulação. Em perspetivas mais conservadoras é dado ao Estado o papel central neste processo. No entanto, em conceções mais abrangentes, assume-se que existe uma elevada pluralidade de atores que se interrelacionam e que procuram recursos e autoridade em meios diversos e ‘arenas fluídas’, sendo este processo característico da contemporaneidade e dos seus modos de reorganização das esferas sociais (Cutler et al., 1999; Sahlin-Andersson, 2004). A segunda dimensão está relacionada com o modo de regulação. Inicialmente a criação de regras esteve largamente associada aos poderes coercivos do Estado Westfaliano e estas tinham o nome de *hard laws*. Atualmente, várias conceções referem que as regras se têm modificado no sentido de serem não obrigatórias – *soft rules* –, como são exemplo os *standards* (Botzem & Dobusch, 2012, p. 1). Desta forma, assiste-se a uma complementaridade entre as *hard laws* e as *soft rules* na governação contemporânea (Djelic & Sahlin-Andersson, 2006, p.

6). Ainda, as organizações podem desempenhar um papel relevante num tipo de regulação *soft* não coerciva (Ahrne & Brunsson, 2006). A terceira dimensão incide na natureza das regras, ou seja, se estas são formais ou informais. As regras informais são mais passíveis de serem ajustadas e interpretadas (Kirton & Trebilcock, 2004; Sahlin-Andersson, 2004). É importante realçar que não deve confundir-se o carácter voluntário e não coercivo de um *standard* com a sua informalidade, pelo contrário este encontra-se muitas vezes inscrito em regras e documentos formais (Djelic & Sahlin-Andersson, 2006, p. 6). Por fim, a quarta dimensão diz respeito à conformidade com os mecanismos, ou seja, o que leva os indivíduos/atores que estão a ser regulados a seguir ou não as regras (*idem*, p. 7). Por outras palavras, de que forma é que as organizações de standardização asseguram que os seus *standards* são os melhores, os mais úteis e os mais confiáveis na gestão da vida social, económica e política (Hallström & Boström, 2010). Nesta linha e como já foi referido, Schmidt (2004) defende que na contemporaneidade tem-se assistido a um controlo menos centrado no Estado e na coerção e mais centrado no que chama de legalismo.

Relativamente à estruturação teórica do que é a regulação transnacional, Djelic e Sahlin-Andersson (2006) entendem que esta tem sido interpretada de acordo com cinco forças institucionais, respetivamente, (1) cientificização, (2) marketização, (3) organização, (4) racionalização moral e (5) democracia. Portanto, a cientificização contribui para o alargamento da autoridade nas sociedades modernas através da criação de várias entidades sociais de organização e criação de regras às quais os atores recorrem utilizando uma argumentação por meio da ciência para legitimarem a sua autoridade (*idem*, p. 29). Associados a este conceito encontram-se os termos de quantificação e medição. A marketização pauta-se pela ideia de que os mercados são rápidos agentes de institucionalização e, como tal, são pensados como ‘naturais’ e adequados para organizar e estruturar as interações humanas, operar reformas, influenciar políticas, discursos e ideias (*idem*). A organização serve o propósito da criação de ordem transnacional, na medida em que pretende aproximar vários Estados-Membros com diferentes valores e tradições culturais (*idem*, p. 30). Neste ponto, a standardização é um dos mecanismos eleitos para o efeito. A racionalização moral generalizada (Boli, 2006) remete para as noções de virtude e virtuosismo passíveis de serem medidas cientificamente em escalas através, por exemplo, de rankings e creditações. Por fim, a democracia vem reforçar o papel participativo e deliberativo e a autonomia dos atores que fazem parte da governação transnacional, bem

como releva a importância e a corrente expansão de formas *soft* de governação (Djelic & Sahlin-Andersson, 2006, p. 30). Ainda, vários autores referem que a dependência entre as redes de atores mostra-se como um dos mecanismos mais importantes para a estabilização da governação (Cutler et al., 1999; Streeck & Schmitter, 1985; Young, 1994).

Tal como se observa nos processos de standardização, também a regulação gera a necessidade de criar e redefinir mais regulação, sendo que a governação transnacional é operada através de forças institucionais dominantes que se inserem em ‘tipografias espaciais’ muito diversas. Tem-se, por um lado, um meio fluído, interacional e relacional e, por outro, um ambiente constrangido e limitado (Djelic & Sahlin-Andersson, 2006, p. 37). As forças institucionais promovem uma governação assente em regras *soft*, ou seja, de carácter voluntário sem vinculação legal. As características supramencionadas permitem que estes tipos de regras possam ser enquadradas no âmbito transnacional, pois facilitam a adaptação local das mesmas, conservando-lhe um certo grau de autonomia. A adequação às características locais é feita através da “elaboration and negotiation of rules, diffusion, translation, appropriation and rejection, potentially stabilization and socialization” (*idem*, p. 31). Clarifique-se que as forças institucionais supramencionadas são parte integrante dos atores, pelo que estes não se limitam a se adaptar às mesmas, também as constroem (*idem*, p. 32). Sob este pano de fundo elencam-se três dimensões da governação transnacional exploradas por Djelic e Sahlin-Andersson (2006) que sistematizam vários dos tópicos que têm vindo a ser referidos, nomeadamente, os (1) atores de governação, os (2) processos de governação e a (3) governação e implementação institucional.

A primeira dimensão reforça o afastamento do Estado enquanto figura central num mundo contemporâneo transnacional e globalizado (Strange, 1996). Neste ponto enfatiza-se que os Estados têm evoluído para o que Majone (1996) intitula de ‘Estados regulatórios’, na medida em que mantendo uma postura ativa na governação se encontram mais dependentes de relações entre atores e estruturas de relação mais complexas. Críticas a esta premissa pautam-se pela continuada centralização do Estado. Scott (2004) como forma de colmatar esta lacuna cunhou o termo ‘Estados pós-regulatórios’ que são definidos como “a loosening of the sharp distinction between states and markets and between the public and the private” (*idem*, p. 3). A conceptualização apresentada por Scott (2004) revela-se um dos vetores explicativos da multiplicidade de redes de interação de atores, bem como a expansão da autoridade privada no contexto transnacional. No âmbito transnacional, as

redes de interação sociais (Haas, 1989, 1992) apresentam-se como instrumentos de governança quer ao nível local/nacional quer ao nível transnacional. Nesta linha de pensamento e a par com as evoluções do papel do Estado, as ‘comunidades epistémicas’ (Haas, 1992) têm vindo gradualmente a assumir um carácter mais transnacional. Esta mudança espelha um contexto de fluidez das fronteiras nacionais, pois ainda que inseridos nas malhas de uma comunidade transnacional de especialistas e práticas, estes atores continuam a conservar as influências da autoridade local e/ou nacional em que se inserem (Djelic & Sahlin-Andersson, 2006, p. 13). O conceito de ‘atores *soft*’ pode ser aqui elencado na medida em que remete para a ideia de que os atores se encontram interconectados e, como tal, influenciam e são influenciados pelos demais, representando a ideia de que as suas identidades são líquidas e permanecem em constante fluxo (Meyer, 1996).

A segunda dimensão – processos de governação – remete para a ideia de que a criação de regras se encontra disseminada por todas as esferas sociais, tanto ao nível nacional como transnacional (Djelic & Sahlin-Andersson, 2006, p. 15). Tendo a governação como referencial, percebe-se que para além das regras, também as atividades de monitorização, de avaliação e de auditoria têm aumentado. Com recurso ao pensamento de Power (1997), considera-se que as sociedades contemporâneas procuram a estruturação de todas as suas atividades e processos de modo a permitirem a transparência e a prestação de contas através de auditorias. A este respeito “[i]t (...) favors more universal types of rules as abstract expertise tends to be highly legitimate while practicing and individual experts often suggest distrust instead” (Djelic & Sahlin-Andersson, 2006, p. 16).

A terceira dimensão, sobre a governação e implementação institucional, vem complementar as dinâmicas entre atores, na medida em que observar as instituições permite uma análise ao plano invisível da governação. É fundamental que se compreenda de que modo a cultura, as normas e as instituições moldam e/ou constroem os fluxos, as relações e as dinâmicas entre diversos atores também eles imbuídos de valores culturais (*idem*, p. 17).

Os atores que direta ou indiretamente são responsáveis pela criação e manutenção da governação transnacional podem ser enquadrados genericamente em diversas categorias. Numa primeira incluem-se os atores que se encontram relacionados diretamente com o Estado e a administração política, sendo que os poderes de coerção continuam a permanecer nestes órgãos (*idem*, p. 35). As organizações públicas

internacionais situam-se na segunda categoria e têm como objetivo o reforço da governação transnacional (*idem*, p. 36). A terceira categoria remete para os ‘atores reinventados’, atores que devido às alterações na governação tiveram de se adaptar e tornar-se agentes ativos da governação transnacional (universidades, média, corporações) (*idem*, p. 36). Por último, na quarta categoria, encontram-se os ‘novos atores’, atores que estão cada vez mais a alcançar um papel de poder e destaque na governança transnacional devido às suas estruturas e características (ONGs) (*idem*, p. 36; Hallström & Boström, 2010). Neste sentido, os atores responsáveis pelos processos de standardização têm como objetivo último “influenciar os outros” (Ahrne, Brunsson, & Garsten, 2005, p. 50).

Para o efeito recorrem a quatro estratégias que visam conduzir os restantes atores na adoção e disseminação de determinado *standard*. A primeira remete para a possibilidade de se dirigirem a outros atores para além dos que seriam óbvios na adoção do *standard* em questão. A segunda tem que ver com a hipótese de se associarem a terceiros que possuam poder e autoridade de modo a encaminhar os atores para um *standard*. A terceira incide no grupo dos que adotam os *standards* e passa por ajudar estes atores a implementar as regras, bem como por dar regalias a quem as segue. Por fim, como quarta estratégia tem-se a criação de uma organização formal que visa aumentar o número de atores que seguem os *standards*, na medida em que os seus membros estão *a priori* obrigados a cumpri-los (*idem*, p. 50). As atitudes, por parte dos indivíduos, perante um *standard* ou a própria organização de standardização podem ser muito diferentes. Hallström e Boström (2010) identificaram oito estratégias de (não) participação em determinado *standard*, nomeadamente, (1) influenciar diretamente os conteúdos do *standard* em questão; (2) ignorar o *standard* de forma a não o cumprir; (3) atrasar ou parar deliberadamente o processo de implementação do mesmo; (4) proteger os seus próprios *standards*; (5) acelerar o processo de implementação de modo a demonstrar que é um *standard* adequado para o efeito; (6) aprender sobre o campo em que este irá atuar; (7) desenvolver redes sociais de interação que o suportem; e, por fim, (8) aumentar o seu valor no meio social (*idem*, p. 95).

O sucesso da standardização no plano nacional e transnacional também pode usufruir da criação de organizações formais. No entanto esta ideia de estrutura formal no processo de criação e implementação de *standards* tem sido apreendida sob dois eixos teóricos distintos. No primeiro encerram-se as visões que entendem as organizações formais como instituições de oposição à standardização (Ahrne et al., 2005, p. 51). No

segundo, compreendem-se as concepções que se apoiam na evolução dos processos tradicionais de standardização para a formação de organizações que se comportam enquanto agentes de standardização. Esta agência permite-lhes que estejam em constante atividade de criação de *standards* de modo a suprir as necessidades de autonomia dos seus membros, bem como a facilitar a organização do ambiente social que os rodeia (Brunsson & Olsen, 1998). Sendo que, segundo Hallström e Boström (2010), a standardização transnacional operada por diversos atores e/ou organizações remete para “[a] large group of organizations representing various interests, values, or bodies of knowledge and expertise that are to be reflected in the standards established (or to be reflected in standard proposals defeated)” (p. 79).

A figura organizacional vem garantir maior capacidade de influência e de organização do outro através de um conjunto de recursos que nem sempre se encontram disponíveis nos processos de standardização aberta (Ahrne et al., 2005, p. 52). Uma das primeiras vantagens que decorre da disponibilidade de recursos tem que ver com a maior possibilidade de controlo da arena espacial e social que está a sofrer o processo de standardização. Uma segunda vantagem remete para uma maior capacidade de promoção de ‘interesses comuns’ entre os atores que optam por utilizar determinado *standard* (*idem*). Dito isto, com a criação de uma organização formal de standardização ocorre uma cimentação do poder e da autoridade para criar *standards* e regulações, como também para escolher quais os membros adequados para usufruir dos mesmos (Ahrne, 1994). Pois, estas limitam-se a representar certos grupos com base no seu conhecimento e nos seus interesses comuns (Hallström & Boström, 2010, p. 79). Neste sentido, a adoção de um *standard* de uma organização em detrimento de outra garante, aos atores, a adoção de uma identidade diferente dos restantes, sendo que é o controlo operado por estas organizações que confere legitimidade à identidade assumida pelos mesmos (Ahrne et al., 2005, p. 55). As vantagens obtidas através das organizações apresentam-se, na maioria das vezes, como superiores às obtidas pelos indivíduos no plano da standardização aberta, ou seja, “standard-based organizations contribute to status differentiation within the field” (*idem*).

As organizações enquanto facilitadoras de interações sociais entre atores, produtoras de uniformidades e de objetivos comuns podem ser, em certas circunstâncias, um obstáculo aos atores que não pertencem nem se regem pelos *standards* da mesma (*idem*, pp. 56-57). Portanto, estas possuem um âmbito de ação que ultrapassa a mera

regulação dos atores nelas envolvidos. Também atuam nos ambientes sociais e económicos em que se encontram e, por conseguinte, contribuem para uma maior diferenciação de *status* entre atores. O seu sucesso quanto à regulação dos indivíduos e dos *standards* concorrentes tem que ver com o facto de conseguirem gerir os recursos do meio a seu favor. Para o efeito, munem-se de leis e regras de modo a afetarem os *standards* que devem ser seguidos, reduzindo ao mínimo a presença de organizações concorrentes (*idem*, p. 57). Esta ‘luta’ pelo poder está diretamente associada com questões de legitimidade e de *status*, na medida em que, “the more exclusive the standards for entry to the organization, the higher the status for the member” (*idem*, p. 58).

A integração de membros na organização é um processo, por norma, relativamente simples, pois o que leva um indivíduo a estar interessado em ser membro tem que ver com o facto de se encontrar em sintonia com os ideais defendidos e os *standards* definidos. Trata-se de fornecer aos membros uma maior garantia de recursos, proteção e de facilidade de interação (*idem*, pp. 59-60). Relativamente à disseminação dos *standards* encontram-se diferenças quanto ao processo de estandardização aberto e à criação de uma organização formal. Prevê-se que uma organização formal seja mais capaz de controlar a aplicação prática de um *standard* do que a estandardização por meio de processos mais tradicionais (*idem*, p. 61). A legitimidade das organizações é um ponto central para a disseminação de *standards*, sendo que uma das formas de a gerir passa pela aplicação de penalizações em caso de situação de irregularidade de algum membro. Deste modo, conseguem garantir a correção do erro e, em simultâneo, que o membro continue a fazer parte da organização após cumprida a sua sanção (*idem*, p. 63).

Enquadrando a criação de organizações formais de estandardização no plano transnacional, percebe-se que estas tendem a facilitar a interação, a alocação de recursos, o reconhecimento de interesses comuns e a coordenação entre membros (Ahrne et al., 2005, p. 66). Sendo que é, por norma, mais fácil para o indivíduo adotar uma identidade que seja reconhecida globalmente, o que pode facilitar a obtenção de credibilidade (*idem*, p. 67). Neste sentido, também a criação de organizações formais ao nível nacional é mais fácil de ser justificada com a existência de uma organização transnacional com o mesmo tipo de *standards* (*idem*).

Os autores terminam com algumas ideias a reter sobre a globalização das organizações formais baseadas nos processos de estandardização. Primeiro, as organizações

formais globais fazem parte do próprio processo de globalização, não se esgotam enquanto resposta ao mesmo. Segundo, estas influenciam tanto o plano nacional como internacional em matéria de standardização (*idem*). Terceiro, “[t]he globalization of standards should be understood as a delicate balance between similarity and difference” (*idem*, p. 68), pois apesar da partilha de regras entre organizações, cada uma é performada de modo diferente em contexto nacional.

(D)standardização do perfil forense de DNA

Desde a descoberta do composto orgânico do DNA e da sua estrutura em dupla hélice os avanços científicos não se mostraram significativos ao ponto de serem responsáveis pela alteração do paradigma em relação ao perfil forense de DNA. Segundo Derksen (2010, p. 215), as alterações têm sido sentidas ao nível da “constellation of social relations surrounding DNA profiling”. A autora baliza a sua análise das ‘constelações das relações sociais’ entre os anos de 1988 e 1997 correspondendo ao hiato de tempo entre a condenação e a exoneração de Milgaard, erradamente acusado de violação e homicídio no Canadá. No seu artigo, Derksen argumenta que a inexistência de standardização em relação às práticas e protocolos de análise de perfis de DNA foi responsável pelos diferentes resultados obtidos na sequência do processo de exoneração de Milgaard (*idem*). Entende-se que a qualidade dos testes realizados às amostras de DNA depende de protocolos escritos que possam ser preservados, disseminados e mantidos no espaço e no tempo nas várias comunidades científicas (Lynch, 2002, p. 207).

Deste modo, em 1988, data da realização dos primeiros testes genéticos, não existiam práticas protocolares standardizadas para a obtenção, comparação e interpretação dos testes ao perfil de DNA forense. Sendo que os tribunais recorriam, com frequência, a várias empresas com métodos de análise incompatíveis entre si (Derksen, 2010, p. 215). Os segundos testes tiveram lugar em 1992, mas ‘a constelação das relações sociais’ continuava complexa, pois a comunidade científica era caracterizada por um elevado clima de competitividade pouco favorável à obtenção de consensos em relação à interpretação do perfil de DNA (*idem*). A exoneração de Milgaard chegou em 1997, com novos testes realizados num contexto científico e social muito diferente do inicial. Os terceiros testes gozaram de uma conjuntura favorável ao consenso na comunidade científica, sendo que os vários laboratórios já se encontravam a performar os testes genéticos através de métodos e protocolos de interpretação standardizados. De modo

semelhante, Lynch (2013), refere no seu trabalho que a objetividade alcançada pela prova de DNA em tribunal é ladeada pela *administrative accountability* (p. 60). Por este motivo, a ‘objetividade administrativa’ do DNA subjaz nas normas burocráticas, registos, protocolos, entre outros. Segundo o autor, as fontes administrativas de objetividade colocam a prova genética “within the context of ordinary organizational and practical routines” (*idem*). Deste modo, o protocolo adquire uma dimensão ritual que integra a cadeia de custódia de uma prova genética, onde os atores do sistema judicial se refugiam no percurso administrativo da prova enquanto marcador objetivo da qualidade e integridade científica dos testes realizados (Lynch, 2002, p. 218). A mudança nas ‘constelações das relações sociais’ foi, em grande medida, impulsionada por uma organização (FBI) que promoveu a regulação de protocolos e diretrizes para assegurar a qualidade das análises. Com isto pretendeu-se também a transferência da disciplina característica dos laboratórios para a dimensão do sistema de justiça criminal (*idem*, p. 207). O FBI realizou ainda um esforço no sentido de alocar recursos económicos para permitir que a tecnologia de análise dos perfis de DNA chegasse aos vários laboratórios forenses (Derksen, 2010, p. 215). Citando, “the scientific procedures that were used at the three time points were very similar, but by 1997, there was a wide-reaching and stable network of social structures supporting the knowledge” (*idem*, p. 216).

O consenso entre a comunidade científica foi possível devido ao papel fundamental de instituições como o FBI e o Grupo de trabalho sobre os métodos do DNA (TWGDAM), também financiado pelo FBI. Tendo como base argumentativa o exemplo do processo de exoneração de Milgaard, Derksen (2010) demonstra que a mobilidade de conhecimento entre estruturas sociais de diferentes dimensões obriga à criação de novas estruturas macro e micro sociais (p. 216). As duas premissas que subjazem o argumento passam pela constatação de que o conhecimento e a ordem social são (co)construídos ao nível macro e micro através de novas estruturas sociais e pela observação de que “to make knowledge is also to make social order” (*idem*, p. 217). Sendo que a produção efetiva de conhecimento é o que permite interconectar o nível micro e o nível macro. Dito isto, é necessário compreender de que modo é que as interações ao nível micro conseguem alcançar domínio suficiente para serem relevantes ao nível macro das estruturas sociais. Neste cenário as instituições ajudam à transmissão do conhecimento científico e da sua credibilidade, sendo que a sua legitimidade é assegurada pelo próprio conhecimento científico (Shapin, 2001).

Importa perceber de que modo é que as interações ao nível micro se relacionam com o nível macro da estrutura social, questão que Derksen (2010) se propôs a responder. Entenda-se que o consenso entre pessoas/cientistas é enquadrado no âmbito de uma microestrutura social, ao passo que a legislação e as bases de dados atuam enquanto estruturas sociais macro. Considerando que o conhecimento e a ordem social são (co)construídos, depreende-se que a criação de estruturas sociais e de conhecimento científico legítimo são o resultado da necessidade de se resolverem problemas associados à ordem social (*idem*, p. 217). Neste caso em particular, a falta de standardização ao nível da análise dos perfis de DNA em tribunal estava a colocar em causa a legitimidade do sistema de justiça em processos que envolviam este tipo de prova genética.

A teorização das estruturas micro e macro sociais que a autora realiza na sua investigação baseia-se no trabalho de Collins (1988). A este respeito o nível micro e macro das estruturas sociais são um espectro contínuo. Ao nível micro encontram-se interações de curta duração entre relativamente poucas pessoas e em espaços limitados. Ao nível macro têm-se as interações mais duradouras que envolvem mais pessoas e em espaços consequentemente maiores (Collins, 1988, pp. 386-388 apud Derksen, 2010, p. 218). Desta forma, o trabalho de cientistas em diferentes dimensões, contextos espaciais e temporais permitiu a estabilização e a standardização do conhecimento acerca do perfil de DNA, permitindo a criação de várias estruturas sociais. Estas estruturas foram passíveis de serem criadas devido aos consensos científicos obtidos ao nível micro que, ao nível macro, se traduziram em novas estruturas sociais. Derksen (2010) enuncia várias dessas novas estruturas, nomeadamente, práticas e protocolos estabilizados; normas de interpretação; profissionalização de grupos; *standards* de prática; laboratórios; bases de dados; projetos políticos; e legislação (*idem*, p. 218). A autora distingue vários momentos que considera serem de grande importância para a estabilização da interpretação e análise do perfil de DNA através da explicação dos movimentos do conhecimento entre o seu nível micro e macro.

Um dos pontos em discussão é a ‘quantificação da margem de erro’ e de que modo a quantificação através dos números veio compensar a subjetividade das práticas entre o que é a teoria e o que é o método (Derksen, 2000, p. 805). A quantificação é, deste modo, o resultado da tradução numérica daquelas que são as características do mundo natural em estudo (*idem*, p. 803). Porém o processo de quantificar é permeado pela negociação ente

agentes humanos (cientistas forenses, advogados, jornalistas, etc.) e não humanos (natureza, amostra de DNA), pois é impossível reduzir o erro a valores nulos. Esta condição tem uma possível justificação na incapacidade de se descrever *ipsis verbis* o que é realizado num laboratório (Lynch, 2002, p. 203). No caso particular da medição da margem de erro em relação ao DNA verificou-se uma disputa tanto científica como legal (Derksen, 2000, p. 803). A disputa na esfera legal, de modo similar à esfera científica, teve o seu início na década de noventa e formalizou-se com a criação de um grupo de trabalho a pedido da *National Association for Criminal Defense Lawyers* (*idem*, p. 804). Este grupo tinha por objetivo a desconstrução da caixa negra das metodologias de interpretação do DNA, pois havia, por parte dos advogados de defesa, a crença de que se considerava o DNA como um veredito ao invés de uma prova complementar ao processo (Mnookin, 2008). Nesta linha, o DNA foi sendo chamado a ocupar o estatuto de *gold standard* na ciência forense, por oposição a outros meios de prova que são encarados como falíveis e subjetivos quando comparados com o DNA (Lynch, 2013, p. 60). O grupo de trabalho avançou com duas estratégias de questionamento da técnica que visaram alcançar a dimensão subjetiva da negociação do que é cientificamente robusto. Para o efeito este grupo avaliou as diretrizes formais da prática científica e deram conta das incongruências entre o que se encontrava escrito e as práticas laboratoriais em particular (Lynch, 2002, p. 215). A primeira estratégia passou pela desconstrução dos protocolos técnicos, utilizados pelos laboratórios forenses²⁵, para determinar um *hit* entre a amostra de DNA de uma cena de crime e a de um suspeito. A segunda estratégia focou-se na contestação. Em particular, a discussão centrou-se no cálculo da probabilidade de uma determinada amostra de DNA corresponder a uma ou mais pessoas numa população aleatória (Derksen, 2000, 2010). A falta de *standards* científicos esteve na origem dos enviesamentos que este grupo encontrou em relação à interpretação da prova de DNA. As estratégias adotadas vieram elucidar de que modo o valor probatório da prova genética está dependente do modo como esta foi recolhida, analisada e interpretada no decorrer da investigação criminal (Lynch, 2013, pp. 60–61).

A medição da margem de erro na interpretação do DNA foi fundamental para dar robustez e objetividade ao conhecimento científico e à sua consequente utilização em tribunal como prova (Derksen, 2000). Importa referir que as correções administrativas

²⁵ O questionamento das metodologias incidiu principalmente nas empresas privadas e nos seus especialistas que testemunhavam em tribunal.

podem, muitas vezes, ser confundidas com correções científicas (Lynch, 2013, pp. 65–66). As primeiras têm que ver com a formulação de relatórios de controlo de qualidade que contêm recomendações protocolares sobre a recolha, análise e interpretação da prova (*idem*). A solução para uma melhoria administrativa – maior robustez da prova – passa por “more rigorous adherence to recommended protocols, more frequente use of blind proficiency testing, higher standards for accreditation of forensic personnel” (*idem*, p. 66). Os caracteres numéricos conferem legitimidade à técnica pois apresentam-se como ‘tecnologias de distanciamento’ (Porter, 1992) capazes de oferecer uma versão estandardizada e compreensível nas diferentes comunidades epistémicas e científicas. Este distanciamento encontra-se intimamente relacionado com uma das características mais importantes de um *standard*, a da invisibilidade (Baines, 2006; Bowker & Star 1999).

A subjetividade consequência de enviesamentos e arbitrariedades com origem nas diferentes culturas, no conhecimento tácito e nas contingências locais é tornada invisível à semelhança dos vários processos de estandardização (Czerniawski, 2007; Derksen, 2000, 2010; Epstein, 2007, 2009; Hallström & Boström, 2010; Igo, 2007; Lengwiler, 2009). A interpretação de uma correspondência de DNA pode também sofrer enviesamentos e carecer de precisão devido a fatores culturais associados à falta de isenção de julgamentos morais por parte dos cientistas forenses. Devido ao tipo de trabalho realizado num laboratório forense é comum que os seus profissionais estejam a par dos pormenores do caso criminal e da identidade dos suspeitos cujas amostras se encontram a analisar/comparar com as amostras presentes na cena de crime (Derksen, 2000, p. 816). Em termos pragmáticos, esta situação pode condicionar a análise ‘desinteressada’ das amostras de DNA por haver uma vontade implícita de se restituir justiça às vítimas ou às suas famílias. A influência de fatores culturais em meio científico e legal coloca em causa o ideal-tipo weberiano de burocracia (Weber, 1968) que tem como premissa o desinteresse e a imparcialidade dos intervenientes no processo. Deste modo, inserir o DNA na malha burocrática é torná-lo credível, imparcial e desinteressado (Lynch, 2013, p. 62) sendo que a verdade, em tribunal, é alcançada através da burocracia.

O percurso da utilização e legitimidade da prova de DNA em tribunal não foi linear nem tampouco consensual, tanto na esfera científica como em meio legal, pelo que pode ser dividida em três fases. Entre 1987 e 1988, a prova de DNA era vista com elevado otimismo e foi largamente aceite em tribunal. Acrescente-se que os advogados de defesa

não tinham capacidade para a contestar e os juízes não compreendiam cientificamente os métodos de interpretação do DNA (Derksen, 2000, p. 806). Neste período, a prova genética em tribunal encontrava-se num “exceptional epistemic space” por ser considerada ‘infalível’, ‘irrefutável’ e uma ‘máquina da verdade’ (Lynch, 2013, p. 63; Lynch et al., 2008). Este ideário foi promovido através das narrativas de promotores públicos, advogados, juízes, juristas, pessoas condenadas ou exoneradas com base em provas genéticas (Lynch, 2013, p. 63). Entre 1989 e 1991, surgiram vários casos de contestação da prova de DNA onde os advogados de defesa começaram a questionar a robustez, objetividade e legitimidade do conhecimento científico em relação ao DNA. Nesta fase colocou-se a descoberto a falta de consenso na comunidade científica que até então trabalhava com *standards* não formalizados que dependiam fortemente dos seus contextos locais (Porter, 1995). Neste sentido, Lynch (2002) defende que apesar de os protocolos serem regras estandardizadas e estabilizadas nas comunidades epistémicas, também deixam espaço para a influência das práticas locais que atuam em complementaridade com os mesmos (*idem*, pp. 205, 210).

Por fim, entre 1992 e 1994 consolidaram-se críticas e apuraram-se grupos de trabalho para que houvesse uma verificação constante da qualidade da prova de DNA (Derksen, 2000, 2010). As várias controvérsias sobre a utilização do DNA em tribunal ocorreram num *liminal space* (Knorr-Cetina, 1999, p. 63) que se caracteriza pela instabilidade de normas e valores em relação a determinada prática devido à transformação societal. Com a inexistência de diretrizes científicas que assegurassem a robustez da tecnologia de DNA, foi necessário criar novas normas e valores de modo a alcançar a objetividade tecnológica que veio colmatar as lacunas ao nível da sua admissibilidade em meio legal. Derksen (2010) defende no seu trabalho que foram as relações sociais e negociações entre atores que permitiram chegar a um consenso em relação aos protocolos a utilizar para a interpretação correta do DNA (*idem*, p. 15). Do mesmo modo Lynch (2013) enfatiza que na década de 90 não eram as técnicas de análise de DNA que figuravam como problemáticas, a maioria das críticas a respeito da prova genética prendeu-se com acusações de incompetência por parte de certas forças policiais e laboratórios forenses (*idem*, p. 65). Portanto, não houve a necessidade de correções de carácter técnico, as controvérsias em torno da robustez do DNA foram resolvidas através de pequenos arranjos técnicos, jurídicos e administrativos (*idem*). Na prática, o perfil de DNA podia ser interpretado à luz de diversos

métodos e, como tal, verificou-se a necessidade de escolher um que favorecesse o consenso entre a comunidade científica (Thompson & Ford, 1991, p. 110).

1.8. Imaginários Sociotécnicos

Os Estudos da Ciência e Tecnologia (STS) têm-se dedicado ao aprofundamento do estudo da complexidade das dinâmicas sociais na produção de ciência (Jasanoff, Markle, Petersen, & Pinch, 1995), da concepção de artefactos tecnológicos (Bijker, Hughes, & Pinch, 1987; Winner, 1986), da avaliação e sistematização de riscos e benefícios da implementação de tecnologias (Wynne, 1987) e da formação de conhecimento e culturas especializadas (Jasanoff, 1990). No entanto, alguns dos teóricos deste campo realçam a necessidade de se expandir o objeto de estudo da investigação através do estudo da promoção e da receção da ciência e da tecnologia por atores e instituições de carácter não científico (Jasanoff & Kim, 2009, p. 119). Neste sentido, Jasanoff e Kim (2009) contribuíram para a temática supramencionada com a introdução do conceito de imaginários sociotécnicos. Sheila Jasanoff é uma investigadora em STS com trabalho desenvolvido no âmbito das interações entre lei/direito, ciência e política nas sociedades democráticas. Em concreto, tem procurado discutir o papel da ciência e da tecnologia na construção de normas, formas de persuasão e de percepção da razão pública nas sociedades modernas. Sang-Hyun Kim é um investigador doutorado em química e em história e sociologia da ciência. Em particular, tem-se focado em políticas de *expertise* e governação da ciência e da tecnologia.

Os autores definem os imaginários sociotécnicos como “collectively imagined forms of social life and social order reflected in the design and fulfillment of nation-specific scientific and/or technological projects” (Jasanoff & Kim, 2009, p. 120). O conceito é relevante para o estudo comparado de diferentes realidades transnacionais relativamente a um mesmo fenómeno por permitir a identificação dos imaginários sociotécnicos a respeito do desenvolvimento da tecnologia e da ciência (Pfotenhauer & Jasanoff, 2017, p. 783). Neste sentido, as alterações sofridas por determinada tecnologia ou ciência na sua transposição para outra realidade nacional demonstram os modos de co-produção de um modelo em consonância com as especificidades nacionais (*idem*). A definição do conceito partiu da premissa de que a “capacity to imagine futures is a crucial constitutive element in social and political life” (Jasanoff & Kim, 2009, p. 122). Esta constatação permitiu que os autores se afastassem da concepção tradicional da noção de imaginação enquanto fantasia

ou ilusão (Sarewitz, 1996). Pelo contrário, a imaginação, enquanto recurso cultural, permite a projeção de metas e objetivos que, por sua vez, orientam os atores sociais para novos modos de vida (Kim, 2018, p. 177). Outro ponto basilar da imaginação tem que ver com a sua interação com a dimensão social, a imaginação vai além da sua dimensão individual. Jasanoff e Kim (2009) afirmam que a “*imagination helps produce systems of meaning that enable collective interpretations of social reality*” (*idem*, p. 122). Por sua vez, a dimensão social permite a uma determinada comunidade social e política a construção daquilo que é a representação ‘do outro’ (Said, 1978 apud Jasanoff & Kim, 2009). A coletivização do conceito de imaginação interfere ainda com a capacidade de estandardização dos atores sociais tornando a sua governação mais eficiente (Bowker & Star, 1999). Por fim, a imaginação enquanto ‘an organized field of social practices’ é um elemento fundamental para a ordem social (Appadurai, 1996; Jasanoff, Kim, & Perling, 2007; Taylor, 2004)

Os Estudos da Inovação também têm contribuído para a aplicabilidade do conceito de imaginários sociotécnicos sobre uma determinada tecnologia ou ciência. A este respeito, através de uma metáfora médica, Pfotenhauer e Jasanoff (2017) compararam três contextos nacionais de forma a explorar de que modo os imaginários acerca de determinado modelo podem contribuir para diferentes métodos de implementação do mesmo. Através do seu estudo empírico os autores concluíram que o (in)sucesso de um modelo tecnológico ou científico está mais dependente dos imaginários sociotécnicos de uma determinada comunidade do que da possível falta de capacidade de implementação e da universalidade do mesmo (Pfotenhauer & Jasanoff, 2017, p. 783). Neste sentido, realçam que quando a implementação de uma tecnologia não é concluída com sucesso, por norma, não se questiona o modelo a cumprir, pois este goza do carácter universal e desejável associado à inovação (*idem*, p. 785). Portanto, o não sucesso é comumente justificado por fatores de ordem contextual e cultural (*idem*, p. 786). Pfotenhauer e Jasanoff (2017) são críticos da invisibilidade dos processos de co-produção dos imaginários sociotécnicos na implementação de um mesmo modelo em contextos nacionais distintos e sugerem que:

“[A]n imported innovation model should be understood as part of a collectively held imaginary of sociotechnical progress that accompanies a complementary diagnosis of a deficiency in the receiving environment. Both the ‘diagnosis’ and the imagined ‘cure’, in the form of the imported model, are shaped

by and reinforce pre-existing visions of desirable and undesirable futures in a given society” (*idem*, p. 786).

Os autores pretenderam com o seu trabalho dar conta de que o facto de um modelo tecnológico ser diferente em vários países não encontra a sua justificação apenas no desencontro entre o modelo e os fatores culturais nacionais. Pelo contrário, as diferentes apropriações de um modelo estão intimamente associadas às expectativas e aos imaginários, também eles diferentes, acerca do papel a desempenhar por uma determinada tecnologia numa determinada sociedade (*idem*).

Os estudos da ciência e tecnologia contribuíram para a desmistificação do carácter individualista da imaginação na investigação científica e tecnológica. As práticas científicas e tecnológicas compreendem “visões e expectativas de possibilidades futuras” (Fujimura, 2003; Mackenzie, 1996), que vão moldar as decisões a seu respeito e, consequentemente, as suas trajetórias (Borup, Brown, Konrad, & Van Lente, 2006; Hedgecoe & Martin, 2003). A co-construção das trajetórias científicas é realizada através da ciência e da compreensão daquilo que é bom ou não para a sociedade (Jasanoff et al., 2007; Levenda, Richter, Miller, & Fisher, 2018, p. 123). Dito isto, os imaginários sociotécnicos não devem ser confundidos com agendas políticas. Citando, os imaginários são “less explicit, less issue-specific, less goal-directed, less politically accountable, and less instrumental; they reside in the reservoir of norms and discourses, metaphors and cultural meanings out of which actors build their policy preferences” (Jasanoff & Kim, 2009, p. 123). Estes não informam ou justificam determinados eventos que ocorreram no passado, o seu âmbito de atuação encontra-se no futuro, citando “imaginaries are instrumental and futuristic” (*idem*; ver também Pfotenhauer & Jasanoff, 2017, p. 788). Portanto, existem dois pontos fundamentais a reter a respeito dos imaginários. Primeiro, apresentam os ideários do que é desejável de alcançar por uma determinada comunidade política. Segundo, concentram em si mesmos a capacidade de dar conta dos potenciais riscos que determinada investigação tecnológica e científica pode acarretar se for levada a cabo demasiado rápido (Jasanoff & Kim, 2009, p. 123). Nas palavras dos autores, ao “activat[e] collective consciousness, imaginaries help create the political will or public resolve to attain them” (*idem*).

A investigação que possui o conceito de imaginários sociotécnicos como conceito basilar pretende compreender de que modo a multiplicidade de narrativas que circulam na sociedade são apreendidas, filtradas e reinseridas na ação pública. Jasanoff e Kim (2009)

defendem que os “imaginaries operate in the understudied regions between imagination and action, between discourse and decision, and between inchoate public opinion and instrumental state policy” (p. 123). De modo a clarificar a aplicabilidade do conceito Jasanoff e Kim (2009) elencam um conjunto de perguntas que visam apreender o papel do Estado em relação ao que este define como ciência e tecnologia que deve usufruir do apoio da sociedade em geral (*idem*). Primeiro, o que é o bem público e que públicos devem usufruir do investimento em ciência e tecnologia. Segundo, quem deve contribuir para o rumo da ciência e através de que meios. Terceiro, como se devem solucionar as controvérsias que possam emergir da ciência (*idem*).

A ciência e a tecnologia com aplicação direta nos objetivos Estatais, como em questões de segurança relacionadas com a redução do crime e do terrorismo, é, geralmente, acompanhada por um conjunto de políticas que permitem o seu desenvolvimento. Políticas essas que, no caso da redução da criminalidade, são o culminar dos imaginários sociotécnicos de vários atores sociais (cientistas, advogados, juízes, polícias e políticos) em relação ao futuro imaginado do papel que o perfil de DNA viria a ter nas atividades de investigação criminal (Pickersgill, 2011, p. 27). Portanto, as bases de dados forenses de perfis de DNA e a sua partilha transnacional entre Estados-Membros da UE são um exemplo da aplicação da ciência e tecnologia nos objetivos securitários do Estado. Sendo que as políticas de promoção científica e tecnológica combinam dois aspetos a realçar. Primeiro, contêm “distinctive national visions of desirable futures driven by science and technology” (Jasanoff & Kim, 2009, p. 121). Segundo, colocam a descoberto “fears of either not realizing those futures or causing unintended harm in the pursuit of technological advances” (*idem*). Um exemplo prático é o da constatação nacional de que a partilha de dados pode ajudar a diminuir o crime não só no país, como nos restantes Estados. No entanto, o medo de causar danos morais a cidadãos nacionais por mau uso dos dados ou por incorreções nos mesmos conduziu os países a optarem por diferentes critérios de partilha de dados relativos aos perfis de DNA. Dito isto, a partilha de dados realizada através do sistema Prüm, um modelo parcialmente estandardizado, não é realizada do mesmo modo nas diferentes realidades nacionais e contextos políticos (Pfotenhauer & Jasanoff, 2017, p. 802). Se por um lado, países como Portugal têm procurado a total implementação de sistemas como o de Prüm (Machado & Silva, 2010). Por outro lado, certos Estados, como o Reino Unido, têm sido politicamente menos recetivos aos mesmos (McCartney, 2013).

Neste sentido, o ‘interesse nacional’ vem mais uma vez justificar as decisões Estatais em relação à priorização e alocação de recursos para determinadas tecnologias em detrimento de outras. Onde a estabilização dos imaginários sociotécnicos verte tanto do papel da cultura nacional como das práticas e decisões políticas (Jasanoff & Kim, 2009, p. 121; Pfotenhauer & Jasanoff, 2017).

Entende-se que os imaginários sociotécnicos têm primazia na estruturação dos discursos antecipatórios (Barben, Fisher, Selin, & Guston, 2008; Guston, 2014) e nas práticas associadas a determinado modelo tecnológico e/ou científico, sendo os responsáveis pela delineação dos futuros imaginados (Pickersgill, 2011, p. 28). Deste modo, a construção dos potenciais futuros assenta num conjunto estrito de perceções sobre o que é a ciência e a ordem social que são amplamente difundidas quer pelos atores sociais, quer por instituições que partilhem os mesmos ideários tecnológicos e científicos (*idem*, p. 27). Estas perceções são ainda influenciadas pelas representações coletivas de solidariedade e pertença nacional que conduzem a diferentes enquadramentos do que são os benefícios, riscos e modos de governação de determinada ciência/tecnologia (Jasanoff et al., 2007). O contributo dado pela ciência forense no âmbito da esfera legal coloca os cientistas forenses, advogados e outros atores sociais relevantes numa posição de suma importância na persecução de uma relação eticamente robusta entre estes dois campos (Pickersgill, 2011, p. 29). Sendo que, os debates relativamente à aplicabilidade da ciência forense em meio legal são permeados pelos imaginários sociotécnicos específicos, tanto ao nível nacional como da classe profissional, que legitimam e promovem uma narrativa em detrimento de outra (*idem*, p. 30). Acrescente-se que o diálogo é realizado naquelas que são as fronteiras da ciência, da lei e da ética (*idem*, p. 36).

Os imaginários sociotécnicos sobre uma tecnologia/ciência possuem a capacidade plástica de tradução a vários níveis, desde o local, ao nacional e ao global (Kim, 2018, p. 192). Contudo, a transferência de um imaginário sociotécnico entre o nível micro, meso ou macro vem acompanhada de uma (re)configuração daquela que era a sua estrutura interpretativa inicial, pois está intimamente dependente da sua comunicação com outros imaginários que podem ou não ser concorrentes (*idem*). Em termos práticos, o sistema Prüm representa um determinado imaginário global sobre cooperação policial e segurança que é (re)configurado ao nível dos imaginários nacionais dos países membros da União Europeia. Sendo que, pode entender-se que, para além de outros fatores, a implementação

do sistema Prüm pode ser mais ou menos célere consoante a proximidade entre os imaginários nacionais e os globais. Enfatize-se, novamente, que os diferentes imaginários sociotécnicos encontram a sua fundamentação nas diferenças geográficas, históricas, políticas e culturais das realidades nacionais (Levenda et al., 2018, p. 2). Dito isto, a aplicação do conceito de imaginários sociotécnicos no estudo de uma tecnologia/ciência permite o questionamento sobre como as “relationships between science, technology, and society are collectively imagined at the broader political levels of state and society” (Jasanoff et al., 2007).

CAPÍTULO 2. METODOLOGIA

2.1. Enquadramento do projeto Exchange

A presente tese foi realizada no âmbito do projeto “Exchange – Geneticistas forenses e a partilha transnacional de informação genética na União Europeia: Relações entre ciência e controlo social, cidadania e democracia”. O projeto é liderado pela Professora Doutora Helena Machado e encontra-se, atualmente, sedado no Centro de Estudos de Comunicação e Sociedade (CECS) do Instituto de Ciências Sociais (ICS) da Universidade do Minho (Portugal). O projeto recebeu financiamento do Conselho Europeu de Investigação (ERC) sob o programa de pesquisa e inovação da União Europeia Horizonte 2020 (Contrato n.º 648608). Deste modo, a tese segue as mesmas diretrizes metodológicas do projeto Exchange.

O projeto Exchange visa explorar as dimensões sociais, culturais, éticas, regulatórias e políticas do uso de tecnologias de DNA para uso forense na União Europeia. De forma a apreender a pluridimensionalidade que caracteriza este objeto de estudo e a privilegiar as perspetivas socialmente construídas pelos diferentes atores sociais que se relacionam profissionalmente com a temática empírica, este projeto ancora-se numa metodologia de carácter eminentemente qualitativo. Esta opção teórico-metodológica, aliada ao condicionalismo de apenas ser possível subtrair dos estudos pré-existentes conceitos sensibilizadores (Charmaz, 2009, p. 34) e não quadros teóricos e hipóteses de trabalho gerais, implica adotar estratégias de pesquisa que possibilitem associar a construção de hipóteses e a elaboração de conceitos teóricos às circunstâncias específicas da realidade empírica localmente situada. Assim, seguindo alguns dos pressupostos da *grounded theory* (Strauss & Corbin, 1990), que viabilizam a construção de teorias “fundamentadas” nos próprios dados com elevado valor heurístico (Charmaz, 2009), esta investigação pauta-se por uma articulação e comparação sistemática e paralela entre recolha e análise, empiria e teoria (Strauss & Corbin, 1990). Este estudo valoriza, assim, a representatividade sociológica de cada caso, sendo que estes se afiguram como generalizáveis a enunciações teóricas e não a populações ou universos (Brandão, 2010, pp. 45–46; Nunes, 1992, pp. 247–248; Yin, 1994, p. 10).

Ao nível das técnicas de recolha de dados, o Exchange utiliza uma abordagem multi-metodológica, que assenta na conjugação de várias técnicas de recolha de dados,

nomeadamente, 1) análise de documentação proveniente de várias fontes relevantes; 2) realização de entrevistas semiestruturadas; 3) observação em encontros científicos da genética forense e outros de natureza interdisciplinar e outros contextos situacionais relevantes; e, por fim, 4) recolha e análise de casos criminais que envolvem o uso de tecnologias de DNA. Em particular, para a concretização da presente tese, a realização de entrevistas semiestruturadas foi a técnica que se afigurou mais relevante, sendo que, a consulta de documentação oficial proveniente de várias fontes (ponto 1) serviu de apoio para a comparação e compreensão do material analisado nas transcrições das entrevistas semiestruturadas. As fontes consultadas remeteram para documentos sobre os ordenamentos jurídicos em relação às bases de dados forenses de perfis de DNA em Portugal e no Reino Unido²⁶, para os *websites* das instâncias europeias que atuam no âmbito da cooperação policial e judiciária, bem como os regulamentos sobre proteção de dados no seio da União Europeia.

2.1.2 Contributos específicos da tese

Atendendo ao enquadramento do presente estudo no âmbito do Exchange, a presente investigação almeja compreender os sentidos atribuídos à conceção de proteção de dados genéticos e privacidade em torno do sistema Prüm, através das narrativas dos Pontos de Contacto Nacionais (NCPs) do sistema Prüm, de cientistas forenses, de membros de comissões de ética e de atores do sistema de justiça. Visa-se, assim, identificar os desafios éticos e sociais que a proteção da informação genética suscita nas várias esferas profissionais. Apesar do ideal de unidade ambicionado pela União Europeia, é imperativo identificar e perceber se existem e quais são as divergências espelhadas nas legislações dos Estados-Membros relativamente à proteção de dados, em específico, a proteção de dados genéticos no âmbito do sistema Prüm. Por fim, quais as implicações práticas que estas podem apresentar aquando da partilha de dados genéticos entre países da União Europeia. A 1) consulta de documentos, regulações e legislação do enquadramento europeu e organizações relevantes neste contexto sobre proteção de dados, privacidade na partilha de dados genéticos e cooperação policial e judicial; e a 2) análise de conteúdo de entrevistas semiestruturadas realizadas a atores sociais do sistema de justiça, membros de comissões

²⁶ Legislação portuguesa e britânica a respeito da base de dados forense, acórdão sobre *S & Marper vs The United Kingdom*, entre outros.

de ética, cientistas forenses e Pontos de Contacto Nacionais para o sistema de Prüm permitirão alcançar a pluridimensionalidade dos dados recolhidos para a análise qualitativa.

O estudo será conduzido pelos seguintes objetivos gerais:

1. Mapear o debate e as tendências atuais da proteção de dados na União Europeia, visando, em particular: a) compreender a especificidade do debate e regulação em relação a dados para investigação criminal face à proteção de dados em geral; b) identificar tensões e controvérsias em torno da proteção de dados pessoais *versus* vigilância e proteção da segurança das sociedades.
2. Explorar os dilemas éticos e sociais que decorrem da partilha transnacional de dados genéticos, inseridos em bases de dados de perfis de DNA para fins forenses, entre países da União Europeia, concretamente o sistema de Prüm. Em particular, perspetivar a possível compressão de direitos civis e humanos e a possibilidade de criminalização e estigmatização de grupos socialmente mais vulneráveis no contexto da União Europeia.
3. Analisar as perspetivas veiculadas pelos Pontos de Contacto Nacionais, pelos atores pertencentes às comissões de ética, à ciência forense e ao sistema de justiça relativamente às representações e sentidos atribuídos à noção de proteção de dados e privacidade.
4. Identificar os “imaginários sociotécnicos” em duas realidades nacionais, nomeadamente, Portugal e o Reino Unido, de forma a compreender o posicionamento, face ao fenómeno da partilha transnacional de dados genéticos e pessoais, de atores de diversas áreas (ética, direito, ciência forense) que têm contribuído para o debate sobre as controvérsias levantadas pelo uso da biotecnologia no sistema de justiça.

2.2. Entrevistas semiestruturadas - Métodos de amostragem

O principal objetivo subjacente às entrevistas semiestruturadas foi o de captar narrativas imbuídas de significados e sentidos ilustrativos da diversidade de perspetivas relativas às dimensões sociais, culturais, éticas, regulatórias e políticas do uso de tecnologias de DNA para fins forenses na União Europeia. No que concerne aos métodos de

amostragem, utilizou-se a amostragem intencional, conjugada com amostragem em bola de neve (Yin, 2011, pp. 88–89). A amostragem intencional foi realizada em três níveis:

1. Consulta da lista oficial de Pontos de Contactos Nacionais do sistema Prüm (National Contact Points – NCPs), através da consulta da lista pública providenciada nos documentos da ‘Working Party on Information Exchange and Data Protection’ (Union, 2015, 2017) e contactos com informantes privilegiados.

2. Seleção de profissionais da genética forense na União Europeia, selecionados por consulta de listas de membros de organizações profissionais, como por exemplo EUROFORGEN²⁷ e VISAGE²⁸, ambas redes de investigação compostas por geneticistas forenses e outros profissionais ligados à ciência forense financiadas pela Comissão Europeia. A seleção de profissionais da genética forense na União Europeia contou também com a pesquisa de autores de artigos científicos na área e pesquisa de profissionais com participação em eventos de interesse como, por exemplo, conferências da *International Society for Forensic Genetics* (ISFG)²⁹.

3. Seleção de outros stakeholders dos países de estudo de caso por via da consulta de listas de membros de organizações profissionais e autores de artigos científicos na área. O processo de amostragem foi também complementado pela amostragem em bola de neve e pelo acesso a informantes privilegiados. O projeto Exchange possui na sua metodologia cinco estudos de caso, respetivamente, Alemanha, Países Baixos, Polónia, Portugal e Reino Unido.

Para efeitos da presente tese foram estudados dois países, nomeadamente, Portugal e Reino Unido. A opção deveu-se ao facto de serem exemplos antagónicos em relação à tradição das bases de dados forenses de DNA e da própria cooperação transnacional. Em particular, Portugal é dos países com uma base de dados forense de perfis de DNA mais recente, mais pequena e com critérios de inserção/retenção de perfis de DNA mais restritivos. O Reino Unido, por sua vez, possui a base de dados forense de perfis de DNA mais antiga e a maior da União Europeia, sendo que os critérios de inserção/retenção são substancialmente mais inclusivos que os portugueses. Em termos de cooperação policial e

²⁷ <https://www.eurofor-gen.eu>

²⁸ <http://www.visage-h2020.eu>

²⁹ <https://www.isfg.org>

judiciária ao nível transnacional os posicionamentos mostram-se igualmente diferentes nos dois contextos nacionais. Portugal apresenta-se como um país que apoia genericamente a cooperação policial e judiciária em prol da reciprocidade e de maior segurança ao nível da União Europeia. O Reino Unido tem demonstrado uma postura de carácter mais utilitário em relação à cooperação policial e judiciária, ou seja, o que é mais útil para a sociedade britânica em termos de redução da criminalidade levada a cabo por estrangeiros no seu país. Importa salientar que as entrevistas semiestruturadas foram aplicadas nos dois países entre os anos de 2015 e 2019. Deste modo, assume particular importância o contexto de instabilidade política sentida no seio da sociedade britânica com a votação do *Brexit*, em 2016. Assim, as narrativas dos/as participantes foram também influenciadas pelo período em que as entrevistas foram realizadas, ou seja, antes ou depois da votação para a saída do país da União Europeia. Posto isto, a escolha dos casos de estudo brevemente apresentados permite compreender as diferentes apropriações e racionalidades aplicadas à implementação do sistema Prüm no seio da União Europeia.

O guião de entrevista (Anexos 1, 2 e 3) foi elaborado pela coordenadora do projeto Exchange – Professora Doutora Helena Machado –, em estreita colaboração com os membros doutorados da equipa. A coordenadora do projeto elaborou o formulário de consentimento informado (Anexo 4) e o folheto informativo (Anexo 5) entregue no momento da entrevista aos participantes do estudo. As entrevistas foram realizadas pelos diferentes membros da equipa. A transcrição das entrevistas foi realizada por profissionais externos contratados para o efeito.

As entrevistas realizadas no âmbito do projeto Exchange foram conduzidas na língua dominada pelo/a entrevistador/a e entrevistado/a, tendo sido maioritariamente conduzidas em inglês (87) e as restantes em português (28), espanhol (3) e alemão (6). As entrevistas em espanhol e alemão foram traduzidas, por profissionais externos, para português. A tradução das transcrições procurou respeitar integralmente o conteúdo e sentido expressos pelo/a entrevistado/a.

As entrevistas realizadas no âmbito do projeto Exchange perfazem um total de 124 entrevistas, com um total de 140 entrevistados/as baseados/as em 25 países diferentes. A distribuição dos/as entrevistados/as pelos respetivos países encontra-se representada na tabela 1. Para a presente tese foram analisadas as entrevistas dos Pontos de Contacto Nacionais: 37 entrevistas com 47 entrevistados/as; as entrevistas dos geneticistas forenses

dos dois estudos de caso: 19 entrevistas; e as entrevistas dos *stakeholders* dos dois estudos de caso: 25 entrevistas com 26 entrevistados. Nos próximos subtópicos será explanada a caracterização dos entrevistados/as cujas entrevistas foram selecionadas para a análise empírica da tese.

Tabela 1-Distribuição dos/as entrevistados/as por país – projeto Exchange

Países	Entrevistas	Entrevistados/as
Alemanha	14	17
Áustria	1	1
Bélgica	2	3
Bulgária	1	3
Chipre	2	2
Eslováquia	1	1
Eslovénia	4	5
Espanha	4	5
Estónia	1	1
Finlândia	1	2
França	3	3
Hungria	3	3
Irlanda	1	1
Letónia	2	3
Lituânia	2	2
Luxemburgo	1	2
Malta	3	3
Noruega	2	2
Países baixos	11	13
Polónia	12	14
Portugal	29	30
Reino unido	16	16
República checa	3	3
Roménia	2	2
Suécia	2	2
Outros ³⁰	1	1
Total	124	140

Entrevistas realizadas no âmbito do projeto EXCHANGE (2015-2019).

Pontos de Contacto Nacionais (NCPs) do sistema Prüm

O relatório mais recente sobre o progresso da implementação do sistema Prüm, datado de setembro de 2019, indica que há 25 Estados-Membros da União Europeia operacionais ao nível de troca de DNA (Council of the European Union, 2019a). No âmbito do projeto Exchange, foram conduzidas 37 entrevistas com 47 profissionais em 22 países

³⁰ Foi realizada uma entrevista a um representante da União Europeia.

operacionais ao nível da troca de DNA no sistema Prüm. Para a realização da presente tese, foram selecionadas todas as entrevistas realizadas aos NCPs do sistema Prüm, pelo que os valores totais da tese coincidem com os do projeto Exchange. A informação sobre formação profissional, organização, tipo de trabalho e atividades relacionadas com o sistema Prüm dos/as entrevistados/as encontra-se detalhada na tabela 2.

O regulamento da União Europeia do sistema Prüm estabelece que, para efeitos de partilha de dados pessoais, cada Estado-Membro deve designar um Ponto de Contacto Nacional cujas responsabilidades serão regidas pela legislação nacional aplicável (Decisão 2008/615/JHA). Os profissionais que atuam como NCPs são atores centrais no sistema Prüm, genericamente, conduzem as atividades diárias que permitem a partilha transnacional de dados pessoais e ocupam uma posição crucial nos processos de tomada de decisão. Em particular, as pessoas que atuam como NCPs têm como responsabilidades organizar e implementar os procedimentos e conexões necessárias para realizar partilhas automáticas de dados com outras bases de dados (enviando e recebendo informações); realizar testes com outros países parceiros; e gerir e reportar correspondências de DNA (*hits/matches*).

Não obstante, as responsabilidades dos NCPs do sistema Prüm podem variar entre os países de acordo com as diferentes estruturas organizacionais e subsequente legislação nacional. Para além disso, diferentes países atribuem a custódia das bases de dados forenses de perfis de DNA a diferentes entidades, desde autoridades judiciais até forças policiais (Santos, 2017). Portanto, os indivíduos que operam como NCPs podem ter formação profissional e educacional diferenciada, e tanto podem trabalhar em laboratórios forenses como em forças policiais (tabela 2.).

Conforme mencionado anteriormente, cada país tem autonomia para definir como atribuir diferentes papéis e responsabilidades aos profissionais forenses que atuam como Pontos de Contato Nacionais do sistema Prüm. Como tal, em alguns países apenas uma pessoa é responsável pelas operações associadas à partilha transnacional de dados de perfis de DNA, enquanto noutros países duas ou mais pessoas podem estar envolvidas nessas tarefas. Nesta última situação, sempre que diferentes indivíduos demonstraram disponibilidade para participar no estudo procedeu-se à realização de uma entrevista semiestruturada.

O guião das entrevistas (Anexo 1³¹) abrangeu os seguintes temas: visões e experiências acerca da implementação do sistema Prüm ao nível nacional e europeu, opiniões sobre os propósitos e contribuições do sistema Prüm, questões éticas levantadas pela troca transnacional de dados de perfis de DNA, expectativas de desenvolvimento e inovação ao nível das tecnologias de DNA e perceções relacionadas com a comunicação com o público em geral.

Tabela 2- Caracterização dos NCPs entrevistados em países operacionais

Formação profissional	
Biologia, ciência forense e campos relacionados	20
Polícia	11
Direito	9
Tecnologias e sistemas informáticos	5
Outros	2
Organização	
Policial	27
Institutos forenses	20
Tipo de trabalho	
Cooperação policial internacional	22
Laboratorial	21
Tecnologias e sistemas informáticos	4
Atividades relacionadas com Prüm	
NCP 1	26
NCP 2	17
Assistentes de NCP1	3
NCP 1 e NCP 2	1
Número total de participantes	47

Fonte: Entrevistas realizadas no âmbito do projeto EXCHANGE (2015-2019).

Geneticistas forenses

Para além das entrevistas conduzidas com NCPs, foram também realizadas entrevistas a profissionais da genética forense na União Europeia. Tendo em consideração a diversidade da comunidade de genética forense (Cole, 2013), a amostra do projeto

³¹ Os anexos disponibilizados respeitam a língua oficial do projeto Exchange, por este motivo encontram-se todos em inglês.

Exchange agrega geneticistas forenses, isto é, indivíduos que trabalham em casos criminais e são empregados por um laboratório forense; e investigadores, ou seja, indivíduos empregados por universidades ou institutos forenses cuja ocupação profissional principal é pesquisa de laboratório cientificamente controlada com aplicação no âmbito da ciência forense. Não raras vezes estas posições são intermutáveis na medida em que profissionais da genética forense na União Europeia podem simultaneamente desenvolver atividades de investigação e aplicar ciência forense em casos criminais específicos. Para a presente tese foram apenas utilizadas as entrevistas realizadas em Portugal (14) e no Reino Unido (5), por serem os casos de estudo selecionados para o efeito, sendo que todos os geneticistas forenses desempenham funções em universidades ou institutos forenses (tabela 3.)

O guião das entrevistas (Anexo 2) abordou os seguintes temas: a organização de serviços de genética forense no país em que o/a participante esteve baseado/a; pontos de vista sobre a troca transnacional de dados de perfis de DNA na União Europeia; representações sobre as perceções públicas sobre genética forense; e opiniões e experiências relativas a desenvolvimentos e inovações ao nível das tecnologias de DNA, tais como, inferência fenotípica, sequenciamento paralelo massivo e pesquisa familiar.

Tabela 3- Caracterização dos geneticistas forenses em Portugal e no Reino Unido e organização onde desempenham funções

País	
Portugal	14
Reino unido	5
Organização	
Policial	0
Universidades / institutos forenses	19
Número total de participantes	19

Fonte: Entrevistas realizadas no âmbito do projeto EXCHANGE (2015-2019).

Stakeholders dos estudos de caso

Por fim, foram ainda entrevistados outros *stakeholders* relevantes no âmbito do sistema Prüm em Portugal e no Reino Unido. A análise destes estudos de caso visou, por um lado, compreender as diferenças entre países com diferentes posicionamentos em relação à partilha transnacional de dados de perfis de DNA, no contexto do sistema Prüm. Por outro lado, almejou também explorar as formas como diferentes legislações nacionais, recursos

científicos variados, distintas tradições ao nível da utilização de ciência forense e desiguais posicionamentos ao nível do envolvimento político com o sistema Prüm produzem configurações específicas que impactam de forma significativa as dimensões sociais, culturais, éticas, regulatórias e políticas do uso de tecnologias de DNA para utilização forense na União Europeia.

Os critérios que conduziram à escolha dos dois países foram os seguintes:

1. Estar operacional no âmbito do sistema Prüm ou não; data de entrada na UE e situação relativa ao espaço Schengen;
2. Legislação nacional relacionada com a base de dados forense e possível impacto de Prüm;
3. Nível de desenvolvimento da base de dados forense e proporção da população incluída;
4. Condições socioeconómicas distintas e capacidade operacional, logística, tecnológica e científica desigual dos laboratórios e das tecnologias de informação e comunicação;
5. Debates públicos (existentes ou inexistentes) relativos à expansão do uso de tecnologias de DNA para fins de investigação criminal.

Em Portugal foram realizadas 13 entrevistas a 14 *stakeholders* e no Reino Unido foram aplicadas 11 entrevistas (tabela 4.). As categorias profissionais mais representadas na amostra são as que correspondem à entidade de supervisão/ regulação com 10 entrevistados/as e à categoria professor(a) universitário(a)/investigador(a) com 6 entrevistados/as. Em número mais reduzido têm-se 4 entrevistados/as pertencentes a órgãos de investigação criminal, seguidos da categoria Organizações Não Governamentais (ONGs) e empresas privadas, ambas com 2 entrevistados/as. Apenas um/a entrevistado/a representa a categoria de legislador(a) (tabela 5.). A maioria dos/as entrevistados/as possui formação em áreas do Direito (13) e da Biologia e campos relacionados (8) (tabela 6.).

O guião das entrevistas (Anexo 3) abrangeu os seguintes temas: perspetivas e desafios colocados pela implementação do sistema Prüm; opiniões sobre os riscos e benefícios do sistema Prüm; expectativas de desenvolvimento e inovação ao nível das tecnologias de DNA. Uma vez que este estudo é guiado pela *grounded theory*, novos tópicos e conceitos abordados entrevistas foram sendo incorporados, sempre que pertinente.

Tabela 4-Número de stakeholders em Portugal e no Reino Unido³²

País	
Portugal	14
Reino unido	11
Número total de participantes	25

Fonte: Entrevistas realizadas no âmbito do projeto EXCHANGE (2015-2019).

Tabela 5-Categoria profissional dos stakeholders

Categoria profissional	
Organizações não governamentais direitos humanos	2
Entidade supervisão/regulação	10
Professor(a) universitário(a)/investigador(a)	6
Legislador	1
Órgãos de investigação criminal	4
Empresas privadas	2
Número total de participantes	25

Fonte: Entrevistas realizadas no âmbito do projeto EXCHANGE (2015-2019).

Tabela 6-Formação educacional dos stakeholders

Formação educacional	
Direito	13
Biologia e campos relacionados	8
Ciências políticas	1
Sem informação	2
Outros	1
Número total de participantes	25

Fonte: Entrevistas realizadas no âmbito do projeto EXCHANGE (2015-2019).

2.3. Procedimentos éticos

O protocolo de entrevistas e os procedimentos foram conduzidos sob os regulamentos éticos do Conselho Europeu de Investigação (*European Research Council – ERC*). Todas as entrevistas realizadas no decorrer do projeto Exchange foram sujeitas a um procedimento de consentimento dividido em duas etapas:

³² Excluindo NCPs e geneticistas forenses

1. No momento do primeiro contacto com os potenciais participantes foram facultadas cópias do termo de consentimento informado e da ficha informativa (Anexos 4 e 5).

2. No momento da entrevista foi solicitado aos/às entrevistados/as que lessem e assinassem um termo de consentimento informado (Anexo 4) no qual os direitos dos/as participantes foram esclarecidos, nomeadamente, o direito de aceder aos seus dados, incluindo a transcrição da entrevista e o seu direito de abandonar o estudo a qualquer momento, mesmo após a realização da entrevista e da respetiva transcrição.

As entrevistas ocorreram nos locais de trabalho dos/as entrevistados/as ou em locais escolhidos pelo/a participante. Os/as entrevistadores/as – membros da equipa Exchange – tomaram notas para ajudar a orientar as suas questões durante as entrevistas, bem como para auxiliar na reflexão realizada pós-entrevista. Após a conclusão das mesmas, os/as entrevistadores/as reviram as anotações e realizaram relatórios, partilhados com toda a equipa, sobre as condições das entrevistas, reflexões acerca das mesmas, bem como sobre sugestões de questões e tópicos que poderiam ser abordados em entrevistas e/ou análises subsequentes.

Em média, as entrevistas tiveram uma duração média de noventa minutos. Todas as entrevistas, exceto duas, mediante pedido do/a entrevistado/a, foram gravadas digitalmente, transcritas na íntegra e anonimizadas. A transcrição foi realizada por membros da equipa Exchange e por serviços externos de transcrição contratados. Em ambos os casos, foi implementado um rigoroso acordo de confidencialidade e privacidade, assinado por ambas as partes (membros da equipa Exchange e os profissionais contratados para a realização das transcrições) (Anexo 6). Uma vez que, informação potencialmente capaz de identificar os/as entrevistados/as foi captada nas gravações de áudio, apenas a equipa Exchange e os serviços de transcrição tiveram acesso aos ficheiros digitais. Os dados foram armazenados no escritório da equipa (com acesso restrito) e sempre que foram partilhados via internet utilizou-se um serviço de encriptação (*AES Crypt*). Todas as medidas de segurança foram, portanto, postas em prática para garantir a proteção física dos dados (informação digital e impressa). De forma a proteger o anonimato dos/as entrevistados/as cada país foi identificado por meio de uma letra e cada entrevistado/a por

via de um número. Essa forma de anonimização é utilizada em todos os extratos que constam na presente tese.

2.4. Análise das entrevistas

No âmbito da análise de dados, as entrevistas foram sistematicamente comparadas, contrastadas, sintetizadas e codificadas por tema e categoria temática seguindo os princípios norteadores da *grounded theory* (Charmaz, 2006; Clarke, 2005), e foram interpretadas usando uma abordagem qualitativa de análise de conteúdo (Mayring, 2004). Adotou-se um processo de análise comparativa constante entre dados empíricos e enunciações teóricas (Strauss & Corbin, 1990; Charmaz, 2009). De forma geral, em vez de colocar a ênfase na dedução de hipóteses a partir de teorias pré-existentes, procurou-se desenvolver indutivamente categorias de análise e conceitos enraizados nos dados (Strauss & Corbin, 1990: 48–50; Charmaz, 2009: 17).

CAPÍTULO 3. ANÁLISE EMPÍRICA

3.1. Perspetivas de Pontos de Contacto Nacionais do sistema Prüm

O desenvolvimento e a aplicação de ‘novas tecnologias de vigilância’ (Bygrave, 2002; Lyon 2001) estão diretamente relacionados com o aumento da preocupação com questões de pendor securitário, nomeadamente, a ‘segurança nacional’ dos Estados-Membros. Esta situação deve-se, em grande medida ao crescimento de alguns tipos de criminalidade, nomeadamente, o terrorismo (Lyon, 2001). As ‘novas biotecnologias de vigilância’ podem ser enquadradas numa versão híbrida do que Marx (2006) define enquanto vigilância *hard* e *soft*, uma vez que, genericamente, podem adquirir modalidades mais ou menos invasivas para o corpo do cidadão. As tecnologias biométricas forenses vieram permitir a identificação de indivíduos suspeitos de terem cometido um crime. O reconhecimento da importância destas tecnologias conduziu à criação de bases de dados nacionais de perfis genéticos de DNA para fins de investigação criminal. Realce-se que estas bases de dados devem responder a critérios coesos no que concerne à proteção de dados das pessoas que nelas constam, sendo o objetivo último o de as enquadrar legalmente no direito à privacidade e proteção de dados de todos os cidadãos (Machado et al., 2015, p. 62).

Os novos desafios à ‘segurança nacional’ dos Estados-Membros trouxeram o que Hert (2005) entende como a luta contra o terrorismo e o crime organizado. Uma das soluções encontradas pelos países para lidar com crescentes ameaças à segurança pública foi o aumento de sistemas tecnológicos de identificação humana, entre os quais a partilha transnacional de informação de bases de dados nacionais. Neste cenário, destaca-se o designado sistema Prüm. Este sistema teve início em 2005, por via de assinatura do Tratado de Prüm, por sete Estados-Membros, e teve como objetivo permitir o acesso mútuo às bases de dados nacionais de perfis genéticos, impressões digitais e registos de veículos (Kierkegaard, 2008, pp. 243-244; O’Neill, 2010). Em 2008 deu-se a transposição do Tratado para a lei da União Europeia ficando conhecido como sistema Prüm (Jornal Oficial da União Europeia, 2008). Deste modo, tornou-se obrigatório o acesso mútuo e a comparação de perfis de DNA entre as bases de dados dos países da UE (Machado & Granja, 2019b, p. 3). Os últimos dados, de 2018, sobre o processo de implementação do sistema Prüm mostram que existem 24 Estados-Membros operacionais (Council of the European Union, 2018a; Machado & Granja, 2018).

O presente capítulo verte da análise empírica de 37 entrevistas semiestruturadas realizadas a 47 entrevistados. Ao nível da formação profissional os participantes, na sua maioria, são da área da 'biologia, ciência forense e campos relacionados' (20), da 'Polícia' (11) e do 'Direito' (9). Em número mais diminuto, cinco entrevistados pertencem à categoria 'Tecnologias e sistemas informáticos' e os restantes 2 foram enquadrados na categoria de 'Outros'. Relativamente à organização de pertença, 27 desempenham atividades no âmbito de instituições policiais e os restantes 20 entrevistados pertencem a institutos forenses. Por fim, quanto às atividades levadas a cabo ao nível do sistema Prüm, foram entrevistados 26 NCP1, 17 NCP2, 3 assistentes de NCP1 (para efeitos de análise foram agregados aos NCP1) e um entrevistado responsável pela posição de NCP1 e NCP2. Genericamente, o guião de entrevista aplicado focou-se nas opiniões sobre 1) a implementação do sistema Prüm tanto ao nível nacional como europeu, 2) os propósitos e contribuições do sistema Prüm, 3) as questões éticas levantadas pela partilha transnacional de informações sobre os perfis de DNA, 4) as expectativas de desenvolvimento e inovação ao nível das tecnologias de DNA e, por fim, 5) as perceções relacionadas à comunicação com o público em geral.

3.2. Representações dos Pontos de Contacto Nacionais do passo 1 (NCP1)

Benefícios e utilidade do sistema Prüm

Os Pontos de Contacto Nacionais (NCP's) responsáveis pelo passo 1 (ou *step 1*) do sistema Prüm, com um perfil tipicamente laboratorial, partilham, *grosso modo*, as mesmas perspetivas no que concerne aos benefícios e à utilidade deste sistema transnacional de partilha de dados. Tal como denotam os entrevistados, a partilha de informação para auxílio em investigação criminal já existia previamente, no entanto, era realizada caso-a-caso (Hufnagel & McCartney, 2015; Machado & Granja, 2019a; McCartney, 2014b; McCartney et al., 2011; Williams & Johnson, 2008). Atualmente, os desenvolvimentos tecnológicos ao nível do armazenamento e fluxo de dados (Goos et al., 2015, p. 56; Mostert et al., 2017; Nissenbaum, 2010, p. 36) conduziram ao aumento das iniciativas estatais que visam garantir a partilha de informações forenses entre Estados-Membros (McCartney, 2017). Neste sentido, o sistema Prüm pode ser elencado como exemplo das iniciativas mencionadas. Sendo que os participantes consideram que o sistema Prüm veio conferir uma maior celeridade aos processos de cooperação policial substituindo as formas tradicionais de partilha de informação entre países (Van Camp & Dierickx, 2007; Williams & Johnson, 2008).

O envio de cartas, de emails ou o pedido de informação através do sistema internacional de solicitação de informação (cartas rogatórias) são exemplos de modos tradicionais de cooperação policial. Deste modo, o sistema Prüm é apresentado, por parte dos entrevistados, como uma forma de empoderamento (*empowering*; Prainsack & Toom, 2010) que permite aos Estados-Membros maior rapidez e capacidade de resposta na resolução de crimes.

“Prüm é apenas um sistema de transmissão que deve aumentar a rapidez da cooperação policial já existente. Antes de Prüm os dados eram transmitidos, mas apenas através de métodos clássicos: cartas e email.” [M01]

“Eu penso que Prüm acelerou bastante as comparações internacionais, porque nós temos – eu gosto de lhe chamar turismo criminal transfronteiriço do País A e País B, e o País C é um desses países; Prüm acelerou [as comparações internacionais], uma vez que o sistema internacional de pedidos é um processo bastante longo. Isto tornou as coisas mais rápidas.” [E01]

Um outro aspeto realçado pelos entrevistados responsáveis pelo passo 1 tem que ver com a capacidade e a necessidade de combate contra a criminalidade transfronteiriça e o terrorismo (Hert, 2005). Desafios que se intensificaram na sequência da celebração do Tratado de Schengen (1997) que visou a promoção da livre circulação de indivíduos entre países europeus através da abertura das fronteiras do Estados-Membros. Deste modo, a criação do sistema Prüm foi uma das respostas estatais encontradas para garantir que a investigação criminal se mantivesse a par desta nova conjuntura europeia (Amankwaa, 2019; Santos, 2017; Santos & Machado, 2017). No primeiro extrato, o entrevistado denota, precisamente, esta noção de que a investigação criminal deve acompanhar o aumento da plasticidade das fronteiras de modo a conseguir atuar com eficácia (Sulca, 2017).

A par com a rapidez e a capacidade de resposta ao crime transfronteiriço, um dos entrevistados referiu como benefício do sistema Prüm a sua potencial utilidade ao permitir procurar correspondências em todas as bases de dados forenses de perfis de DNA dos Estados-Membros. Por outras palavras, realça-se que, o sistema Prüm, enquanto instrumento contemporâneo de biopolítica (Pugliese, 2012, p. 2), pode apresentar-se como

uma mais valia para a resolução de crimes perpetrados por indivíduos que não constam nas bases de dados dos países onde os crimes ocorreram. Deste modo, a existência de ‘uma base de dados virtual da UE’ (Human Genetics Commission, 2009, para 5.10) com informações forenses disponíveis entre todos os Estados-Membros tem sido ladeada por argumentos que enfatizam a importância do bem-coletivo e de uma maior segurança tanto ao nível nacional, como ao nível europeu (Costa & Nunes, 2001; Heinemann et al., 2012; Lynch et al., 2008; Maciel & Machado, 2014, p. 143; Schwartz-Marín & Wade, 2015). As narrativas presentes nos extratos encontram-se em linha com uma noção otimista da criação de bases de dados e mecanismos de partilha de informações genéticas enquanto potenciadores do combate e da prevenção da criminalidade (Gilbert, 2007). Esta posição é também consonante com os resultados obtidos por Machado (2011) e Maciel e Machado (2014). Dito isto, através dos excertos apresentados, compreende-se a influência das tecnologias e das redes sociais em que estas circulam na transformação da utilização das bases de dados enquanto ‘local uncertainties’ (Star, 1985) com uma utilização pontual para ‘global certainties’ através do seu uso mais amplo e regular (Williams & Johnson, 2004b, p. 206).

“No meu ponto de vista, isto foi uma necessidade, porque depois de entrarmos na UE temos as fronteiras abertas para a circulação de cidadãos europeus; é muito fácil de entender que a criminalidade e as pessoas que cometem crimes irão ultrapassar as fronteiras geográficas, políticas ou administrativas e irão para outros países.” [J01]

“Tornou possível a resolução de crimes impossíveis de solucionar ao nível nacional, porque as pessoas não estão na vossa base de dados, mas estão noutras bases de dados. Portanto, penso que o benefício principal é que podem ser solucionados mais crimes ao nível nacional.” [A01]

Os benefícios do sistema Prüm supramencionados estão intimamente relacionados com outro aspeto de relevância para os entrevistados, nomeadamente, a automatização de processos. Esta automatização ocorre, principalmente, ao nível do passo 1 onde apenas se verifica se há ou não a existência de uma correspondência de perfis de DNA entre Estados-Membros (McCartney, 2017; McCartney et al., 2011) Tal como Machado e Granja (2019a)

denotam o sistema Prüm é encarado como uma ferramenta que através da automatização de procedimentos vem acelerar a comunicação na cooperação policial (p. 9). Do mesmo modo, os entrevistados encaram o sistema Prüm como um ‘descomplicador’ dos sistemas tradicionais de cooperação policial que tinham de ser acionados mesmo antes de se saber se existia informação com potencial interesse para a investigação criminal.

“Antes de Prüm, para comparar um perfil [de DNA], tinha de ser enviado um pedido internacional que tinha de passar pela INTERPOL e por um juiz; e não se sabia se se iria obter algum resultado. Com Prüm, tem-se automaticamente uma resposta, o conhecimento de que há ali qualquer coisa, e pode dar-se início à elaboração do processo para o juiz se existir alguma coisa de interessante. É realmente uma forma de ganhar tempo, de ganhar dinheiro...” [H01]

“Antes de Prüm era apenas por comissão rogatória, mas o problema é que assim tinham de enviar várias comissões rogatórias para cada país. Agora, é mais fácil: há um perfil de DNA que pode ser enviado automaticamente para todos os países e, em seguida, recebe-se um *hit* ou um *no-hit*. Mas depois, se se quiser mais informação é preciso uma comissão rogatória. Mas o primeiro passo é automático.” [I01]

Passo 1 do sistema Prüm

A divisão do processo de partilha de informação à escala transnacional em dois passos (*step 1* e *step 2*) é uma das medidas implementadas no âmbito do sistema Prüm que visa reforçar a proteção de dados dos indivíduos cujos dados são partilhados (Prainsack & Toom, 2010). Genericamente, quando há a confirmação de um *hit* de perfis de DNA entre os Estados-Membros – *step 1* –, segue-se a partilha de mais informações – *step 2* – sobre o indivíduo suspeito (nome, morada, crime cometido, etc.). Esta partilha é realizada de acordo com a lei de proteção de dados dos países envolvidos, bem como com os critérios mínimos estabelecidos pela Comissão Europeia para a proteção de dados (Machado & Silva, 2010; Prainsack, 2010; Prinsack & Toom, 2010). No entanto, os dois passos são percecionados de diferentes modos de acordo com os profissionais entrevistados. Em particular, o *step 1* é comumente encarado como um procedimento obrigatório e estandardizado que não

levanta questões com relevância acrescida para a partilha de dados. Deste modo, o caráter estandardizado desta fase do sistema Prüm entalha a partilha de dados na ótica da *administrative objectivity* (Lynch, 2013) onde apenas são elencados, pelos entrevistados, aspetos de ordem técnica e protocolar, como se pode observar nos extratos apresentados.

“O *step 1* tem a ver só com a comunicação de *hit, no hit*. Isso, a nível nacional, tem funcionado bem. Não temos tido qualquer problema. Digamos que é um passo pacífico, é preciso controlar de vez em quando a ver se as coisas estão a correr bem, mas em si as coisas funcionam bem.” [N10]

“A primeira parte é obrigatória: cada país tem de ter a sua base de dados de DNA disponível para todos. Isso é Prüm.” [A01]

As questões da estandardização da prática científica no sistema Prüm continuam a ser alvo de discussão (Johnson & Williams, 2007; Jordan & Lynch, 1998; Machado & Granja, 2018; McCartney, 2014b). No entanto, os procedimentos científicos encontram-se suficientemente consolidados para permitir a partilha de dados genéticos entre Estados-Membros (Johnson & Williams, 2007, p. 112). No primeiro extrato o entrevistado enfatiza que a estandardização inerente ao passo 1 permite que este seja completamente automático e, conseqüentemente, mais rápido, duas das características que facilitam o início do processo de partilha de informações. As narrativas de ambos os entrevistados situam-se numa ótica da neutralização das subjetividades do passo 1 (Machado & Granja, 2018). Sendo que os Pontos de Contacto Nacionais responsáveis pelo *step 1* não trabalham diretamente com dados identificáveis. A estrutura do sistema em dois passos vem, deste modo, favorecer a perceção de que a privacidade dos indivíduos que constam nas bases de dados está protegida.

“É feito automaticamente, totalmente automático.” [O02]

No segundo extrato, a reflexão feita pelo entrevistado continua subjacente à neutralidade aparente dos *standards* e *softwares*, condição fortemente contestada em vários trabalhos por não abarcar os possíveis enviesamentos decorrentes dos contextos

loais e das relações de poder entre os atores da rede (Botzem & Dobusch, 2012, p. 23; Timmermans & Epstein, 2010, p. 70). Tal como Machado e Granja (2018) denotam, o fluxo de informação aquando do passo 1 é remetido para a impessoalidade numérica e para ‘black-boxed ICT systems’ (p. 254; Porter, 1995).

“Em princípio todos implementam o passo um do mesmo modo. Usam software diferente – em alguns casos usam o CODIS e noutros usam os seus próprios dados – mas as mensagens que são partilhadas são as mesmas, não interessa o tipo de programa que é usado, o resultado é o mesmo.” [A01]

Desafios e riscos do sistema Prüm

Uma das dimensões em análise decorrente das entrevistas aos NCPs pauta-se pelas suas narrativas acerca dos desafios e potenciais riscos do sistema Prüm. Deste modo, emergiram vários pontos que se encontram balizados entre os potenciais desafios à implementação do sistema Prüm e os riscos que este pode apresentar para as liberdades dos cidadãos inseridos nas bases de dados forenses de DNA. Em relação à implementação do sistema Prüm, os entrevistados identificaram como mais relevantes os que se prendem com a capacidade de resposta nacional às especificidades da partilha transnacional de dados na UE. Em particular, os profissionais responsáveis pelo passo 1 remeteram para problemas de ordem técnica relacionados com:

- 1) Os sistemas informáticos (IT) utilizados para o contacto entre bases de dados;

“São maioritariamente problemas técnicos: fazer o contacto entre bases de dados. Porque nem todos os países têm o CODIS: alguns países têm uma espécie de programa local.” [E01]

- 2) Deficiências no enquadramento legal das bases de dados de DNA ao nível local;

“A lei [da base de dados] era de 1999 e não permitia a partilha internacional de DNA. Portanto, tivemos de adaptar a nova lei. E, finalmente, foi publicada em

2011, mas tivemos de esperar por um *higher decree*. Por isso, não foi possível começar antes.” [I01]

3) A falta de recursos humanos que consigam responder em tempo útil aos pedidos realizados em Prüm;

“Nós não temos pessoal que chegue, por isso, temos algum atraso nas respostas, mas não mais do que um mês, se compararmos com outros países dos quais não obtemos nenhuma resposta durante meio ano.” [S03]

4) E, a falta de recursos económicos para equipar os laboratórios forenses e criar uma estrutura para a bases de dados de DNA, uma vez que, nem todos os países da União Europeia possuíam uma base de dados com estas características;

“Há países que não tinham base de dados, tiveram que a criar, tiveram que fazer todo esse processo. Pronto, depois é todo aquele processo de ter que ter a base de dados, primeiro ter legislação, criar a base de dados, depois todo o conjunto de formalidades que é preciso para fazer a troca de perfis.” [N10]

“O custo de Prüm ao nível do DNA depende se o país tem uma prática forense estabelecida na área e apenas precisa de instalar equipamentos de computação e pessoal adicional ou se tem de construir tudo do zero.” [T01]

Os pontos enunciados pelos responsáveis pelo passo 1 destacam, essencialmente, questões de ordem técnica no que concerne à implementação do sistema Prüm (McCartney, 2017, p. 169). O enfoque na tecnicidade deste tipo de sistema tecnológico foi uma das tendências identificadas por alguns autores que enfatizam a escassa reflexão, de indivíduos com um perfil tipicamente laboratorial, sobre a complexidade das relações de confiança, controlo e segurança entre países (*idem*). Sendo que a confiança entre Estados-Membros é o vetor potenciador da cooperação transnacional (Hufnagel & McCartney, 2015, 2017). Segundo Perras (2017), os problemas que têm como origem a comunicação entre diferentes programas, tal como identificado no ponto (1), devem-se ao facto de não existir uma

harmonização total de todos os aspetos da partilha transnacional de dados (p. 227). Pelo que, o que se observa é uma ‘aproximação’ que oferece aos países um maior controlo nas suas escolhas em relação aos programas a utilizar (*idem*). Deste modo, os Estados têm poder de decidir as regras pelas quais funcionam tendo apenas a obrigação de corresponder aos *standards* mínimos estabelecidos pela União Europeia. No ponto (2) encontra-se latente, mais uma vez, uma narrativa que está em linha com o conceito de *administrative objectivity*, na medida em que as controvérsias em torno da partilha transnacional de dados foram encerradas com base em correções jurídicas (Lynch, 2013, p. 65).

Nos pontos (3) e (4) conseguem discernir-se as lógicas transnacionais para a criação de sistemas estandardizados, principalmente nas regras estabelecidas em relação ao sistema Prüm. Tal como os entrevistados denotam, verifica-se um acesso desigual a recursos humanos e económicos, pelo que nem todos os países acederam à participação do processo de negociação do sistema Prüm (Bellanova, 2008; Cochoy, 2004; Hallström, 2004; Schmidt & Werle, 1998; Werle & Iversen, 2006). Dito isto, tal como a literatura refere, no plano transnacional é exigida uma maior alocação de recursos do que ao nível nacional (Smith 2005, 2008). Sendo que, tendo por base a assimetria de poderes no campo de forças transnacional, apenas os países e atores sociais com elevados níveis de legitimidade e de alocação de recursos estão em condições de impactar a governação do sistema Prüm (Hancher & Moran, 1989; Young, 1994). Nesta linha, McCartney e colegas (2011) defendem no seu trabalho que a falta do envolvimento democrático de todos os Estados-Membros na criação do sistema Prüm levou ao retorno do que os autores chamam de ‘diplomacia tradicional interestadual’, pois os países com mais recursos (logo mais poder) acabaram por impor o Tratado de Prüm aos restantes países, com menos poder de influência através das Decisões Prüm. Alertando-se para o facto de que a assimetria de poderes que caracterizou a criação do sistema Prüm conduz à perda da sua legitimidade, aceitabilidade e viabilidade (*idem*).

Relativamente aos riscos que um sistema como o de Prüm pode acarretar para as liberdades civis dos cidadãos os entrevistados apresentaram perspetivas mais heterogéneas. As suas noções a este respeito podem ser enquadradas em dois grupos, ainda que não sejam estanques. Por um lado, os entrevistados que efetivamente reconhecem que o sistema pode apresentar certos riscos no decorrer da sua utilização, nomeadamente, a possibilidade de se verificarem falsos positivos que podem implicar pessoas inocentes no

decorrer de uma investigação criminal. Esta posição, notoriamente residual, pode ser situada no pragmatismo biométrico (Williams & Johnson, 2004b) por dar conta da relevância da legitimidade dos contextos da utilização de DNA forense por parte da polícia (p. 217). A percepção dos entrevistados a este respeito encontra-se em linha com a ideia de que a comparação automatizada de perfis de DNA pode gerar falsos negativos e falsos positivos devido ao aumento substancial de perfis partilhados num sistema transnacional como o de Prüm (Machado & Granja, 2019a, p. 9; McCartney, 2014a; Kierkegaard, 2008, p. 245; Prainsack & Toom, 2010, p. 1124). Sendo que, tal como se observa no extrato, se se verificar a ocorrência de falsos positivos podem estar em causa as liberdades civis dos cidadãos, como também a eficácia e a credibilidade das autoridades responsáveis pela aplicação da lei (Hustinx, 2010). Um falso positivo ocorre quando uma correspondência é validada, mas uma análise mais detalhada (em laboratório ou por via da investigação) permite concluir que o resultado está errado (Machado & Granja, 2018; McCartney, 2014b). Onde, um falso positivo pode ter origem na contaminação da prova em laboratório como em erros na interpretação dos perfis genéticos.

“Eu penso que os maiores desafios são os falsos positivos, podem causar muitos problemas se a polícia os levar a sério. E muitas pessoas inocentes podem ser afetadas por isso.” [B01]

Por outro lado, a maioria dos profissionais revela uma postura mais próxima do minimalismo genómico (Williams & Johnson, 2004b) minimizando os potenciais riscos às liberdades civis dos cidadãos. Reiteraram a existência de regulamentos e leis que visam tornar claro o tipo de utilização expectável do sistema Prüm, por exemplo, que cidadãos podem ou não ser inseridos nas bases de dados de perfis de DNA. Portanto, *grosso modo*, entendem que não existem riscos na utilização da partilha transnacional de informação de perfis de DNA para fins de investigação criminal. Nesta situação, a legislação e os protocolos do sistema Prüm atuam enquanto elemento harmonizador dos contextos nacionais. A reflexão sobre os processos de standardização que levaram à formulação destes documentos é escassa e está relacionada com a invisibilidade característica da criação de *standards* (Lampland & Star, 2009, p. 11), pelo que só ocorre questionamento em relação a uma destas normas quando é necessário proceder à sua modificação (Thévenot, 2009, p.

795). As narrativas dos entrevistados em torno dos desafios do sistema Prüm são permeadas por um entusiasmo associado à automatização de procedimentos a par da conceção de que a existência de protocolos/leis asseguram a legalidade e legitimidade de todo o processo de partilha transnacional:

“Não vejo muitos riscos desde que se tenham algumas diretrizes que mencionem o que pode ser incluído e o que não pode ser incluído.” [Y01]

“Particularmente quando temos a certeza que a informação apenas será usada para combater o crime.” [C02]

Como observado nos extratos acima apresentados, a neutralização pela estandardização dos riscos e desafios da partilha de dados transnacional enquadra-se na cultura epistémica (Knorr-Cetina, 1999) dos entrevistados, com um perfil maioritariamente laboratorial. Deste modo, a diluição dos riscos do sistema Prüm, por parte dos participantes, encontram-se em linha com os pressupostos da *administrative accountability* (Lynch, 2013, p. 60). Onde a utilização de material genético em meio judicial se pauta por uma ‘objetividade administrativa’ que encontra nos registos, protocolos e leis a sua legitimidade (*idem*). Por esse motivo, as ‘diretrizes’ assumem uma dimensão ritualista integrada e tornada invisível na cadeia de custódia da prova genética. Sendo que, os entrevistados, na sua maioria, se refugiam no percurso administrativo da prova enquanto garante de objetividade e integridade de todo o sistema Prüm (Lynch, 2002, p. 218).

Neste ponto, os entrevistados acrescentaram que, para o cidadão cumpridor da lei, o sistema Prüm será certamente uma ferramenta útil para combater o crime a que estão sujeitos. Este discurso revela-se polarizado entre a categoria do bom cidadão que cumpre a lei e do ‘mau’ cidadão que comete crimes não deixando espaço para a reflexão sobre a erosão de direitos, como por exemplo, o direito à presunção da inocência (Kreissl et al., 2015, p. 161; Marx, 2006, p. 5).

“Não [há riscos]. Como um cidadão comum que segue as regras, penso que é uma boa ferramenta para lidar com os crimes. Quer dizer, pessoas comuns estão a

ser burladas ou atingidas por coisas. Há tantas leis que apenas protegem o suspeito ou o condenado, mas nunca a vítima.” [U02]

O passo 2 do sistema Prüm, onde pode ou não ocorrer a partilha de informações (Prainsack & Toom, 2010), foi apresentado como um dos desafios à cooperação policial e judiciária devido ao tempo de resposta (Machado & Granja, 2019a; Matos, 2019; McCartney, 2014b). Neste sentido realçam-se vários aspetos, que no entender dos entrevistados podem tornar-se potenciais obstáculos à partilha de dados através do sistema Prüm e devem ser reajustados no futuro. Um dos pontos mais elencados respeito do passo 2 foi o da necessidade de se otimizar o tempo de resposta desta fase do processo que é, por norma, a parte mais morosa da partilha transnacional de informação no sistema Prüm. Sendo que uma das soluções apresentadas passa pela gestão prioritária dos dados de DNA e da informação policial ao nível da sua partilha entre Estados-Membros.

“Penso que é muito importante acelerar o segundo passo. Não faz sentido que se espere por uma resposta durante 3 meses. Temos de o acelerar e já existem tratados que cheguem, como a *Swedish initiative*, entre outros. Portanto, isto não é feito através da regulação, faz-se ao dar outro valor, ou prioridade, às correspondências de DNA e à partilha de informação policial.” [O02]

O sistema Prüm enquanto elemento de standardização técnico-científica pretendeu auxiliar a cooperação transnacional entre instituições através da neutralização das diferenças legais, culturais e políticas dos diferentes Estados-Membros (Lampland & Star, 2009, pp. 4-5; Prainsack & Toom, 2010, 2013). Deste modo, o fluxo da informação está intimamente dependente da criação de *standards* que procuram garantir a interoperabilidade (Balzacq et al., 2006; Bigo, 2008, p. 105; De Hert & Gutwirth, 2006; McCartney 2014a, 2014b) entre as bases de dados nacionais de perfis de DNA. Porém, a harmonização tecnológica e científica tem como principal desafio a diversidade legislativa dos países da União Europeia (Prainsack, 2010, p. 22; Prainsack & Toom, 2013). Os entrevistados referiram que a demora supramencionada dos procedimentos do passo 2 está diretamente relacionada com o facto de a partilha transnacional de informação estar dependente dos contextos regulatórios nacionais que carecem de standardização. A falta

de consensos a este nível pode também estar relacionada com a falta de compatibilidade entre bases de dados (McCartney, et al., 2011). Um outro aspeto relevante do passo 2 é o facto de interferir com o princípio da disponibilidade estipulado pelo programa de Haia. Isto porque, com a estrutura de dois passos, à partida, será partilhada menos informação através de um acesso indireto que pode resultar na decisão de não partilhar os dados solicitados pelos países (*idem*).

“Infelizmente, o passo 2 não foi regulado com o Tratado de Prüm original e isso permitiu muita influência ao nível nacional, e é por isso que não está a funcionar adequadamente.” [P03]

A desarmonização desta etapa permite que a custódia da base de dados de perfis de DNA seja diferente entre países, estas podem encontrar-se sob a alçada do Ministério da Justiça ou sob o controlo do Ministério da Administração Interna. Neste sentido, os entrevistados realçaram que os modelos de cooperação são diferenciados consoante o tipo de custódia da base de dados (Machado & Granja, 2019a, pp. 11-12; Matos, 2019, p. 158). As narrativas expressas pelos profissionais revelam que os procedimentos envolvidos na partilha de informação através das autoridades judiciais são mais lentos do que ao nível policial, contribuindo para a morosidade do step 2 do sistema Prüm.

“No meu país o DNA não é uma informação policial. Portanto, o que acontece agora é que se outro país quiser ter mais informação sobre uma pessoa, têm de nos enviar uma comissão rogatória. Isto é muito complicado, porque se fosse do departamento policial, telefonavam e perguntavam: ‘Pode dar-me o nome?’ E estava feito. Mas no meu país não é assim.” [I01]

Diferentes práticas de cooperação transnacional entre autoridades policiais e judiciais podem, assim, constituir-se como um obstáculo à troca de informações para fins de investigação criminal (Machado & Granja, 2019a; Matos, 2019). Dito isto, os órgãos policiais operam sob uma racional que dá primazia à inteligência com base no acesso alargado a todas as informações disponíveis, com o objetivo de acelerar a investigação criminal (Innes, Fielding, & Cope, 2005). Por outro lado, o modo de ação das autoridades judiciais é visto

como mais restritivo porque é um processo mais lento e, geralmente, resulta partilha de informação mais reduzida (Machado & Granja, 2019a; Matos, 2019). A escassa experiência em cooperação transnacional atribuída às autoridades judiciais são, de acordo com os entrevistados, um dos obstáculos para a fluidez da comunicação (*idem*). Sendo que estas autoridades não estão tipicamente envolvidas na fase investigativa. Portanto, a lógica e o *modus operandi* das duas entidades são diferentes, pois, também elas possuem diferentes objetivos no sistema de justiça criminal. Por um lado, as forças policiais procuram resolver e identificar os indivíduos com condutas criminais. Por outro, os órgãos judiciários têm a responsabilidade de julgar as pessoas que cometeram, ou não, os crimes. Como Machado e Granja (2019a) afirmaram:

“The clash between these different working methods (...) therefore undermines the principle of reciprocity and trust that police professionals claim is needed within transnational cooperation and prevents the construction of relationships based on trust with their judicial counterparts.” (p. 14)

Um outro aspeto elencado pelos entrevistados tem que ver com a diferença de critérios entre os Estados-Membros em relação às correspondências (*hits*) que devem ser consideradas para a partilha de dados para fins de investigação criminal (*follow-up*). Esta situação é mais uma vez reveladora da flexibilidade de critérios desta fase do processo de partilha. Neste sentido, o passo 2 é um procedimento opcional e cabe aos países ou aos profissionais responsáveis pela decisão escolher os critérios que melhor se adequam ao seu contexto. Por um lado, observou-se que certos países fazem o seguimento de todas as correspondências positivas que recebem através do sistema Prüm. Por outro lado, constatou-se que existem países que realizam a seleção das correspondências através, por exemplo, do tipo de crime que envolveu a recolha do perfil de DNA.

“Todos [os crimes]. A teoria é que não existem crimes menores. Porque se deixarmos passar um crime menor, ele pode escalar para um maior. Então, se o apanharmos à primeira, não há outros.” [H01]

“Não há nenhuma obrigatoriedade em usar uma correspondência e seguir para o segundo passo. E também se pode dizer: ‘Só faço trabalho extra se for um crime grave: um homicídio, uma violação ou algo do género, o resto ignoro’.” [A01]

Eficácia e futuro do sistema Prüm

Uma das questões centrais relativa à eficácia real do sistema Prüm tem que ver com a dificuldade em medir os rácios entre os *hits* positivos e os casos criminais que, efetivamente, culminam numa condenação em tribunal. Esta situação está relacionada com vários aspetos, sendo um dos principais a falta de *feedback* a que os profissionais responsáveis pelo *step* 1 têm acesso. Atendendo a esta situação, a legitimidade do sistema Prüm pode ser colocada em causa, pois não se podendo verificar estatisticamente variáveis que meçam o número de *hits* que terminam na abertura de um caso judicial, estão em causa princípios legais (Harbo, 2010; Prainsack & Aronson, 2015; Williams & Johnson, 2004a; Williams & Wienroth, 2014). Neste sentido, na sua maioria, os entrevistados revelaram que os polícias e os Procuradores não têm por hábito dar conta do resultado final da investigação. Sendo que, uma das estratégias reveladas por um/a dos/as entrevistados/as passa pela procura de algum tipo de resposta nos média, quando sabe tratar-se de um caso mediatizado.

“Os processos depois são encaminhados para os tribunais, para o Ministério Público, para os juízes, para o responsável do caso, a partir daí perdemos o rasto.” [N10]

“Procuro nos média os resultados do meu próprio trabalho, porque não recebo nenhuma resposta por parte da polícia, a menos que seja um caso criminal de elevado perfil com conferências de imprensa. Mas, normalmente, leio no jornal que um criminoso foi apanhado porque teve uma correspondência com a base de dados de DNA e depois tento encontrar o caso a que se referem [risos].” [A01]

A falta de comunicação entre as instituições envolvidas no processo criminal – laboratórios, polícia, tribunal – torna difícil a compreensão da eficácia quantitativa do sistema Prüm. Um *hit* em Prüm, como supramencionado, não tem qualquer obrigatoriedade

de ser levado em conta pela polícia nacional, pelo que se não existir um modo eficiente de comunicar os resultados pode estar em risco a proporcionalidade de todo o sistema. A legitimização e proporcionalidade de um sistema de vigilância como o sistema Prüm está dependente da sua eficácia, pelo que se o sistema não estiver a ser eficaz pode não ser legítimo para a finalidade para a qual foi pensado.

Considerando os aspetos enunciados pelos participantes do estudo nos tópicos supramencionados, foi pedido aos entrevistados que refletissem sobre o futuro do sistema Prüm. As respostas foram no sentido da necessidade de um esforço conjunto para colmatar os atuais riscos e desafios do sistema de partilha de dados. Em particular, 1) a utilização de mais marcadores na análise dos perfis de DNA, de modo a dissipar a probabilidade de se verificarem falsos positivos com a conexão plena entre todos os países. 2) A possível inclusão, no sistema Prüm, de países que se encontram fora da União Europeia. 3) A necessidade de tornar a cooperação entre os Estados-Membros mais eficaz pressionando os países que ainda não estão totalmente operacionais no sistema Prüm a regularizarem a sua situação. E, por fim, 4) a premência da harmonização que vem garantir que todos os países têm práticas técnico-científicas semelhantes.

“Espero que as pessoas comecem, finalmente, a usar mais *loci* e que comece a ser utilizado em mais países. Fora da Europa também não será problemático, assim não são precisos os acordos bilaterais que são processos manuais e podem ter vários erros. Prüm, com a automatização, é uma boa plataforma.” [S03]

“Pessoalmente, esperaria uma cooperação mais efetiva de todos os 28 países membros. Na minha opinião, o Parlamento [Europeu] não fez grandes ajustes a este respeito. O Conselho tem de assegurar os passos necessários. Num primeiro nível, colocar mais pressão nos países problemáticos. Porque não podemos tolerar um atraso de 5 anos em certos países, sem razão nenhuma.” [P03]

“Penso que temos de nos harmonizar e que todos devemos fazer a mesma coisa.” [W02]

A aceitação generalizada dos *standards* do sistema Prüm é condicionada pela existência de infraestruturas físicas, culturais e técnico-científicas ao nível dos contextos nacionais. A pressão aos ‘países problemáticos’, que ainda não procederam à total implementação do sistema Prüm, referida pelos entrevistados tem que ver com a falta de harmonização de certas práticas. Sendo de realçar que se a implementação de um *standard* ao nível nacional encontra obstáculos, ao nível transnacional pode ser um processo ainda mais exigente. No sistema Prüm esta premissa é concretizada nas diferentes práticas, ferramentas e legislações locais/nacionais (Timmermans & Berg, 1997), como referido ao longo da presente secção. A tentativa de harmonização da União Europeia em matéria de cooperação policial e judiciária tem como base a dimensão flexível dos *standards* que procuram permitir a compatibilidade entre contextos nacionais diferentes (*idem*). Um outro aspeto fundamental para a execução do sistema Prüm que pode ser entendido enquanto uma ‘rede massiva de circulação de medidas’ (Timmermans & Epstein, 2010, p. 80) tem que ver com a constante incompletude dos *standards* (*idem*, p.81). Deste modo, torna possível que estes se alterem e reajustem às novas epistemologias locais/nacionais, exemplo desta dimensão é a necessidade de se aumentar o número de *loci* em utilização com o aumento do número de perfis de DNA comparados transnacionalmente.

O sistema Prüm tem materializado várias dificuldades nos processos de estandardização transnacional no plano da cooperação policial e judiciária. A dimensão rígida da estandardização está associada, por exemplo, aos formulários e procedimentos de recolha e comparação de perfis de DNA, na medida em que os laboratórios que performam os testes têm de ser acreditados pela ISO17025. Atividades desenvolvidas, principalmente, ao nível do *step* 1. Por outro lado, a dimensão flexível da estandardização está mais presente na segunda etapa do sistema Prüm, pois a partilha de dados está inteiramente dependente da interpretação da legislação dos países envolvidos. Para que o sistema Prüm continue em atividade é necessário que os Estados-Membros encontrem o equilíbrio entre a rigidez e a flexibilidade dos *standards* adotados. Permitindo, em simultâneo, a sua adaptação aos vários contextos sociais locais e às suas especificações (Timmermans & Epstein, 2010, p. 81).

Privacidade e proteção de dados no sistema Prüm

Os entrevistados foram questionados a respeito das medidas de proteção de dados implementadas no âmbito do Sistema Prüm através da descrição das práticas implementadas para a proteção dos dados das pessoas incluídas nas bases de dados de perfis de DNA. Genericamente, a maioria das respostas dados pelos profissionais entrevistados encontram-se em linha com o que Michael Lynch chama de ‘objetividade administrativa’ (Lynch, 2013, p. 60). No contexto do sistema Prüm, a ‘objetividade administrativa’ permite a credibilização da prova de DNA através da existência de um conjunto de procedimentos burocráticos, nomeadamente, relatórios e protocolos estandardizados (*idem*). Deste modo, a estandardização de procedimentos atua enquanto agente neutralizador dos riscos através dos números (Porter, 1995). As respostas dos participantes foram no sentido de considerarem que as medidas de proteção de dados e privacidade são adequadas e asseguradas por um conjunto de protocolos estandardizados. Este tipo de narrativa encontra-se em linha com o minimalismo genómico (Williams & Johnson, 2004b) numa retórica que coloca de parte o debate ético mais aprofundado sobre o carácter da informação presente no DNA forense (p. 215). Sendo que a confiança na utilização forense do DNA no sistema Prüm é justificada com medidas de segurança exclusivamente de carácter técnico.

De acordo com as narrativas dos entrevistados, a privacidade das pessoas que constam nas bases de dados de perfis de DNA para fins de investigação criminal é salvaguardada através de várias etapas. Os entrevistados foram unânimes ao afirmar que é possível rastrear todas as pessoas que têm acesso aos dados presentes na base de dados através de um sistema restrito com *login*. Por outras palavras, este sistema permite guardar todas as alterações efetuadas na base de dados, bem como o funcionário cujas credenciais de acesso são intransmissíveis. Ainda a este respeito, também o grau de acesso e de autorização para alterar a base de dados pode variar de acordo com o país.

“Sim, temos um *login*. Por isso, consegue ver-se quando se inseriu um perfil, quando se removeu um perfil, (...) quem inseriu o perfil e quando o inseriu.” [W02]

“Obviamente nem todos os policias têm acesso à nossa base de dados. Têm de ter um motivo para aceder. (...) Por exemplo, a secretária do nosso departamento

não tem acesso à base de dados, só tem acesso ao ficheiro sobre o qual vai trabalhar. O acesso será especificado para cada trabalhador de acordo com as suas tarefas e necessidades.” [Y01]

“Todos os especialistas do Centro de Ciência Forense têm acesso [à base de dados]. Podem inserir perfis, pesquisá-los e calcular o que quiserem. Mas não podem fazer mais nada. Apenas os administradores têm mais acesso.” [B01]

Os recursos informáticos (IT) são, na maioria das vezes, encarados pelos entrevistados como fundamentais para garantir a proteção dos dados pessoais, não só através de um sistema de *logins*, como também da utilização de redes de e-mail (ou outros canais de comunicação semelhantes) encriptadas. A encriptação apresenta-se, neste contexto, como uma opção viável para evitar que as trocas de comunicação entre as entidades nacionais e internacionais sejam *hackeadas*. Situação que coloca em risco todos os dados partilhados no âmbito transnacional e, por conseguinte, a privacidade e proteção de dados dos indivíduos envolvidos.

“Eu acho que é [seguro], porque só se podem trocar perfis de DNA que estão encriptados e são enviados através de uma rede segura, a TESTA.” [A01]

“E se recebermos informação de DNA dos laboratórios esta é enviada através de emails encriptados.” [I01]

Um outro aspeto realçado por diversas vezes pelos entrevistados, tem que ver com a existência de leis de proteção de dados que lhes fornecem esclarecimentos sobre o que pode ou não ser partilhado no sistema Prüm. Desta forma, grande parte dos entrevistados referiu que as leis nacionais se encontram adequadas para o propósito, referindo ainda que, na maioria dos países, o sistema Prüm não veio alterar significativamente as leis sobre proteção de dados. Neste ponto a reflexão sobre a privacidade no sistema Prüm continua a permear-se de narrativas instrumentalizadas que se refugiam em ‘protocolos’ legais como fontes de ‘objetividade administrativa’ (Lynch, 2013, p. 60).

“O meu país tem uma lei de proteção de dados relativamente forte há já uns anos. O que nos disseram foi que, genericamente, é tão forte que não houve necessidade de implementar medidas extra de proteção de dados.” [P03]

“A legislação de proteção de dados é bastante rigorosa no meu país. (...) Só precisamos de manter a lei e seguir os termos estipulados por Prüm: cada país deveria possuir leis específicas para a proteção de dados e já as tínhamos.” [C02]

A supervisão das atividades realizadas no âmbito do sistema Prüm, como se pode observar nos excertos, é semelhante e operada, na maior parte das vezes, pelo mesmo órgão encarregue de supervisionar as atividades da base de dados nacional de perfis de DNA. No entanto, esta opção, tomada por alguns dos Estados-Membros, colide com um dos aspetos críticos do sistema Prüm em relação à escassa supervisão ética do processamento de informações pessoais, principalmente, ao nível nacional (Gonçalves & Jesus, 2012, p. 123). Ainda a este respeito, vários autores têm, igualmente, chamado a atenção para a falta de supervisão ética também ao nível transnacional da partilha de dados para efeitos de investigação criminal (Hufnagel & McCartney, 2015; McCartney, 2010, 2014a; McCartney et al., 2011; Prainsack & Toom, 2010, 2013). Relativamente à supervisão ética ao nível das práticas laboratoriais, para a produção e análise dos perfis de DNA, o controlo é realizado através da obediência a códigos deontológicos e duplas confirmações entre colegas. Sendo que o sucesso da partilha transnacional de dados genéticos, no sistema Prüm, passa pelo recurso a métodos e protocolos de interpretação estandardizados de modo a que possam ser preservados e disseminados nas várias comunidades científicas nacionais (Lynch, 2002, p. 207). Atendendo a que para além dos protocolos que garantem as ‘boas’ práticas científicas que preservam a integridade da prova de DNA, os profissionais de laboratório também devem responder em conformidade com o código deontológico do seu instituto.

“[A entidade de supervisão] possui uma lista com o nome de pessoas que pediram para serem removidas da base de dados e verifica se já o foram.” [H01]

“As atividades relacionadas com a base de dados e com o Instituto são supervisionadas pelo órgão nacional de supervisão. O Ministério do Interior tem o

seu próprio departamento de controlo e inspeção, que também realiza verificações.”
[T01]

“Depois a nível ético, é assim as pessoas que trabalham no instituto têm um código deontológico, faz parte das suas funções, não podem andar a divulgar informação nesse conjunto de pressupostos. Implementações legais, acho que é o termo correto.” [N10]

Como se pode observar, as narrativas dos Pontos de Contacto Nacionais para o passo 1 em matéria de privacidade carecem de uma reflexão aprofundada dos dilemas éticos e das questões de privacidade e proteção de dados no sistema Prüm. Neste sentido, a privacidade foi apresentada numa perspetiva minimalista (Williams & Johnson, 2004b) que se cingiu aos pontos técnicos, protocolares, informáticos e à existência formal de entidades de supervisão (Lynch, 2012) como garante da proteção de dados. Ou seja, as controvérsias em torno da privacidade e da proteção de dados do sistema Prüm, enunciadas na literatura, são, para os entrevistados um ponto “closed (...) within their circle of expertise” (Machado & Granja, 2018, p. 18). Sendo que a maioria destes profissionais possui um perfil laboratorial, o seu posicionamento encontra-se em linha com a neutralização e mitigação das questões éticas da partilha de dados de DNA característica da sua cultura epistémica (Knorr-Cetina, 1999).

Interoperabilidade entre bases de dados com diferentes finalidades

O exponencial desenvolvimento das tecnologias de informação permitiu a criação de infraestruturas técnico-científicas como os biobancos e as bases de dados de perfis de DNA para fins de investigação criminal. Foi notória a evolução da capacidade de armazenamento de dados, o aumento da velocidade do fluxo de informação partilhada e a simplificação no cruzamento de dados através da harmonização de sistemas (Goos et al., 2015, p. 56; Mostert et al, 2016; Nissenbaum, 2010, p. 36). A proliferação dos biobancos e das bases de dados forenses desenvolveu-se a par com preocupações acerca da manutenção dos sistemas e as práticas de utilização deste tipo de infraestruturas. Sendo que, as vulnerabilidades mais prementes encontram-se, num primeiro momento, relacionadas com

as medidas de proteção de dados e a privacidade dos indivíduos cujos dados genéticos se encontram inseridos nestes sistemas (Mostert et al, 2016).

A existência de biobancos e de bases de dados para fins de investigação criminal é justificada com base na premissa de que ambos têm potencial para oferecer benefícios sociais quer no âmbito da medicina, quer no âmbito criminal (Machado & Silva, 2015a, p. 820). Por um lado, os biobancos têm como objetivo assegurar o cuidado com a saúde pública através da luta contra doenças que afetem a sociedade (Gaskell et al., 2013). Por outro lado, as bases de dados forenses foram criadas sob a expectativa de que poderiam desempenhar um papel fundamental na segurança da sociedade através da identificação eficiente de pessoas suspeitas de cometerem crimes (Cho & Sankar, 2004; Patyn & Dierickx, 2010; Santos, Machado, & Silva, 2013; Van Camp & Dierickx, 2008). Como consequência das diferentes racionais de atuação, a informação que consta nestes dois tipos de bases de dados é diferente. Nos biobancos constam os dados de qualquer cidadão que pretenda ser voluntário num estudo médico ou dador de material biológico, ao passo que numa base de dados criminal verifica-se a seleção de elementos da sociedade que devem ter os seus dados inseridos na mesma (Machado & Silva, 2015a, p. 820).

Uma outra diferença incremental tem que ver com a localização física das suas infraestruturas. Os hospitais ou instalações de saúde semelhantes são as instituições nomeadas para acolher os biobancos que recolhem e armazenam amostras de tecido humano e informação médica do indivíduo que podem ser úteis para pesquisa em determinadas doenças. Porém, as bases de dados para fins de investigação criminal encontram-se sob a custódia de entidades policiais ou judiciais e pretendem a recolha e armazenamento de perfis de DNA de suspeitos, ofensores condenados, vítimas, entre outros. Neste caso os perfis são comparados com amostras de uma cena de crime com o objetivo último de levar a pessoa que perpetuou um crime à justiça.

De modo a apreender as perceções dos entrevistados a respeito da interoperabilidade entre os biobancos e as bases de dados forenses o guião de entrevista incluiu uma questão a este respeito. Dito isto, as narrativas a respeito deste tópico foram heterogéneas e situaram-se entre a recriminação total deste tipo de prática e a recetividade à mesma. Neste sentido, as reflexões éticas e técnico-legais realizadas pelos entrevistados revelaram diferentes construções sociais de noções de prestação de contas, bem público, risco, privacidade e solidariedade. A categorização apresentada nesta secção inspirou-se no

trabalho de Granja e Machado (2019) sobre as controvérsias éticas da pesquisa familiar. As autoras serviram-se das categorias de ‘regulating through exceptionality’ e ‘regulation through expansion’ para classificar os posicionamentos de diversos *stakeholders* sobre a prática da pesquisa familiar em dois contextos nacionais (Granja & Machado, 2019). Por um lado, a categoria ‘regulating through exceptionality’ abarca as perspectivas que enfatizam a utilização de pesquisa familiar em casos criminais de alto perfil de acordo com as circunstâncias, o tipo e os riscos sociais associados ao crime (*idem*, p. 1077). Por outro lado, na ‘regulation through expansion’ inserem-se as narrativas que, apesar de reconhecerem os riscos e potencialidades da prática, remetem para baixos índices de controvérsia na sua utilização.

No âmbito da presente tese propõe-se uma adaptação à categorização avançada pelas autoras supramencionadas de modo a adequar as mesmas ao objeto em estudo, neste caso, a interoperabilidade entre biobancos e bases de dados forenses. As categorias que serão apresentadas são fundamentadas tendo por base a análise dos dados recolhidos através das entrevistas realizadas. Portanto, num primeiro extrato encontram-se as narrativas que se inserem na categoria de ‘negação técnico-legal’. De modo genérico, os entrevistados incluídos nesta categorização possuem respostas que se pautam pela justificação da não interoperabilidade tendo por base motivos de ordem técnica e/ou legal carecendo, na maioria das vezes, de uma reflexão ética a respeito desta prática. No extrato, em particular, pode observar-se que a interoperabilidade não é equacionada devido a questões técnicas que se relacionam com a inexistência de práticas standardizadas entre diferentes laboratórios (médicos e forenses). Constata-se, deste modo, a carência de uma reflexão mais robusta que equacione as questões éticas que podem estar em causa com a interoperabilidade entre biobancos e bases de dados forenses, nomeadamente, questões de privacidade, proteção de dados, altruísmo, entre outras.

“Penso que no meu país seria impossível [a interoperabilidade] do ponto de vista técnico e nunca iriam permitir este tipo de investigação cruzada, porque têm diferentes regras de funcionamento. Uma das regras é que os laboratórios [médicos] não usam a norma ISO17025, têm outro tipo de norma, que não é compatível.” [J01]

Uma outra franja dos entrevistados posicionou-se na categoria da ‘interoperabilidade pela excecionalidade’, como o próprio nome indica, nesta categoria enquadram-se as perspetivas que estão a par com a interoperabilidade condicionada, restrita a casos específicos, entre biobancos e bases de dados forenses. Nesta categoria torna-se mais perceptível o questionamento ético desta prática, em concreto, no que concerne ao direito à privacidade, a erros de análise dos dados e ao possível mau uso da informação recolhida. Em particular, no primeiro extrato, verifica-se uma maior atenção aos princípios gerais da proteção de dados em relação à criação de bases de dados, remetendo a discussão para os quatro princípios básicos da proteção de dados, nomeadamente, limitação da finalidade, minimização de dados, proporcionalidade e controlo de dados (Brown, 2009; European Data Protection Supervisor, 2006; Gamero et al., 2008; Gonçalves, 2018; Gonçalves & Jesus, 2012, 2013; Harbo, 2010; Hert, 2005; IRISS, 2012). Dito isto, entende-se que para que a interoperabilidade possa ocorrer, ainda que de modo condicionado, seria necessário proceder à criação de novas bases de dados que se iniciassem com os preceitos corretos para permitir este tipo de prática. O segundo extrato também se encontra na categoria da ‘interoperabilidade pela excecionalidade’ pois, segundo o entrevistado, a interoperabilidade entre biobancos e bases de dados forenses é aceitável desde que se especifiquem as situações em que esta pode ser realizada. Sendo que se assiste novamente a uma reflexão mais aprofundada a respeito dos problemas que podem advir do recurso a esta prática. Em particular, foram realçadas questões associadas a possíveis interpretações erradas dos dados, bem como ao uso desadequado de dados sensíveis por parte da polícia (Amankwaa, 2018; Gamero et al., 2008; Liu, 2013, p. 13; Wallace et al., 2014, p. 58).

“Tudo depende do propósito para o qual a base de dados foi criada. (...) A legislação de proteção de dados é bastante restritiva e rigorosa, na medida em que, para se criar uma base de dados é necessário ter uma lei que o permita e, no âmbito dessa lei, é preciso referir qual é o motivo da sua criação, os seus propósitos e o que se pretende fazer com os dados obtidos.” [C02]

“Um médico pode fazer uma interpretação errada de dados específicos para fins forenses e, ao mesmo tempo, um polícia pode fazer um mau uso de informação

de âmbito médico. Não, não acho que seja uma boa ideia misturar. (...) Acho que pode ser utilizado, mas em casos específicos.” [H01]

Em número diminuto encontram-se os entrevistados cujas perspectivas foram classificadas como ‘negação pela finalidade’. Nesta categoria encontram-se as narrativas que, por um lado, são totalmente desfavoráveis a qualquer tipo de manifestação desta prática e, por outro lado, apresentam uma reflexão ética mais robusta e fundamentada. Nos extratos que se seguem os entrevistados justificam o seu posicionamento com base nos princípios de solidariedade, ponto fulcral para a manutenção de biobancos, e de confiança, nomeadamente, a confiança depositada pelos utilizadores nas instituições, sejam elas médicas ou policiais (Chadwick & Berg, 2001; Machado & Silva, 2015a; Prainsack & Buyx, 2013). Esta reflexão encontra-se em linha com a literatura sobre os princípios pelos quais um biobanco deve ser regido, respetivamente, a voluntariedade, o altruísmo e a solidariedade do dador (Bexellius, Hoyer, Lynoe, 2007; Forsberg, Hansson, Eriksson, 2009; Gamero et al., 2008; Machado & Silva, 2015; Wilson-Kovacs, Wyatt, Hauskeller, 2012). Sendo que, estes princípios implicam que, no ato da recolha e do armazenamento do material biológico, não ocorra coação física nem psicológica do indivíduo, contrariamente ao que pode ocorrer numa base de dados forense. Em suma, a interoperabilidade é encarada como disruptiva para a solidariedade, privacidade e confiança dos cidadãos.

“Sou contra isso [interoperabilidade]. Nós tivemos um caso em que isso foi pedido e eu me recusei a fazê-lo, disse não. Somos um país pequeno e, se começarmos a fazer este tipo de coisas, as pessoas perderão a confiança não só nas operações relacionadas com polícia, como também com a investigação (médica). Por exemplo, vão recusar-se a participar.” [W02]

“Na minha opinião, a interoperabilidade das bases de dados médicas e forenses seria um enorme risco de disrupção dos direitos de privacidade.” [T01]

A categoria ‘interoperabilidade pela expansão’ abarca as narrativas cujo enfoque é o da transparência total e, portanto, remete para aceitação da interoperabilidade entre biobancos e bases de dados forenses. A este posicionamento subjazem argumentos

relacionados com o facto de que o cidadão cumpridor da lei não tem nada a esconder - “nothing to hide, nothing to fear” (Crossman, 2008, p. 116). Neste caso em particular, a expansão é operada através de uma racional de culpabilização e suspeição generalizada onde a não participação voluntária neste tipo de prática pode trazer consigo perdas morais significativas para os lesados. Perdas morais que podem ter várias consequências para os implicados, nomeadamente, a (re)categorização de um indivíduo enquanto ‘mau cidadão’ e a erosão do direito à presunção de inocência e da dúvida razoável (Kreissl et al., 2015, p. 161; Lyon, 2014, p. 10; Marx, 2006, p. 5). No entanto, no diálogo abaixo apresentado, os entrevistados tentam de algum modo situar a sua posição num ideal-tipo de país que assegura por completo o uso correto da informação. Contudo, remeter unicamente para o nível macro (Estatual) da proteção da privacidade dos indivíduos envolvidos numa possível interoperabilidade deixa de parte todas as potenciais ameaças ao nível micro, por exemplo, na atuação das polícias ou na má interpretação de dados médicos.

“Como cientistas forenses, acredito que estamos muito abertos a todo o tipo de partilha entre bases de dados. Acredito que se não se é um criminoso, não é necessário esconder nada. Mas é claro que pode ser uma forma ingénua de pensar.” [Y01-02]

“Se não se tem nada a esconder não deve haver problema.” [Y01-01]

“Eu não em importo de estar em bases de dados. Mas nunca se sabe o que vai acontecer à informação, é preciso ter a certeza de que se vive num país onde se sabe que a informação não será dada para [fins desadequados].” [Y01-02]

Neste diálogo foram elencados vários pontos fundamentais para a discussão acerca da interoperabilidade dos biobancos com as bases de dados criminais. Desde logo, na situação de acesso forense a uma base de dados médica, os quatro princípios gerais de proteção de dados podem não ser cumpridos pelas entidades que os detêm. Isto porque na limitação da finalidade está patente a ideia de que os dados pessoais recolhidos devem servir finalidades específicas, explícitas e legítimas. Deste modo, os dados não devem ser utilizados para fins diferentes dos que motivaram a sua recolha estando em causa a

potencial ‘function creep’ (Dahl & Sætnan, 2009; Liu, 2013, p. 66, 87) da base de dados consultada. O princípio da minimização dos dados pretende garantir que não seja recolhida informação pessoal para além da necessária. Porém se as autoridades policiais acederem a um biobanco encontram-se perante um manancial de informações que podem não ser importantes para a investigação criminal. Portanto, também a proporcionalidade fica em causa, na medida em que pode não se conseguir assegurar que os dados recolhidos sejam “adequados, relevantes e não excessivos” para os fins para os quais serão utilizados. Por fim, o controlo dos dados – a supervisão – não é realizado do mesmo modo no âmbito médico e no âmbito da esfera criminal, pelo que pode não se conseguir assegurar uma correta supervisão dos dados acedidos (Brown, 2009; European Data Protection Supervisor, 2006; Gamero et al., 2008; Gonçalves & Jesus, 2012, 2013; Harbo, 2010; Hert, 2005; IRIS, 2012).

Um aspeto a realçar da análise das entrevistas, para além dos já mencionados, pauta-se pelo facto de a grande maioria das respostas serem conduzidas sob a premissa de que a interoperabilidade ocorreria no sentido do acesso forense a biobancos, isto é, para fins de investigação criminal. Deste modo, não foi possível chegar a conclusões acerca das perspetivas dos entrevistados em relação ao acesso médico a bases de dados forenses. Uma possível explicação para esta reflexão unilateral acerca da interoperabilidade pode estar relacionada com o tipo de trabalho desenvolvido pelos profissionais que foram entrevistados no âmbito do presente estudo. Como referido no início da secção, os NCP 1 possuem um perfil tipicamente laboratorial e desempenham funções na esfera da investigação criminal e cooperação policial transnacional. Na figura 1. encontram-se esquematizadas as categorias propostas, no decorrer da secção, relativamente às perspetivas acerca da interoperabilidade com as suas respetivas características. A figura 2. Remete para as dimensões das respostas fornecidas pelos participantes do estudo, pelo que na base da pirâmide encontram-se os entrevistados cuja categoria se denomina por ‘interoperabilidade pela expansão’, na medida em que, a sua perceção acerca desta prática se limita exclusivamente ao acesso forense a biobancos para fins de investigação criminal. A categoria ‘negação técnico-legal’ é remetida para dimensão dos requisitos, pois as respostas careceram de uma abordagem mais inovadora e híbrida que transcenda os aspetos técnicos que são de algum modo solucionáveis através de alterações administrativas (Lynch, 2013). Por fim, as categorias ‘interoperabilidade pela excecionalidade’ e ‘negação pela finalidade’

enquadram-se no topo da pirâmide, na medida em que se observou, por parte dos entrevistados, uma reflexão mais aprofundada daqueles que poderiam ser os obstáculos à interoperabilidade. Contudo, é fundamental que se compreenda que a categorização não deve ser considerada inflexível, pois poderá ser possível a existência de indivíduos com um perfil híbrido em relação à prática da interoperabilidade entre biobancos e bases de dados forenses.

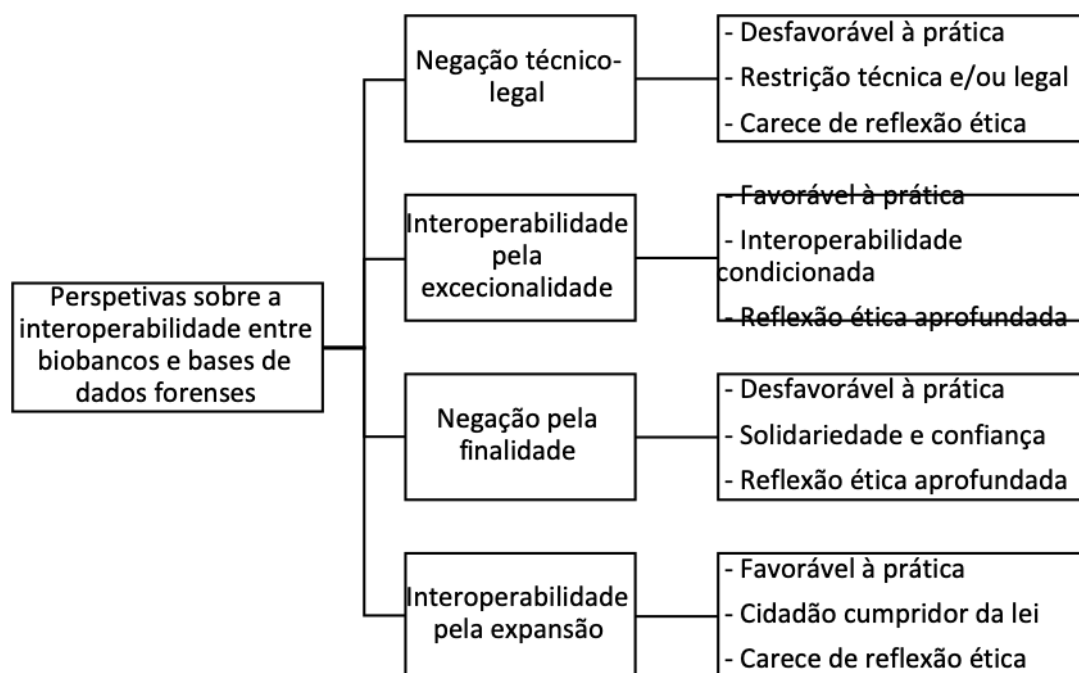


Figura 1 - Categorização das perspectivas sobre a interoperabilidade entre biobancos e bases de dados forenses



Figura 2 - Dimensões de resposta sobre as perspectivas sobre a interoperabilidade entre biobancos e bases de dados forenses

3.3. Representações dos Pontos de Contacto Nacionais do passo 2 (NCP2)

Benefícios e utilidade do sistema Prüm

A necessidade do aprofundamento da cooperação policial e judiciária entre os Estados-Membros teve como principal alavanca o carácter simultaneamente global e localizado das ameaças terroristas e da criminalidade transfronteiriça. Neste cenário, uma das soluções encontradas para a melhor articulação da cooperação foi, como supramencionado, a implementação de um sistema em rede dedicado à partilha de dados – o sistema Prüm (Decisão 2008/615/JAI, 2008 e Decisão 2008/616/JAI, 2008). Este sistema veio agilizar o combate à criminalidade transfronteiriça e ao terrorismo através da identificação e controlo de populações e indivíduos ‘suspeitos’ (Lyon, 2007; Marx, 1988 sobre categorias de suspeição). No entanto, a União Europeia tem-se debatido com o dilema do equilíbrio entre a segurança coletiva e a proteção de direitos humanos fundamentais, como a privacidade e a proteção de dados (Heinemann et al., 2012; McCartney, 2014b; Toom et al., 2016). O equilíbrio enunciado possui uma componente fortemente flexível e parcial, na medida em que quando colocado sob pressão a decisão tem sido frequentemente a de favorecer a segurança em detrimento da privacidade (Cavoukian, 2001, p. 1).

Os profissionais responsáveis pelo *step 2* do sistema Prüm possuem, na sua maioria um perfil policial e de cooperação transnacional. Os pontos elencados pelos entrevistados em relação aos benefícios avançados pela criação do sistema Prüm encontram-se em linha com as disposições iniciais da Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras. De modo genérico, os NCPs responsáveis pelo passo 2 perspetivam o sistema Prüm enquanto um instrumento de empoderamento (*empowering*; Prainsack & Toom, 2010) que subjaz o imaginário europeu a respeito do ideal-tipo da cooperação policial e judicial. Dito isto, o sistema Prüm veio “franquear uma nova dimensão na luta contra a criminalidade”, bem como promover “novas abordagens de investigação aos Estados-Membros” (considerando 12, Decisão 2008/615/JAI do Conselho). De modo complementar, o considerando 24 da mesma Decisão realça o carácter comunitário da União Europeia ao referir que “a[s] melhoria[s] do intercâmbio de informações na UE, não podem ser suficientemente realizad[a]s pelos Estados-Membros isoladamente, devido à natureza transfronteiras da luta contra a

criminalidade e das questões de segurança”. Em concreto, os benefícios do sistema Prüm apontados pelos entrevistados operacionalizam estas disposições iniciais ao referir que o sistema permite facilitar o ‘combate’ ao terrorismo e a atividades criminosas transnacionais potenciadas pelo fluxo migratório.

“Para combater o terrorismo, atividades transfronteiriças, principalmente se pertencem ao crime organizado. E hoje, neste grande fluxo migratório, temos que gerir [fluxos]. Prüm também pode ser útil na luta contra a facilitação da imigração ilegal.” [P01]

“Para apanhar os criminosos que têm identidades falsas para se deslocarem de país em país. E sempre que entram noutro começam um novo registo.” [U01]

O sistema Prüm é comumente entendido como um avanço positivo face aos modos de investigação e de cooperação tradicionais (Van Camp & Dierickx, 2007; Williams & Johnson, 2008). Sendo que as perspetivas dos entrevistados alinham-se com a narrativa política da União Europeia acerca dos benefícios de sistemas tecnológicos como o de Prüm. Os considerandos 8 e 11 da Decisão 2008/615/JAI do Conselho são ilustrativos desta concordância. Pode ler-se no considerando 8 que “[o] objetivo é estabelecer procedimentos para um intercâmbio de dados célere, eficaz e de baixo custo”. Em particular, “este método deverá acelerar consideravelmente os procedimentos vigentes, permitindo aos Estados-Membros verificar se qualquer outro Estado-Membro e (...) qual, tem as informações de que precisa” (considerando 11). Dito isto, nos extratos apresentados, encontra-se explícita a alusão à economia de tempo trazida pelo novo modelo de cooperação policial e judicial que assenta no direito de acesso a ficheiros de análise automatizada de DNA (considerando 10).

“Prüm economiza muito tempo e funciona para os polícias. Porque antes de Prüm, se se quisesse verificar DNA e impressões digitais, tinha de se enviar [uma solicitação] através da INTERPOL para todos os países, e todos os países verificavam as impressões digitais e o DNA. Hoje, isso é feito automaticamente.” [K01]

“Essa é uma maneira de demonstrar que podemos, na Europa, organizar a cooperação policial da forma mais rápida possível.” [H02]

Da análise das entrevistas observou-se que o discurso político europeu quanto às novas dimensões da cooperação policial e judiciária foi completamente assimilado e internalizado pelos NCP 2, atores fulcrais no funcionamento do sistema Prüm. Deste modo, os benefícios apresentados pelos entrevistados, nomeadamente, o combate ao terrorismo e à criminalidade organizada e a celeridade na partilha de dados entre Estados-Membros, coincidem cabalmente com o que se encontra oficializado na Decisão 2008/615/JAI do Conselho.

Desafios e riscos do sistema Prüm

Nesta secção serão apresentadas as perspetivas dos participantes do estudo no que concerne aos potenciais desafios e riscos que podem emergir no recurso ao sistema Prüm para efeitos de cooperação policial e judiciária na UE. As situações de risco presentes nas narrativas dos/as entrevistados/as balizam-se nos procedimentos de partilha de informação ao nível do passo 2 do sistema Prüm. Dito isto, uma das preocupações avançada tem que ver com a necessidade do cumprimento dos princípios gerais de proteção de dados, nomeadamente, em relação à limitação da finalidade de recolha de informação e à necessidade de controlo dos dados partilhados (Brown, 2009; European Data Protection Supervisor, 2006; Gamero et al., 2008; Gonçalves & Jesus, 2012, 2013; Harbo, 2010; Hert, 2005; IRISS, 2012). Segundo os extratos apresentados, a tónica no possível desvirtuamento da utilização dos dados partilhados não incide necessariamente no sistema Prüm. É, pelo contrário, considerado que tal responsabilidade recai sobre os próprios países envolvidos nos procedimentos do passo 2. Isto deve-se ao facto deste passo ser inteiramente dependente da legislação nacional.

“A questão não está no sistema em si. Está no depois. Precisamos de verificar [a correspondência]. Cabe ao país [recetor] provar que há um uso legal dessas informações, que as pessoas não serão condenadas por uso indevido das informações partilhadas. É, principalmente, o modo como se usam as informações provenientes de [Prüm] no seu processo, no seu caso judicial.” [H02]

“Há sempre o risco de que algumas informações possam ser usadas contra a lei ou fora do âmbito para o qual foram enviadas. Mas acho que no nosso país a probabilidade de isso acontecer é muito pequena. Porque se for à base de dados, cada consulta é registrada digitalmente. E se houver um *login*, tem que se ter um motivo para a consulta, deve digitar-se tudo, é um risco muito pequeno.” [S02]

Deste modo, as narrativas dos/as entrevistados/as acerca desta temática enquadram-se na categoria do ‘pragmatismo biométrico’ que se caracteriza, por um lado, pela relevância nas diferentes fontes de obtenção de DNA (Williams & Johnson, 2004b). E, por outro lado, na avaliação da legitimidade da extração do material genético tendo por base avaliações distintas acerca da integridade física por associação a diferentes partes do corpo humano (Machado & Silva, 2008b, pp. 155-161; Williams & Johnson, 2004b, pp. 211-219). No sistema Prüm em particular, propõem-se que esta categorização abarque as preocupações com a legitimidade da utilização dos dados genéticos partilhados entre os Estados-Membros, estando esta sempre dependente das fontes de obtenção do DNA e da informação partilhada.

De um ponto de vista mais tecnicista, com uma reflexão diminuta ou praticamente inexistente em relação à legitimidade das informações partilhadas, alguns/mas entrevistados/as apontaram a possibilidade de ocorrerem falências técnicas no sistema Prüm. No extrato, em particular, é referida uma situação hipotética onde a inatividade dos canais de comunicação/verificação de um país pode condicionar o fluxo dos dados e, consequentemente, levar a que algumas solicitações de informação não sejam atendidas. No entanto, depreende-se deste mesmo extrato, o constante discurso de minimização de riscos, onde nenhum desafio/risco é significativo ao ponto jeopardizar o funcionamento do sistema Prüm em si. Este tipo de narrativa encontra-se em linha, por um lado, com a sobrevalorização da tecnologia em relação aos meios tradicionais de investigação criminal (Maciel & Machado, 2014, p. 143). Por outro lado, com a mitigação de riscos que advém dessa mesma sobrevalorização (*idem*), pois uma ‘notificação para todos os países’ (S01) revela-se suficiente para resolver o problema.

“Talvez alguns pedidos [de informação] perdidos. Se o sistema de um país estiver inativo e outro país estiver a enviar solicitações, o primeiro não envia resposta. Mas temos um acordo de que, se um sistema estiver inativo, enviamos imediatamente uma notificação para todos os países.” [S01]

A necessidade da garantia da privacidade e da proteção dos dados partilhados no âmbito da cooperação policial e judiciária foi elencada como um dos potenciais desafios associados ao sistema Prüm. A perspetiva destes/as entrevistados/as a respeito do presente tópico encontra-se a par daquelas que têm sido as preocupações ao nível da União Europeia, sendo que se tem assistido à criação e implementação de diferentes documentos legislativos que visam uma maior proteção aos dados dos cidadãos. No entanto, as normas europeias para o tratamento e a partilha de dados para fins de investigação criminal não são vinculativas permitindo aos Estados-Membros diferentes apropriações em relação às mesmas. Logo, diferentes modos de apreender a proteção dos dados dos cidadãos no âmbito da esfera criminal (Jasanoff, 2005; Machado & Santos, 2016). Realce-se, contudo, que à reflexão sobre a proteção de dados na esfera criminal e em esferas não-criminais subjazem diferentes estruturas de valores e normas sociais.

No âmbito da partilha transnacional de dados forenses, como se pode observar nos extratos apresentados, a escala é ampliada a um ponto em que não se questionam apenas as estruturas de um país, mas de todos os países intervenientes. Desta premissa depreende-se que tanto a privacidade como a proteção de dados carecem de uma solução híbrida que lhes permita serem compreendidas à luz dos seus contextos específicos (Nissenbaum, 2010). Ou seja, uma solução que permita a implementação de legislação geral sobre privacidade e proteção de dados, mas que não exclua a criação de diretrizes que abranjam os contextos específicos em que esta possa ser ameaçada (Liu, 2013). Portanto, no âmbito da UE, em particular no sistema Prüm, é fundamental que o *standard* da privacidade e proteção de dados conserve o seu caráter flexível, pois só assim se torna alcançável equacionar a privacidade à luz da sua integridade contextual (Nissenbaum 2010; Timmermans & Berg, 1997). Neste sentido, a adaptação do *standard* da privacidade e da proteção de dados encontra-se em constante mutação pois também as epistemologias nacionais sofrem alterações a par com as normas europeias (Jasanoff, 2005; Timmermans & Epstein, 2010, p. 80).

“Um grande risco é a proteção de dados. A maneira como [o meu país] encara a proteção de dados pode ser diferente da de [outro país]. No entanto, em toda a Europa, há algumas semelhanças nas legislações de proteção de dados. Possivelmente, sem ter qualquer exemplo específico em mente, [Prüm] também poderia ser desadequadamente utilizado.” [W01]

“Eu gostaria que ninguém tivesse informação acerca de mim. Na realidade, do ponto de vista da privacidade talvez eu gostasse de ser invisível. Quando eu era jovem sempre quis ser invisível, isto é, 100% de privacidade. Mas depois apercebi-me de que não posso ser invisível...” [S01]

No entanto, no âmbito do presente estudo constata-se que as narrativas a respeito dos desafios de privacidade e proteção de dados no sistema Prüm cingem-se a discursos institucionalizados que carecem de concretização prática. Nesse sentido, não é possível avaliar em profundidade quais são as perspetivas destes profissionais em relação aos riscos associados à supressão do direito à privacidade e à proteção de dados dos indivíduos cujos dados são partilhados transnacionalmente. As situações hipotéticas supramencionadas nos extratos são simultaneamente reduzidas a potenciais riscos que não são significativos para a implementação e recurso ao sistema Prüm para fins de investigação criminal. Deste modo, os potenciais benefícios públicos deste tipo de tecnologia são encarados como um dado adquirido. Isto revela um encerramento dos riscos éticos e das questões de direitos humanos numa caixa negra (*black box*; Latour, 1987b) que deixa de fora uma discussão abrangente quanto à natureza e significado da partilha transnacional de dados genéticos (Jasanoff, 2011; Nuffield Council on Bioethics, 2007). Mais concretamente, quanto à natureza sensível dos dados genéticos, às possíveis perdas e desvirtuamento dos dados por parte das entidades nacionais recetoras (Gamero et al., 2008; Liu, 2013, p. 13; Wallace et al., 2014, p. 58).

De modo complementar ao referido anteriormente, verificam-se também perspetivas que vão no sentido de eliminar por completo os desafios do sistema Prüm. Como se pode observar nos extratos apresentados, os/as entrevistados/as não consideram que o sistema possui riscos tanto para as liberdades individuais dos cidadãos, como para a segurança dos dados genéticos partilhados entre Estados-Membros. Deste modo, assume-

se, por um lado, a segurança física e virtual dos canais de comunicação do sistema. E, por outro lado, a legitimidade das informações recolhidas e partilhadas transfronteiras.

“Eu não consigo ver nenhum risco em concreto. Não me parece que nós andemos a trocar informação que não seja efetivamente necessária. Nós temos canais que são protegidos e que são seguros, também não me parece que por aí haja [algum] risco. Não há concretamente uma ingerência em nenhum ordenamento jurídico.” [N14]

“Penso que os Estados-Membros estão bem preparados e neste sistema de comparação (Prüm), a parte informática está protegida. Penso que os *hackers* não podem intrometer-se no sistema, suponho que está bem protegido. (...) Não vejo riscos porque os enquadramentos legais são muito semelhantes e seguimos os mesmos *standards*.” [P01]

Como se observa nos excertos supracitados, as narrativas assentam numa retórica que realça a objetividade da standardização técnico-legal enquanto garante da eliminação de riscos do sistema Prüm. Sendo que os processos de harmonização legal e da standardização tecnológica vieram permitir uma maior coordenação transnacional do meio social, particularmente, ao nível da cooperação policial e judiciária (Botzem & Dobusch, 2012, p. 1). Pois, os *standards* do sistema Prüm operam enquanto ferramentas de tradução das práticas e símbolos de contextos nacionais que poderiam *a priori* ser incompatíveis. Deste modo, é possível assegurar a interoperabilidade das bases de dados forenses de DNA permitindo, simultaneamente, a cooperação ao nível da investigação criminal entre países culturalmente diferentes e geograficamente distantes (Balzacq et al., 2006; Bigo, 2008; Bowker & Star 1999; De Hert & Gutwirth, 2006; McCartney 2014a, 2014b; Timmermans & Epstein, 2010).

As narrativas dos/as entrevistados/as em relação à não existência de riscos relevantes no sistema Prüm são coincidentes com as políticas europeias que se têm apoiado na ideia de harmonização e standardização técnica, científica e legal com o objetivo de neutralizar as diferenças legais, culturais e políticas dos Estados-Membros (Lampland & Star, 2009, pp. 4-5; Prainsack & Toom, 2010, 2013). No entanto, estas narrativas tendem a

revestir-se de uma aparente neutralidade quanto às práticas associadas à partilha dos dados genéticos no sistema Prüm. Assumir que a estandardização mitiga os riscos associados a este tipo de sistemas condiciona uma reflexão mais profunda sobre as relações de poder associadas à criação dos *standards*, bem como das práticas de recolha de informação que ocorrem ao nível nacional. Por outras palavras, relega para o plano do invisível as condições éticas que se colocam com a utilização do sistema Prüm. Isto porque a criação e implementação do sistema Prüm pode, em certos países, ter origem em processos políticos enviesados (Timmermans & Epstein, 2010, p. 74).

Eficácia e futuro do sistema Prüm

O sistema Prüm, como já foi anteriormente referido, teve como principal objetivo a otimização das ferramentas de cooperação policial e judiciária de modo a permitir a detenção de indivíduos responsáveis de cometerem crimes ao nível transnacional (Amankwaa, 2019; Sallavaci, 2017; Santos, 2017; Santos & Machado, 2017). Este sistema encontra-se plasmado na lei da União Europeia desde 2008, sendo que até à data a Itália, a Grécia e a Irlanda continuam não operacionais quanto à partilha de dados genéticos (Council of the European Union, 2019b, p. 20). Deste modo, torna-se necessária a reflexão acerca da eficácia e dos possíveis caminhos a seguir na sua implementação. Os/as entrevistados/as chamam a atenção para as dificuldades sentidas na compreensão daquela que é a eficácia real do sistema Prüm. Isto porque a existência de uma correspondência entre bases de dados não gera necessariamente um *follow-up* a solicitar mais informação ou uma condenação. Portanto, o facto de o segundo passo não ser um procedimento estruturado não permite que se consigam performar estatísticas relevantes, pelo que a medição da sua eficácia será sempre relativa. De modo complementar, no segundo extrato é explícita a crítica à sobrevalorização das estatísticas dos *hits* no passo 1. Pois estas condicionam a relevância dada, por parte de certos países, às necessidades da polícia quanto aos resultados da partilha de dados através do sistema Prüm.

“O passo 2 é um problema para as estatísticas, porque não temos dados estruturados neste passo. Este é o problema. Mas a informática só vê estatísticas técnicas, não consegue ver as estatísticas do passo 2.” [S01]

“Todos os anos há uma publicação das estatísticas oficiais, mas só para o primeiro passo da cooperação acerca dos *hits*. E o segundo passo, se os casos têm sucesso, não há opinião acerca de como o fazer, como harmonizar a União Europeia. Por exemplo, (...) para o Parlamento Europeu seria importante saber se Prüm é uma ferramenta eficiente, se temos muitos *hits* e muitos casos de sucesso. E penso que alguns países não têm informação acerca da necessidade que os polícias têm destes dados em termos práticos.” [L03]

A produção de análises estatísticas capazes de aferir sobre a eficácia do sistema Prüm, principalmente ao nível do passo 2, deveria incluir indicadores mais específicos. Por exemplo, o número de *hits* que levaram à abertura de um processo judicial e em que processos se verificou a condenação com base na correspondência gerada no sistema Prüm. No entanto, este tipo de dados é estatisticamente difícil de traduzir, pois, de modo geral, os países não têm informação disponível a este respeito. Sendo que, fazer a monitorização das informações referidas exigirá aos Estados-Membros um dispêndio de recursos que pode ser demasiado elevado para as suas capacidades. Atendendo à presente conjuntura importa realçar que a legitimação de um sistema de partilha de dados passa pela medição da sua eficácia real, neste caso em particular, enquanto ferramenta de resolução de crimes. Constata-se, neste estudo, que a eficácia do sistema é maioritariamente associada ao seu estado de implementação na UE. Contudo, é necessário que se englobe uma outra dimensão que remeta para a sua mensurabilidade em termos de detenção e deteção do crime. Pois, tal como é referido por Toom, Granja e Ludwig (2019) “the utility and efficacy (...) cannot effectively be measured in a meaningful way (...) making it impossible to answer the question whether the Prüm regime is a proportional crime control mechanism” (p. 55). Portanto, para uma efetiva e global avaliação do sistema Prüm em termos de utilidade e eficácia é preciso mover a tónica do estado de implementação para sua proporcionalidade enquanto sistema de biovigilância transnacional. Não sendo possível discernir os dados de deteção do crime estão em causa princípios legais fundamentais como o da proporcionalidade (Harbo, 2010; Prainsack & Aronson, 2015; Williams & Johnson, 2004a; Williams & Wienroth, 2014).

Relativamente ao futuro do sistema Prüm as narrativas dos/as entrevistados/as realçam a necessidade de se concluírem os processos de implementação do sistema em

todos os Estados-Membros da União Europeia. Por um lado, para que a partilha de dados para fins de investigação criminal não continue a depender de acordos bilaterais entre países. Por outro lado, para fomentar as práticas de cooperação policial e judiciária ao nível transnacional.

“Espero a conexão entre todos os países. Penso que é a base para esta cooperação. Porque quando temos apenas parceiros bilaterais é bom, mas não é o objetivo de Prüm. E espero que os países comecem a cooperar mais uns com os outros.” [L03]

De modo complementar, os/as participantes do presente estudo referem que o futuro do sistema Prüm passa pelo encurtamento dos tempos de resposta ao nível no segundo passo, ou seja, quando ocorre a solicitação de partilha de informação. A celeridade ambicionada tem como principal obstáculo as especificidades nacionais das normas dos procedimentos que possibilitam o envio de informações pessoais para países terceiros (Prainsack, 2010, p. 22; Prainsack & Toom, 2013). Por sua vez, a alteração de procedimentos ao nível nacional é condicionada, por exemplo, pela falta de recursos para assegurar a proteção de dados e de especialistas em questões de privacidade (Costa & Nunes, 2001; Fiodorova, 2014, p. 130; Prainsack & Toom, 2013). Como se pode observar no extrato abaixo apresentado a não harmonização dos requisitos envolvidos no passo 2 do sistema Prüm coloca em causa a eficácia da própria cooperação policial e judiciária.

“Espero que melhore, que haja maior (...) rapidez, mais concretamente, na circulação da informação. Mas compreendo que não é fácil. Se o procedimento dos outros Estados-Membros [não] for parecido com o nosso, é difícil. Mas gostava que estes prazos fossem mais curtos efetivamente.” [N14]

A este respeito as narrativas dos/as participantes encontram-se em linha com o princípio da celeridade plasmado na Decisão 2008/615/JAI do Conselho de 23 de junho de 2008. Pode identificar-se em vários parágrafos do documento a celeridade da resposta como objetivo a alcançar com o sistema Prüm. Em particular, nos considerando seis, oito e onze e no número 2 do artigo 4.º. Decorrente da situação supramencionada é reiterada a

importância da operacionalidade de todos os países da UE para permitir a realização do *follow-up* no *step 2* com sucesso (Machado & Granja, 2019b). Realçando-se que a cooperação transnacional estagna no *step 1* do sistema Prüm, ou seja, na confirmação do *hit* relativo ao perfil de DNA solicitado.

“Nem todos os países estão operacionais em Prüm. Para mim isto é uma das coisas mais negativas. Penso que tornaria a vida das pessoas muito mais fácil, (...), mas fica-se pelo passo 1.” [W01]

O presente estudo contribui para a compreensão daquelas que são as aspirações dos Pontos de Contacto Nacionais relativamente à evolução do sistema Prüm. Deste modo, observa-se que as suas avaliações a respeito do futuro deste sistema encontram-se intimamente condicionadas pelo seu estado atual de implementação na UE. No entanto, a análise realizada não permite discriminar, ao nível nacional, a associação entre os indicadores de eficiência e as perspetivas dos/as entrevistados/as acerca do futuro do sistema Prüm. Dito isto e de modo a apreender com maior profundidade a situação enunciada é essencial que em investigações futuras seja possível a realização de uma caracterização nacional da eficiência e das expectativas futuras desta ferramenta. Num último ponto, este estudo vem reiterar a necessidade de se enquadrar a eficácia do sistema Prüm para além da sua implementação nos Estados-Membros, de modo a que se estimulem mecanismos de mensurabilidade para a deteção real do crime.

Estrutura de dois passos no sistema Prüm

O sistema Prüm, enquanto estrutura de dois passos é, genericamente, descrito como um fator de *empowerment* (Prainsack & Toom, 2010) para os Estados-Membros em termos de cooperação policial e judiciária. Por um lado, porque confere maior velocidade aos mecanismos de partilha de informações entre países. Por outro lado, porque este tipo de estrutura permite que se realize a confirmação de correspondências previamente ao envio das informações pessoais das pessoas envolvidas. Considerando-se esta uma medida de reforço da privacidade em linha com os princípios da proteção de dados da União Europeia (Machado & Silva, 2010; Prainsack, 2010; Prainsack & Toom, 2010). Deste modo, o *step 1* é encarado de forma semelhante entre o primeiro grupo de profissionais analisado neste

capítulo e os entrevistados que desempenham funções no *step* 2. Continua a ser elencado, como se pode observar nos extratos abaixo, o caráter automático e a celeridade desta fase do processo de partilha de dados, não descurando o papel dos sistemas informáticos no sucesso da operação.

“Portanto, o passo 1 é muito simples, ao nível técnico da informática não tem qualquer problema.” [S01]

“Quanto aos benefícios, penso que, no primeiro passo é mais rápida a partilha de informação. Mas só no início, mas é preciso o início para começar a cooperação.” [L03]

O *step* 1 é consistentemente avaliado através da lente da *administrative objectivity* (Lynch, 2013), sendo encarado como um procedimento estandardizado no contexto do sistema Prüm. Devido à objetividade imprimida nesta fase da cooperação transnacional verifica-se a inexistência do aprofundamento dos vários desafios éticos e técnicos que podem colocar em causa o correto funcionamento do passo 1. Os desafios éticos e técnicos relacionam-se, ainda que genericamente, com as boas práticas científico-laboratoriais, a possibilidade de contaminação das amostras que chegam ao laboratório para análise, a divulgação de falsos positivos para países terceiros, a proteção de dados e a capacidade de prestação de contas através da produção de relatórios para consulta pública (Machado & Granja, 2018, p. 257). No entanto, a formação académica e profissional dos Pontos de Contacto Nacionais para o passo 2 pode estar na origem da falta de sensibilidade para as questões técnicas e científicas enunciadas. Grosso modo, como referido na parte introdutória do presente capítulo, o perfil destes NCPs baseia-se na formação policial e no direito. De modo complementar, observa-se a mitigação dos riscos através da premissa de que nesta fase os geneticistas forenses trabalham com dados que não permitem identificar a pessoa a quem corresponde o perfil de DNA a ser comparado (Machado & Granja, 2018). Esta justificação está em linha com o caráter de neutralidade atribuído aos números (Porter, 1995) que neste contexto operam como ‘tecnologias de distanciamento’ (Porter, 1992) permitindo a apreensão de significados por diferentes comunidades epistémicas e científicas. Recuperando o trabalho de Williams e Johnson (2004), as perceções dos/das

entrevistados/as em relação ao passo 1 do sistema Prüm, remetem também para a categoria do 'minimalismo genómico', como se pode observar no extrato abaixo apresentado. Em particular, no extrato, é enfatizada a anonimidade do perfil de DNA através da utilização de códigos “neutro(s) de identificação” [P01], sendo o seu potencial informativo diminuto nesta fase da cooperação.

“Os especialistas do instituto forense confirmam que os dois perfis de DNA correspondem. Mas esta parte do *hit* é anónima. Portanto, durante a primeira parte deste procedimento não sabemos quem é que está por trás do *hit*, não vemos as pessoas, só recebemos um código neutro de identificação.” [P01]

Relativamente ao segundo passo do sistema Prüm são observados vários pontos relevantes acerca da sua reflexão a respeito da eficácia desta etapa, tanto ao nível do fluxo de informação, como ao nível da velocidade da partilha de dados pessoais entre Estados-Membros. Um dos pontos elencados aponta para a premência de melhorar o *follow-up* das correspondências verificadas na fase anterior (passo 1). Após a confirmação do *hit* podem verificar-se três cenários: 1) o Estado-Membro requerente opta por não pedir informação adicional a respeito do perfil de DNA; 2) O Estado-Membro requerente solicita, ao Estado-Membro recetor, o envio de informação pessoal acerca do perfil de DNA e o pedido é acedido (os dados são enviados); 3) O Estado-Membro requerente solicita, ao Estado-Membro recetor, o envio dos dados pessoais respeitantes ao perfil de DNA e estes não são partilhados (os dados não são enviados). Dito isto, no extrato apresentado, a flexibilidade da decisão de partilhar os dados entre países é um elemento problemático para o fluxo expectável dos dados no âmbito do sistema Prüm. Deste modo o funcionamento e eficácia do sistema Prüm encontra-se maioritariamente dependente do sucesso da concretização do segundo passo.

“É uma partilha em massa, mas não temos de seguir para o passo 2. O que devíamos realmente fazer para ter a certeza que Prüm funciona era seguir para o passo 2. Mas é difícil.” [U01]

Estando ultrapassados os obstáculos que surgem na fase do pedido de *follow-up* das correspondências com *hits* positivos, os profissionais entrevistados reconhecem que mesmo quando ocorre a partilha de dados na segunda fase existem aspetos que condicionam a eficácia processo. Genericamente, os pontos elencados como problemáticos estão diretamente associados com a diversidade das práticas de partilha de informação ao nível nacional. A partilha transnacional automatizada de perfis genéticos teve e tem como objetivo a estandardização técnico-científica de modo a neutralizar a diversidade legal, cultural e política dos Estados-Membros da UE (Lampland & Star, 2009; Prainsack, 2010, p. 22; Prainsack & Toom, 2010, 2013). Deste modo, a fixação de determinados *standards* vem permitir que os países usufruam dos benefícios da harmonização de práticas que garantem a interoperabilidade tecnológica das bases de dados dos países signatários (Balzacq et al., 2006; Bigo, 2008; Botzem & Dobusch, 2012; De Hert & Gutwirth, 2006; McCartney 2014a, 2014b). No entanto, o sucesso da interconexão técnica entre as bases de dados de perfis de DNA não é extensível à comunicação entre países. Esta situação é justificada pelo facto de não existir a estandardização completa da partilha transnacional de dados, o que se possui até ao momento é uma ‘aproximação’ que, simultaneamente, permite a partilha de dados e conserva o controlo dos países em relação às suas escolhas quanto às práticas a adotar para a realização da mesma (Perras, 2017). Dito isto, os Estados-Membros possuem apenas a obrigatoriedade de corresponder aos *standards* básicos da partilha de dados estabelecidos pela União Europeia.

O primeiro fator de destandardização do passo 2 do sistema Prüm elencado pelos/as entrevistados/as tem que ver com a falta de compactação da informação possuída que vem tornar o processo de partilha mais moroso e a inexistência de um formato estandardizado para o envio de informação para o Estado-Membro requerente. Deste modo, quando um país recebe a informação solicitada esta pode ser apresentada de acordo com diversos modelos com campos de preenchimento e tipos de informação a partilhar diferentes, tal como se pode observar no segundo extrato apresentado.

“Mas no segundo passo talvez tenhamos 100 páginas de dados, como as formatamos? Podemos ter 1.000.000 de campos para preencher.” [S01]

“Acho que os Estados-Membros não chegaram a acordo sobre o formato textual do passo dois, sendo que o primeiro passo é formatado para todos os parâmetros do DNA. Mas o segundo passo não é o mesmo em todos os países. (...) Tipo de crime (...). Penso que diferentes Estados-Membros apresentam a informação de formas diferentes.” [S01]

Consequência da não estandardização do formulário a utilizar para a partilha transnacional de dados pessoais é a heterogeneidade dos canais de comunicação escolhidos pelos Estados-Membros (Machado & Granja, 2019a, 2019b). Deste modo, os pedidos de informação no passo 2 podem ser efetuados por canais como a Europol, a Interpol, o SIENA, entre outros – segundo fator de destandardização. Apesar de serem infraestruturas tecnicamente consolidadas deixam ao critério do utilizador o canal de comunicação a que pretende recorrer. Por outras palavras, o profissional encarregue de fazer o pedido de informação pode estar mais familiarizado com o funcionamento de um canal em detrimento de outro e a opção escolhida pode não ser a mais eficiente (Sulca, 2017, p. 245). Sintetizando, não há no âmbito da partilha de dados no sistema Prüm uma estratégia delineada para a escolha do canal de comunicação o que torna o processo demasiado complexo. Como se pode observar nas narrativas dos/as participantes, a falta de estandardização neste ponto leva a que alguns Estados-Membros optem pela criação de unidades de comunicação centralizadas com o objetivo de responder aos pedidos de acordo com os canais escolhidos pelo outro país.

“Alguns países usam a EUROPOL, outros a INTERPOL. O motivo pelo qual decidimos utilizar SIENA teve a ver com o facto de Prüm ser apenas para Estados-Membros da UE. Mas outros países usam a INTERPOL porque está disponível 24h por dia e 7 dias por semana, é fácil e não existe nenhum formato de texto específico. E nós decidimos criar esta unidade de Prüm como um PUC – Ponto Único de Contacto. São-nos enviados todos os pedidos, analisamo-los e respeitamos a escolha do canal de comunicação dos nossos parceiros.” [K01]

O passo dois do sistema Prüm possui, nas palavras dos/das entrevistados/as, um terceiro potenciador de destandardização, nomeadamente, a custódia da base de dados

forense de perfis de DNA. Dito isto, quando as bases de dados forenses se encontram sob a alçada de autoridades judiciais o processo de partilha de informações é, tendencialmente, mais lento e complexo do que quando se realiza através de instituições policiais (Machado & Granja, 2019a, p. 11; Matos, 2019, p. 158). Constata-se, portanto, que as diferentes práticas de cooperação transnacional da polícia e das autoridades judiciais podem apresentar-se como um obstáculo à partilha de informação (*idem*). De modo breve, as instituições policiais operam segundo o princípio de acesso ao máximo de informação disponível (inteligência) com o objetivo de concluir com sucesso a investigação criminal (Innes et al., 2005; Spapens, 2017, p. 151). Por outro lado, as autoridades judiciárias têm um modo de atuação que tende a ser mais restritivo, pois para além de ser um processo mais moroso, por norma, resulta na partilha de menos informação (Machado & Granja, 2019a; Matos, 2019). De modo complementar, a racional de atuação das duas instituições é diferente devido às diferentes funções que estas desempenham no âmbito do sistema de justiça criminal (Perras, 2017, p. 224). As forças policiais têm como objetivo a apreensão e deteção dos indivíduos que cometem crimes. As instituições judiciárias julgam os indivíduos que cometeram (ou não) determinado crime (Matos, 2019). As discrepâncias em termos da metodologia de atuação na cooperação transnacional encontram-se explicitamente plasmadas em Machado e Granja (2019a, p. 14), citando:

“The clash between these different working methods (...) therefore undermines the principle of reciprocity and trust that police professionals claim is needed within transnational cooperation and prevents the construction of relationships based on trust with their judicial counterparts.”

Nas narrativas dos/as entrevistados/as encontram-se implícita e explicitamente descritas algumas das tensões que derivam de diferentes custódias nas bases de dados forenses de perfis de DNA. No primeiro extrato está patente a premissa de que quando a partilha de dados pessoais depende de um país com custódia judicial o processo de obtenção de informações é mais burocrático e difícil. Isto porque para além de, como já foi referido, se partilharem menos dados, é preciso realizar com frequência um pedido subsequente para obtenção de mais informação (carta rogatória). No segundo extrato, denota-se uma das consequências que advém do difícil fluxo de informação quando as autoridades judiciárias estão envolvidas no processo de cooperação transnacional. Nas palavras do/a entrevistado/a, os profissionais responsáveis pelo pedido de informação e,

por conseguinte, os seus respetivos países, podem ver o passo 2 do sistema Prüm com alguma frustração em situações onde a cooperação tenha sido condicionada devido à custódia da base de dados. Deste modo, ambos os extratos expressam perspetivas críticas a respeito do funcionamento das instituições judiciais no que concerne à cooperação transnacional. Por um lado, o facto da obtenção de informações ser mais trabalhosa. Por outro lado, a possível frustração que deriva de uma negação da cedência de dados pessoais ao país requerente que pode resultar em tensões nas relações entre os países envolvidos.

“Enviam-nos o nome da pessoa, enviam pouca informação: nome, ofensa... Não é automático. Portanto, temos um nome, mas se quisermos ter algo mais do que isso temos de enviar outro pedido. Um pedido judicial.” [H02]

“Eu diria que, às vezes, conduz a mais frustrações. Quero dizer, o [País A] está tão aborrecido com o [País B] neste momento. Eles têm a identidade de um homicida, mas recusam-se a dar a informação ao [País A] porque estão sob a alçada do Ministério do Interior.” [U01]

O quarto fator de destandardização remete para os critérios de *follow-up* das correspondências positivas no sistema Prüm, sendo que estes são igualmente heterogéneos entre os Estados-Membros da União Europeia. Neste sentido, nos excertos que se seguem, os/as participantes identificam as diferentes práticas quanto à quantidade e tipo de informação partilhada no âmbito da cooperação transnacional. Em particular, por um lado, o envio de informação para um país requerente pode ser condicionado pela tipologia e pela gravidade do crime em termos de moldura penal. Por outro lado, a não cooperação pode estar ainda relacionada com o facto de se considerar que o crime não justifica o envio de informações pessoais sobre o indivíduo que consta na base de dados nacional. Neste caso, o facto de o país decidir manter as informações privadas, independentemente de auxiliar ou não na resolução de um caso criminal, pode ser encarado como uma medida de proteção de dados.

“Se se tiver um caso menor, a maior parte das vezes as pessoas não fazem o seguimento do processo.” [H02]

“Mesmo que haja uma correspondência, continua a existir a opção de a polícia local decidir não começar o caso, porque pode ser um caso antigo, sei lá, um roubo de há dez anos (...) e talvez o procurador [já] tenha fechado o caso e não há nada a fazer. Então, eles têm a informação do laboratório a dizer que têm um *hit*, mas ninguém nos vai enviar um pedido para iniciar o segundo passo.” [G06]

Considerando o terceiro e quarto fator de destandardização, alguns dos/as entrevistados/as, encetam uma possível solução cujo objetivo é o de fomentar a cooperação transnacional e, por conseguinte, a partilha de informações entre países. O extrato apresentado é representativo daquilo que os/as participantes referiram nas suas narrativas. Deste modo, considera-se que é importante que se comece a impor que os países iniciem os procedimentos do passo 2, pois a cooperação policial e judiciária deve e tem de assentar no princípio da confiança mútua entre os Estados-Membros (Balzacq & Hadfield, 2012; Matos, 2019; McCartney, 2014a).

“Agora temos de forçar as pessoas a fazer o passo 2. Depois temos de forçar os países com a Iniciativa Sueca – é apenas um acordo – que se se tiver um pedido em Prüm deve mesmo enviar-se a informação. Não se pergunta de que Ministério são as pessoas, estamos a cooperar com a Europa, se fizerem um pedido de Prüm e forem cumpridores, então têm a informação. Eu tenho uma informação, claro que eu quero ajudar os outros países. Se preencherem o processo corretamente, nós confiamos.” [U01]

O ponto subjacente às perspetivas dos/as entrevistados/as quanto à partilha de informação e aos seus obstáculos tem que ver diretamente com questões de confiança entre os respetivos Estados-Membros. Sendo que os obstáculos à implementação do sistema Prüm, principalmente, ao nível do passo 2 podem estar fortemente associados à falta de confiança entre alguns países (Hijmans, 2006, pp. 2-3). Como se observou nos extratos supra apresentados verifica-se o condicionamento do envio de dados pessoais, bem como da informação a partilhar para terceiros. Situação que pode levar ao condicionamento da eficácia do sistema Prüm, bem como da resolução de uma investigação

criminal cujo objetivo se pauta pela restituição da justiça à vítima e pela detenção do indivíduo perpetrador do crime.

A evolução das políticas transnacionais de partilha de dados tem assentado, tal como demonstra o/a entrevistado/a, na confiança das autoridades de um país tanto nos processos como na produção de dados obtidos por autoridades em território externo (McCartney, 2017, p. 170). Neste sentido, o que começou por ser o reconhecimento mútuo entre Estados-Membros de decisões de tribunal tem-se expandido para a esfera da investigação criminal pelo reconhecimento de provas forenses recolhidas por um país terceiro, como se observa no sistema Prüm (*idem*, p. 172). Apesar de defender a cooperação sem condicionamentos, o/a participante ressalva que só os países ‘cumpridores’ devem ter acesso às informações solicitadas. Neste ponto observa-se a importância atribuída à integridade dos dados pessoais partilhados, integridade essa que pode ser condicionada por práticas policiais desadequadas, falta de creditação dos laboratórios, erros de interpretação de dados, entre outros. Portanto, torna-se imprescindível a integridade dos sistemas de acreditação das instituições e profissionais envolvidos na cooperação, nos diversos países da União Europeia (*idem*, p. 173).

Privacidade e proteção de dados no sistema Prüm

A proteção de dados e privacidade da partilha de informações pessoais no âmbito do sistema Prüm, como já referido, foi um dos pontos abordados ao longo das entrevistas aos Pontos de Contacto Nacionais para o passo 2. Nesta secção pretende-se compreender quais são as perspetivas dos/as entrevistados/as relativamente às medidas que estão a ser utilizadas para garantir que a partilha de dados respeita os princípios da proteção de dados no âmbito da cooperação na esfera criminal. Observando o extrato abaixo apresentado é possível discernir alguma preocupação no cumprimento daqueles que são os princípios estabelecidos pela União Europeia para os *standards* mínimos da privacidade. No entanto, é escassa ou praticamente inexistente a elaboração acerca do modo como é assegurado o cumprimento das leis de proteção de dados na cooperação policial e judiciária transnacional. Ficam por identificar e compreender quais os mecanismos de proteção específicos mobilizados pelos diferentes países.

“O que é certo é que quando enviamos a resposta da base de dados de DNA temos de assegurar que esta está de acordo com as nossas leis de proteção de dados.” [X02]

Não obstante as narrativas salientarem que é necessário garantir que os países recetores da informação respeitem as normas e leis estabelecidas ao nível nacional. Constata-se que a generalidade dos/das participantes não se mostram particularmente preocupados com falhas que possam comprometer a privacidade e a proteção dos dados pessoais partilhados. No entanto é necessário não cair na interpretação fácil de que estes/as profissionais entendem que os indivíduos que constam nas bases de dados não devem usufruir de proteção dos seus dados pessoais. Pois, o motivo para a não preocupação a respeito da garantia de privacidade na cooperação realizada nestes moldes recai no facto de considerarem que o sistema Prüm em si está preparado para assegurar a segurança dos dados. Deste modo, são realçadas várias medidas que visam a proteção das informações que constam nas bases de dados forenses de perfis de DNA, bem como a sua, consequente, partilha para outros países.

Cabalmente, como se pode observar nos extratos apresentados, as narrativas remetem para a implementação de acessos restritos às bases de dados através de *logins* individuais que permitem controlar os acessos e a informação consultada pelos profissionais envolvidos no processo. Este posicionamento mostra-se bastante favorável à co-construção da ordem social por meio do recurso a tecnologia enquanto garante dos princípios da proteção de dados (Gottweis, 1998; Jasanoff, 2004, 2005). Deste modo, constata-se que o sistema Prüm é percecionado pelos/as entrevistados/as à luz de argumentos baseados na neutralidade e imparcialidade relativamente às práticas sociais daí resultantes (Lyon, 2007; Monahan, 2010). Onde a dimensão social, condicionada por fatores económicos, culturais e ideológicos de uma tecnologia é totalmente invisibilizada (Baines, 2006; Bowker & Star 1999; Lampland & Star, 2009).

“Tudo o que colocamos, tudo o que procuramos no nosso sistema é *logged*. Se eu fizer alguma coisa nesses sistemas que têm dados pessoais, tudo é *logged*. Portanto, podemos voltar atrás e ter a certeza [de que está tudo correto].” [U01]

“O que temos nos ficheiros a que temos acesso, temos um *username* pessoal e uma palavra-passe, portanto, todas as pesquisas que eu faço são gravadas.” [H02]

Para estes profissionais a proteção de dados passa não só pelas soluções ao nível tecnológico, como também pela adequação da legislação nacional às necessidades da partilha e da proteção de dados. O *step 2* do sistema Prüm, pelo qual os entrevistados estão encarregues, permite avaliar a legislação nacional e discernir se a partilha se encontra de acordo com os parâmetros legais (McCartney et al., 2011, p. 316; Prainsack & Toom, 2010). No que concerne à legislação nacional em vigor, a maioria dos entrevistados revelou que, na generalidade, esta compreende as especificidades dos dados partilhados e, como tal, o sistema Prüm não veio trazer alterações significativas à mesma. De modo residual, alguns destes profissionais, principalmente os que possuem formação profissional em ‘direito’, realçam que apenas transmitem para os outros países a informação que consideram ser necessária e legítima para a investigação.

A linha de atuação em situação de correspondência entre perfis de DNA enunciada pelo entrevistado elenca três pontos relevantes. Primeiro, ao nível da proteção de dados, coloca em questão a partilha indiferenciada de todo o tipo de informação retida pelas instituições nacionais. Segundo, ao selecionar que informações serão partilhadas potenciam-se as atividades de inteligência desenvolvidas através da cooperação policial e judiciária do sistema Prüm (Machado & Granja, 2019a). Sendo que a construção de *intelligence* enquanto modo de informação passa pelo princípio de que os dados foram “interpreted and analysed in order to inform future actions of social control against an identified target” (Innes et al., 2005, p. 42). Terceiro, de modo menos explícito, tem-se a problemática da propriedade dos dados partilhados no sistema Prüm (Bigo et al., 2007). Dito isto, a partilha de dados pessoais no sistema Prüm pode encontrar obstáculos devido à resistência na cedência de soberania dos países em matéria criminal (Hufnagel, 2012; Perras, 2017), como também devido à falta de confiança entre os Estados-Membros (Hufnagel & McCartney, 2015). Ao exigir ‘as razões exatas’ pelas quais os dados são solicitados depreende-se que o entrevistado pretende garantir que os países terceiros oferecem as condições necessárias à proteção de dados na partilha de informação.

“Normalmente tentamos transferir o mínimo de dados necessários (...). Não damos todos os dados que podem ser encontrados nos nossos ficheiros nacionais. Eles [de outros países] têm de indicar as razões exatas, pelas quais precisam dos dados: apenas para identificação ou outras razões sérias.” [P01]

Relativamente à formulação das Decisões Prüm em matéria de proteção de dados, a maioria dos entrevistados considera que são equacionadas as salvaguardas necessárias para a realização da partilha de dados ao nível transnacional. Contudo, a literatura tem apontado duas fragilidades ao sistema no que concerne à proteção de dados. Primeiro, o documento das Decisões cinge-se à regulação transnacional da partilha de dados, pelo que não incide na recolha e análise de informações pessoais realizadas ao nível nacional (Gonçalves & Jesus, 2012, p. 123). Segundo, as negociações que envolveram a criação do sistema Prüm não usufruíram de um envolvimento ativo tanto das autoridades nacionais de proteção de dados como da Autoridade Europeia para a Proteção de Dados (Bellanova, 2008, p. 205).

Num outro posicionamento em relação à privacidade no sistema Prüm, um dos entrevistados, com perfil policial, realça o ‘conforto’ que sente em relação à proteção dos dados partilhados encetando um cenário de divisão de responsabilidades. Neste sentido, demarca-se das responsabilidades associadas à legalidade do documento de Prüm que, no seu entender, fazem parte de um conjunto de situações que devem ser resolvidas por especialistas em direito. Neste excerto, em particular, constata-se a (des)responsabilização acerca do funcionamento do sistema em matéria de proteção de dados em função da demarcação de fronteiras (Gieryn, 1983) entre as culturas epistémicas dos profissionais de direito e da polícia (Machado & Granja, 2019a).

“Apenas posso expressar o sentimento geral de que me sinto confortável, tenho a base legal nas Decisões Prüm, penso que várias pessoas ponderaram este documento legal. Portanto, estou praticamente certo de que este não é um documento que possa magoar alguém. Se sim, espero que os advogados encontrem a lacuna e a corrijam.” [G06]

Um outro aspeto relevante na proteção de dados na sua partilha transnacional tem que ver com a restrição na utilização dos dados recebidos. Alguns Estados-Membros,

quando operam a partilha, optam por colocar no documento enviado para o Estado requerente que os dados enviados não podem ser utilizados no tribunal do país requerente. Desta forma, limitam a sua utilização à fase da investigação do processo destituindo-os totalmente do seu valor probatório. Porém, esta opção gera diferentes perspetivas sobre a reciprocidade implícita e o reconhecimento mútuo na cooperação internacional (Hufnagel & McCartney, 2017; McCartney, 2017) e, em particular, no sistema Prüm. Os excertos escolhidos mostram a polarização de narrativas quanto à limitação da utilização de informações em tribunal. O primeiro extrato apresentado é representativo do modo como é reiterado o valor investigativo da informação pessoal que é partilhada entre Estados-Membros, exigindo um procedimento mais moroso caso se pretenda utilizar os dados em tribunal.

“A seguinte afirmação é sempre incluída: ‘A informação abaixo, incluindo os dados pessoais relacionados com os indivíduos mencionados, apenas pode ser utilizada para uso operacional interno da polícia e não pode ser utilizada como prova no seu respetivo país. De modo a adquirir uma prova que possa ser utilizada em processos legais, as vossas autoridades devem requerê-la às autoridades competentes nacionais por meio de uma carta rogatória internacional.’” [G06]

Sob o argumento da estandardização dos métodos científicos para a análise da prova genética, o segundo extrato, demonstra uma postura crítica quanto ao posicionamento restritivo adotado por alguns países no sistema Prüm. As barreiras referidas pelo/a participante colocam tensões na ‘construção de uniformidades no tempo e no espaço’ (Brunsson & Jacobsson, 2005, p. 14) que, consequentemente, podem atrasar e/ou condicionar o processo de partilha de dados. A situação realçada no extrato põe a descoberto a dificuldade da estandardização quando esta é operada ao nível transnacional, neste caso em particular, devido a diferentes perceções sobre qual deve ser a utilização dos dados pessoais enviados aos países terceiros. Desta situação, depreende-se a importância da estabilização da “constellation of social relations surrounding DNA profiling” (Derksen, 2010, p. 215) na cooperação policial e judicial com base na partilha de informações genéticas. Neste caso em particular, é demonstrada uma posição crítica quanto à destituição do valor probatório da prova de DNA, sendo que a restrição já enunciada vem

colocar em causa a qualidade e a integridade científica dos testes realizados (Lynch, 2002, p. 218), bem como as próprias práticas policiais. Portanto, no panorama transnacional, a estandardização que visa assegurar a legitimidade e credibilidade do conhecimento científico (Shapin, 2001) e do sistema de justiça criminal encontra-se sujeita a tensões numa dimensão mais abrangente.

“Mas se nos dizem: ‘Não pode usar isto em tribunal’, como é que posso dizer como é que obtive a informação? Não a posso usar. Portanto, isto coloca uma barreira. Quero dizer, é uma correspondência de uma pessoa com DNA, porque é que não a posso usar? Todos praticamos os mesmos métodos científicos para decidir que esta é a pessoa, este é o DNA, correspondem. Temos os mesmos métodos científicos e todos somos certificados: ‘Porque me está a dizer que eu não posso usar esta informação em tribunal? Se a usa em tribunal no seu país’.” [U01]

Por fim, uma das medidas implementadas para garantir a privacidade e a proteção dos dados partilhados no sistema Prüm passa pela supervisão quer das bases de dados forenses de DNA, quer pelo processo de partilha de informações. No entanto, nem sempre é claro o papel dos órgãos de supervisão quanto às partilhas transnacionais por se assumir que a inspeção da base de dados forense de DNA é suficiente para evitar falhas na proteção de dados num plano internacional. Quanto ao modo como a supervisão é realizada, segundo os extratos apresentados, esta apoia-se maioritariamente na verificação aleatória, havendo exceções consoante os países em análise, dos dados consultados e guardados nas bases de dados de DNA ao nível nacional. Sendo que a janela temporal para a averiguação de possíveis lacunas na proteção de dados e privacidade não é homogénea entre os países. Recorrendo novamente aos excertos observa-se que a supervisão da base de dados forense pode ocorrer de 10 em 10 anos, como pode também realizar-se anualmente. Esta situação pode ser encarada enquanto problemática, pois num período de 10 anos é passível de ocorrerem situações de flagelo em relação à proteção de dados de um indivíduo que, certamente, demorarão demasiado tempo para serem descobertas e corrigidas de modo a restituir um dos direitos humanos fundamentais.

“A cada dez anos recebemos uma visita da comissão de proteção de dados para verificar os nossos registos. (...) Por isso havia algum tempo para fazer nova inspeção. Mas o nosso trabalho estava inspecionado. E agora também temos um responsável pela proteção de dados na polícia.” [X02]

“Essa supervisão da proteção de dados é realizada uma vez por ano. Eles fazem uma verificação aleatória, porque não podem verificar toda a gente. Pegam em 10 casos e verificam-nos cronologicamente, se alguma coisa estiver errada chamam-nos.” [S02]

De modo geral as percepções dos/as entrevistados/as a respeito dos órgãos de supervisão responsáveis pela privacidade e proteção de dados na partilha transnacional de dados forenses são vagas e sem reflexão a respeito da sua pertinência. Apesar do sistema Prüm, através dos dois passos, visar a criação de um *standard* mínimo de privacidade, o facto de não existir uma homogeneização das medidas de proteção de dados pode conduzir a uma supervisão ineficiente. Isto porque deixa ao critério dos Estados-Membros as medidas a serem adotadas ao nível da supervisão da base de dados forense de DNA, cujas informações podem ser partilhadas no âmbito da cooperação policial e judiciária. Neste sentido, na literatura, têm-se encontrado vozes críticas quanto à falta de investimento na supervisão ética do processamento dos dados pessoais e da sua consequente partilha transnacional no seio da União Europeia (Gonçalves & Jesus, 2012; Hufnagel & McCartney, 2015; McCartney, 2010, 2014a; McCartney et al., 2011; Prainsack & Toom, 2010, 2013).

A discussão em torno da privacidade e da proteção de dados no âmbito do sistema Prüm, salvo raras exceções, cinjiu-se à enunciação de algumas das medidas técnico-legais implementadas, como a utilização de *username* com palavra-passe e a existência de órgãos de supervisão. Deste modo, as narrativas a este respeito enquadram-se, na sua maioria, no minimalismo genómico (Williams & Johnson, 2004b). Sendo que a existência formal de medidas técnicas e legais, como as mencionadas, vêm escudar o sistema Prüm contra os argumentos associados à falta de investimento na privacidade e proteção de dados. Em número diminuto, as perspetivas de certos entrevistados/as encontram-se em linha com o pragmatismo biométrico (*idem*) por referirem que limitam a partilha de informações ao estritamente necessário atendendo aos motivos do pedido de cooperação.

Interoperabilidade entre bases de dados com diferentes finalidades

A interoperabilidade entre bases de dados forenses e biobancos médicos é uma das dimensões em análise no presente estudo, como já foi referido anteriormente neste capítulo. Importa realçar que sem os desenvolvimentos tecnológicos ocorridos nas últimas décadas, nomeadamente, ao nível da capacidade de armazenamento e da velocidade da transmissão de dados não seria possível encetar a criação de bases de dados interconectáveis (Goos et al, 2015; Mostert et al, 2016; Nissenbaum, 2010). No entanto, ainda que a criação de bases de dados possa permitir o melhoramento da qualidade de vida da sociedade nas suas várias esferas (Machado & Silva, 2015a), esta não é escudada contra certas vulnerabilidades. Remetendo, em particular, para as bases de dados forenses de DNA e os biobancos médicos, um dos pontos mais periclitante tem que ver com a garantia do direito à privacidade e proteção de dados associados a informação tipicamente classificada como sensível (Mostert et al, 2016). Relembre-se que os biobancos têm como principal enfoque a garantia da saúde pública (Gaskell et al., 2013) e os dados que constam nestas infraestruturas são voluntariamente cedidos por qualquer cidadão (Machado & Silva, 2015a). Ao passo que as bases de dados forenses se baseiam na manutenção da segurança da sociedade, onde as informações inseridas advêm de uma seleção de pessoas que, na maioria das vezes, teve algum tipo de contacto com o sistema de justiça criminal (Cho & Sankar, 2004; Machado & Silva, 2015; Patyn & Dierickx, 2010; Santos, Machado, Silva, 2013; Van Camp & Dierickx, 2008).

As perspetivas dos Pontos de Contacto Nacionais para o segundo passo do sistema Prüm em relação à interoperabilidade entre bases de dados forenses e biobancos serão analisadas à luz da categorização anteriormente proposta neste estudo (página 120). A categorização é composta por quatro categorias analíticas, nomeadamente, a ‘negação técnico-legal’, a ‘interoperabilidade pela excecionalidade’, a ‘negação pela finalidade’ e, por fim, a ‘interoperabilidade pela expansão’. As narrativas analisadas ilustram que o acesso a biobancos médicos para fins de investigação criminal é vantajoso para estes profissionais. No entanto, as mesmas narrativas, compreendem a interoperabilidade enquanto um procedimento bastante delicado no que toca à proteção dos dados que constam nestas infraestruturas. Motivo pelo qual nenhum/a dos/as participantes se mostrou favorável com a total conexão entre bases de dados forenses e biobancos médicos. O extrato abaixo

apresentado demonstra inequivocamente a dualidade da narrativa entre a utilidade e as preocupações éticas em torno deste tipo de interoperabilidade.

“Do que eu sei, não é permitido. A minha opinião pessoal é de que talvez devesse ser, iria ajudar. Mas, por questões de proteção de dados e de ética, deveria estar numa base de dados médica, para doação de medula óssea, e a minha informação ser verificada para propósitos de investigação criminal? Talvez não. Seria útil? Extremamente útil. Portanto, é uma linha muito ténue que tenho a certeza de que é difícil de responder para todas as pessoas.” [W01]

Como já referido, na sua maioria, os entrevistados performam narrativas que são favoráveis à interoperabilidade entre bases de dados forenses e biobancos médicos para fins de investigação criminal. No entanto, a reflexão sobre as questões éticas da interconexão levou parte dos profissionais do passo 2 a encetar soluções que entendem ser mais adequadas para a realização ética desta prática. Um dos pontos de maior preocupação foi o do direito à privacidade e proteção de dados das pessoas que constam nos biobancos. As sugestões de atuação passaram, substancialmente, pela imposição de regras e critérios de acesso que não permitissem o acesso ‘massivo’ e abusivo destes dados pessoais. No primeiro extrato, é referida a importância da limitação do fluxo e comunicação de dados médicos no decorrer de uma investigação criminal sob pena de atentar contra o direito à proteção de dados. No segundo excerto, o/a entrevistado/a sugere uma possível tipificação dos critérios de interoperabilidade baseada no tipo e na gravidade do crime em investigação de modo a evitar o desvirtuamento da utilização dos dados pessoais. Neste excerto realçam-se também as tensões entre o direito à proteção da privacidade e à segurança pública em situações extremas, como é exemplo o terrorismo (Bigo, 2008, p. 92). Apesar da reflexão acerca dos potenciais problemas éticos da interoperabilidade, o/a participante reconhece que esta prática pode ser uma ‘oportunidade’ relevante no âmbito de uma investigação criminal.

“Penso que se se limitar a quantidade de registos pode funcionar, mas não de uma forma massiva. Se se conseguir limitar de acordo com certos critérios o número

de registos, penso que será legítimo. Se não, não é aceitável do ponto de vista da proteção de dados.” [P01]

“Claro que é uma oportunidade muito importante para encontrar novos suspeitos. Em casos mais graves, porque não? Temos que os definir. Isto é, o nível [da gravidade]. Isto é, definitivamente, agressões físicas, homicídios, assassinatos (...). Mas tem que ser controlado, porque se coloca um rótulo [a dizer] ‘Terrorismo’ pode verificar o que quiser. Essa é a questão. Tem de ser realmente definido. Mas porque não?” [H02]

As narrativas dos entrevistados a respeito da prática de interoperabilidade entre bases de dados forenses e biobancos médicos enquadram-se na categoria de ‘interoperabilidade pela excecionalidade’. Pois, ainda que sejam favoráveis à conexão destas infraestruturas, entendem que existem riscos éticos no acesso desmedido a dados médicos para fins de investigação criminal, optando por uma postura que visa o condicionamento da prática. O facto de nenhum/a participante se opor completamente a esta opção pode estar relacionado com o seu perfil profissional, sendo que a maioria dos/as profissionais responsáveis pelo passo 2 do sistema Prüm possui um perfil tipicamente policial. Em particular, a noção de utilidade aliada à produção de inteligência segundo o princípio de máximo acesso à informação disponível para a investigação criminal é um dos modos de atuação privilegiados pelas instituições policiais (Innes et al, 2005; Machado & Granja, 2019a; Matos, 2019; Spapens, 2017). Deste modo, os/as entrevistados/as denotam que a interoperabilidade nestes moldes, através do condicionamento, pode auxiliar na produção de inteligência para uma condução mais eficiente da investigação de crimes.

CAPÍTULO 4. Análise empírica de dois estudos de caso: Portugal e Reino

Unido

O presente capítulo irá debruçar-se na comparação entre dois contextos nacionais – Portugal e Reino Unido – quanto à implementação do sistema Prüm através do conceito teórico de imaginários sociotécnicos cunhado por Jasanoff e Kim (2009). A relevância desta ferramenta teórica para o estudo prende-se pelo facto de permitir comparar diferentes realidades transnacionais relativamente ao mesmo fenómeno, neste caso em particular, a implementação do sistema Prüm. Esta comparação é realizada através da identificação dos imaginários sociotécnicos a respeito do desenvolvimento tecnológico e científico dos países em estudo (Pfotenhauer & Jasanoff, 2017, p. 783). Por outras palavras, pretende-se compreender de que modo a multiplicidade de narrativas que circulam nestas sociedades são apreendidas, filtradas e reinseridas na ação pública. A pluralidade de narrativas visa ser apreendida por via da análise de entrevistas semiestruturadas a vários profissionais envolvidos na área, designadamente: geneticistas forenses e outros *stakeholders* (membros de entidades de supervisão, de órgãos de investigação criminal, entre outros) em ambos os países.

O capítulo encontra-se dividido em três subtópicos, respetivamente, no enquadramento sócio-histórico, nas perspetivas dos geneticistas forenses e *stakeholders* e, por último, na perspetiva comparativa entre Portugal e o Reino Unido: o papel dos imaginários sociotécnicos. No primeiro subtópico são aprofundados os contextos sociais e históricos de Portugal e do Reino Unido aquando da criação das bases de dados forenses de perfis de DNA. Em particular, a respeito de Portugal abordam-se temas como o ambiente de formação e criação da base de dados, o contexto legal e regulatório da mesma (lei n.º 5/2008 e lei n.º 90/2017) e o papel do país na cooperação internacional. Relativamente ao Reino Unido procura-se dar conta do contexto de criação da base de dados (NDNAD), do panorama político à data, bem como do seu funcionamento, supervisão e estatísticas e o papel do país na cooperação transnacional. São também abordados o caso de S. e Marper *versus* Reino Unido e o ‘Protection of Freedoms Act 2012’ (PoFA) por terem influenciado diretamente a alteração de certos aspetos da NDNAD.

No segundo subtópico, em Portugal, são analisadas as seguintes dimensões à luz das entrevistas realizadas a geneticistas forenses e a *stakeholders*: 1) contexto legal da base de

dados forense de perfis DNA, 2) critério de inserção do perfil de DNA na base de dados forense, 3) vantagens e desafios do sistema Prüm, 4) privacidade e proteção de dados na base de dados forense, 5) interoperabilidade entre bases de dados forenses e biobancos e, por último, 6) direito ao apagamento dos dados - artigo 17.º do Regulamento (EU) 2016/679. No Reino Unido analisam-se as seguintes temáticas: 1) desafios éticos da utilização das bases de dados de perfis de DNA para fins forenses, 2) regime de retenção ‘Protection of Freedoms Act 2012’ na base de dados forense nacional, 3) vantagens e desafios do sistema Prüm, 4) envolvimento das entidades de supervisão no sistema Prüm, 5) implicações do contexto político do *Brexit* no sistema Prüm, e por fim, 6) interoperabilidade entre bases de dados forenses e biobancos. As dimensões analisadas verteram da análise dos dados e da teoria de acordo com os pressupostos da *grounded theory* (Charmaz, 2009; Strauss & Corbin, 1990). O subtópico final enceta a comparação empírica e teórica das dimensões previamente analisadas de modo a compreender e identificar os imaginários sociotécnicos a respeito do sistema Prüm e o seu papel nos diferentes modos de implementação deste sistema.

4.1. Enquadramento sócio-histórico

4.1.1 Portugal

A primeira lei portuguesa para o estabelecimento da base de dados forense de perfis de DNA viu a sua aprovação em fevereiro de 2008, denominada Lei n.º 5/2008. A base de dados possui duas faculdades, a de identificação civil e a de investigação criminal.

A discussão em torno da pertinência da base de dados de perfis de DNA para auxiliar na identificação civil e forense data de 2005 (Machado & Silva, 2010, p. 218). Num primeiro momento, a proposta avançada pelo Governo Português pretendia que fosse realizada a recolha integral dos perfis de DNA de toda a população portuguesa (*idem*). No entanto, segundo os especialistas que estiveram no comité responsável por esta iniciativa, existiram vários fatores que condicionaram esta opção generalista. Primeiro, em Portugal, a criminalidade grave é relativamente baixa quando comparada com outros países. Segundo, os recursos económicos necessários para um investimento desta envergadura, ao nível nacional, eram bastante limitados (Machado & Silva, 2008b). Por fim, esta prática não se enquadrava naquela que era a decisão de maior parte dos Estados-Membros que optaram

por restringir as suas bases de dados de perfis de DNA à população que já havia passado pelas malhas da justiça (Machado & Silva, 2010, p. 218).

Apesar de inicialmente se apontar para a criação de uma base de dados de DNA que abrangesse toda a população, a decisão política recaiu sobre a limitação da mesma à ‘população criminal’ (Machado, 2011, p. 157). No entanto, a base de dados forense tem-se apresentado como uma das mais restritivas e conservadoras quanto à informação que é incluída, sendo os procedimentos de preservação da qualidade dos dados dos mais exigentes (*idem*; Machado & Silva, 2010, p. 218). Os critérios para a inserção de perfis de DNA na base de dados exemplifica claramente o seu carácter tendencialmente restritivo. Apenas são inseridos na base de dados os perfis de indivíduos que sejam condenados a pena efetiva de prisão igual ou superior a três anos, por crime doloso (n.º 2 do artigo 8.º da Lei n.º 90/2017). Do mesmo modo, a lei portuguesa não permite a retenção indefinida dos perfis de DNA e da informação pessoal que constam na base de dados, os perfis e a informação são eliminados consoante os anos de prisão que o indivíduo tem de cumprir (n.º 3 do artigo 26.º da Lei n.º 90/2017). Os perfis de DNA e os correspondentes dados pessoais são eliminados decorrida a duração da pena de prisão concretamente aplicada acrescida de 5 anos, quando a pena tiver sido inferior a 5 anos; acrescida de 7 anos, quando a pena se situe entre 5 e 8 anos; acrescida de 10 anos, quando a pena seja superior a 8 anos; e acrescida de 23 anos, no caso de condenação por um crime previsto no capítulo V do título I do livro II do Código Penal.

Helena Machado e Susana Silva (2010) realçaram que as tecnologias forenses de DNA foram encaradas com bastante positivismo aquando da implementação da base de dados forense. As autoras referem como ilustrativo o anúncio da proposta de Lei n.º 5/2008 realizado no dia 1 de julho de 2007 pelo Ministro da Justiça. *Grosso modo*, foram destacados os três grandes contributos que uma base de dados forense de perfis de DNA poderia facultar ao país. Dito isto, realçou-se a sua capacidade na dissuasão e na resolução de crimes; de melhorar a justiça através de uma maior eficiência e rapidez na identificação da pessoa que cometeu um crime; e, por último, na sua capacidade de contribuir para o bem-comum e a confiança pública na justiça (Machado & Silva, 2010, p. 219). Num texto sobre perspetivas de peritos e políticos acerca da criação de uma base de dados de perfis de DNA em Portugal, Helena Machado (2011), avançou com três argumentos complementares à construção da (bio)segurança no país (p. 153), estando os mesmos em linha com o discurso

do então Ministro da Justiça. Primeiro, a ciência veio auxiliar à construção de um imaginário onde a justiça é mais eficaz e credível. Segundo, Portugal tem tentado manter-se a par do percurso dos países mais experientes na investigação criminal e na cooperação transnacional. Terceiro, a base de dados forense de perfis de DNA pode contribuir ativamente para a segurança coletiva da sociedade portuguesa. Os argumentos a favor da base de dados elencados pelos peritos e políticos são reveladores de um “imaginário coletivo assente no medo do crime e do criminoso” que, por consequência, relega para um plano inferior os riscos destas bases em prol das suas “promessas de utilidade imaginada e de eficácia de identificação de criminosos” (Machado, 2011, p. 153; ver também Lentzos, 2006).

Alberto Costa, Ministro da Justiça português, revelou também no seu discurso que a base de dados forense seria uma ferramenta fundamental para levar os culpados à justiça, bem como para exonerar os injustamente acusados (Machado & Silva, 2010, p. 219; Machado, 2011, p. 154). O discurso político que acompanhou a criação da Lei n.º 5/2008 permeou-se da conceção generalizada de que a ciência desempenha um papel importante na justiça (Jasanoff 2006; Lynch et al. 2008), à semelhança do que os trabalhos citados de Machado e colegas demonstram. Sob esta ótica através da ciência aplicada é possível tornar a investigação criminal mais célere e objetiva e, consequentemente, tornar a justiça e os tribunais mais eficientes. Um estudo realizado ao nível nacional sobre perspetivas públicas em relação à base de dados forense de DNA demonstrou que a maioria dos participantes entendem que a base de dados portuguesa é uma ferramenta útil para ‘combater’ eficientemente o crime e tornar a justiça mais eficaz (Machado & Silva, 2015b, p. 1; Machado & Silva, 2016). A exaltação destas características e a dissipação discursiva dos riscos e desafios da criação das bases de dados forenses têm sido responsáveis por “efeitos sociais, culturais e éticos que convergem para dispositivos retóricos destinados a apoiar mecanismos de construção de confiança pública” (Machado, 2011, p. 155). A confiança pública, por sua vez, assenta na conceção do perfil de DNA como objeto da ciência que permite inquestionavelmente identificar a pessoa que deixou a sua marca genética num local onde um crime foi perpetrado (Aas, 2006, p. 150). Machado e Costa (2012) argumentam, a este respeito, que a utilização das tecnologias de DNA por parte de Portugal pode gerar impactos nos níveis de confiança pública que os cidadãos demonstram em relação ao sistema judicial (p. 62).

A necessidade de acompanhar os parceiros europeus foi bastante enfatizada aquando da aprovação da Lei n.º 5/2008. Foi referido no mesmo discurso que Portugal deveria seguir o exemplo dos países mais desenvolvidos em relação à utilização dos perfis de DNA para auxílio na investigação criminal, bem como a adesão a sistemas de cooperação transnacional que visavam a promoção de políticas de segurança e de ‘combate’ ao crime (Machado & Silva, 2010, p. 219; Machado, 2016, p. 12). As palavras do Ministro da Justiça permitem perceber o clima político português no momento da criação da base de dados forense de DNA, bem como da introdução das tecnologias de DNA aplicadas à ciência forense (Machado & Silva, 2010, p. 220). O imaginário positivista que revestiu o discurso em torno da criação de uma base de dados forense de DNA e o seu contributo para o bem-comum é a primeira plataforma para a análise das questões sociais, éticas e legais que advêm da utilização das tecnologias forenses de DNA em contexto nacional. A elevada aceitação desta iniciativa política por parte da sociedade portuguesa teve que ver com a perspicácia no realce daqueles que eram os medos da sociedade. Em particular, o medo do crime, regularmente fomentado pelos meios de comunicação que, por sua vez, se mescla com o sentimento de insegurança generalizada e o decréscimo da confiança nos sistemas de justiça criminal (Fox et al. 2007; Contini & Mohr 2007; Machado & Silva, 2010, p. 220). Parafraseando Machado e Silva (2010) a ideia de otimização do sistema de justiça através das tecnologias forenses de DNA mostrou-se um dos fatores mais preponderantes para a adoção deste tipo de tecnologia de prevenção e resolução do crime (*idem*; Williams & Johnson, 2005).

A aparente aura de aceitação das tecnologias forenses (e da base de dados forense de DNA) não foi suficiente para invisibilizar certos pontos críticos em relação à perceção dos portugueses quanto ao seu sistema de justiça. Alguns trabalhos mostraram que os portugueses possuem uma perceção pouco favorável quanto ao sistema de justiça e à investigação criminal no país (Santos et al. 1996; Costa 2003). Tendencialmente os cidadãos portugueses entendem que a justiça não está devidamente protegida contra pressões externas perpetuadas por pessoas em lugares de poder. Em relação à investigação criminal identificam três situações problemáticas: a corrupção, problemas com a confidencialidade e a falta de segurança da informação que detêm acerca das pessoas que estão a investigar (Machado & Silva, 2010). De modo complementar, os portugueses revelaram-se preocupados com a falta de segurança a respeito do controlo e acesso dos dados pessoais e

a possibilidade de os dados genéticos serem utilizados para fins diferentes dos que motivaram a sua recolha (*function creep*) (Machado & Silva, 2015b, p. 1). Numa outra perspetiva levanta-se ainda a noção de proporcionalidade associada à criação da base de dados (Machado & Silva, 2010, p. 220). Neste sentido, é questionada a pertinência da sua existência face aos custos de manutenção e à reduzida taxa de criminalidade grave. A este respeito, Machado e Silva (2008a) argumentam que é igualmente importante refletir sobre o elevado investimento nas tecnologias forenses de DNA quando as políticas portuguesas de reabilitação social de pessoas que cometeram crimes continuam a ser demasiado escassas.

Contexto legal e regulatório – Lei n.º 90/2017

A criação da base de dados forense de perfis de DNA foi aprovada em 2008 pela Lei n.º 5/2008 de 12 de fevereiro. Em 2017 a lei sofreu novas alterações nas disposições iniciais através da Lei n.º 90/2017 de 22 de agosto. Este documento pretendeu estabelecer os princípios de criação e manutenção da base de dados e a regulação da recolha, tratamento e conservação das amostras biológicas, bem como a metodologia de análise e obtenção de perfis de DNA e o tratamento e conservação da respetiva informação em ficheiro informático (n.º 1 do artigo 1.º da Lei n.º 90/2017). Deste modo, a base de dados forense só pode ser acedida para fins de identificação civil e de investigação criminal (n.º 1 do artigo 4.º da Lei n.º 90/2017). A identificação civil é realizada, nos termos da lei, através da comparação de perfis de DNA relativos a amostras de material biológico colhido em pessoa, cadáver, parte de cadáver ou local onde se proceda a recolhas com aquelas finalidades, bem como a comparação daqueles perfis com os existentes na base de dados de perfis de DNA, com as limitações previstas nos artigos 19.º e 19.º-A (n.º 2 do artigo 4.º da Lei n.º 90/2017). A investigação criminal é realizada através da comparação de perfis de DNA relativos a amostras de material biológico colhidas em locais de crimes e em pessoas que, direta ou indiretamente, a elas possam estar associadas, com os perfis de DNA existentes na base de dados de perfis de DNA, com vista à identificação dos respetivos agentes, sem prejuízo das limitações previstas nos artigos 19.º e 19.º-A (n.º 3 do artigo 4.º da Lei n.º 90/2017). O acesso à base de dados para fins de estatística ou de investigação científica também se encontra regulado na lei. Deste modo, a informação obtida a partir dos perfis de DNA pode ser comunicada para fins de investigação científica ou de estatística, após anonimização irreversível da mesma (n.º 1 do artigo 23.º da Lei n.º 90/2017).

O Instituto Nacional de Medicina Legal e Ciências Forenses (INMLCF) foi a entidade nomeada responsável pela base de dados e pelas operações que lhe sejam aplicáveis (n.º 1 do artigo 16.º da Lei n.º 90/2017). O INMLCF é uma instituição pública que se encontra sob a supervisão do Ministério da Justiça. Pode ler-se no *site* do Instituto³³ que este tem como missão a “cooperação com os tribunais, com o Ministério Público e com os órgãos de polícia criminal e demais serviços e entidades que intervêm no sistema de administração da justiça” através da realização de “exames e perícias de medicina legal e forenses que lhe forem solicitados, nos termos da lei, bem como prestar-lhes apoio técnico e laboratorial especializado, no âmbito das suas atribuições”. No que concerne às atividades realizadas no âmbito da gestão e manutenção da base de dados, o INMLCF é, nos termos da lei, fiscalizado por uma entidade independente criada para o efeito – o Conselho de Fiscalização da Base de Dados de Perfis de ADN (CFBDP ADN)³⁴ (n.º 5 do artigo 16.º da Lei n.º 90/2017). O Conselho responde apenas perante a Assembleia da República e é composto por três cidadãos de reconhecida idoneidade e no pleno gozo dos seus direitos civis e políticos (n.º 2 e n.º 3 do artigo 29.º da Lei n.º 90/2017). A entidade responsável pela base de dados tem ainda a obrigação de consultar a Comissão Nacional de Proteção de Dados (CNPd)³⁵ para quaisquer esclarecimentos quanto ao tratamento de dados pessoais, devendo cumprir as deliberações desta Comissão nesta matéria (n.º 2 do artigo 17.º da Lei n.º 90/2017).

A lei portuguesa respeitante a esta matéria clarifica também a definição de ‘ficheiro de perfis de DNA’. A base de dados para identificação civil e criminal define-se como um conjunto estruturado de perfis de DNA, acessível segundo critérios determinados (alínea i do artigo 2.º da Lei n.º 90/2017). A base de dados pode ser expandida através da inserção de sete tipos de ficheiros de perfis de DNA, nomeadamente, informação relativa 1) a amostras de voluntários; 2) a amostras-problema para fins de identificação civil; 3) a amostras-referência de pessoas desaparecidas (ou dos parentes); 4) a amostras-problema para fins de investigação criminal; 5) a amostras de pessoas condenadas em processo criminal (por crime doloso com pena concreta igual ou superior a três anos) por decisão judicial transitada em julgado; 6) a amostras dos profissionais que procedem à recolha e análise das amostras; por fim, 7) a amostras de arguidos em processo criminal, em que seja

³³ Disponível em http://www.inmlcf.mj.pt/index.php?option=com_content&view=article&id=122&Itemid=288. Acesso a 12 de maio de 2020.

³⁴ Disponível em <https://www.cfbdadosadn.pt/pt/Paginas/default.aspx>. Acesso a 12 de maio de 2020.

³⁵ Disponível em <https://www.cnpd.pt/>. Acesso a 12 de maio de 2020.

aplicável pena igual ou superior a três anos de prisão, os quais não podem ser considerados para efeitos de interconexão fora dos casos previstos (ficheiro provisório) (n.º 1 do artigo 15.º da Lei n.º 90/2017). Uma das alterações mais significativas entre o documento de 2008 e a Lei n.º 90/2017 tem que ver com a possibilidade de criação e inserção na base de dados de ficheiros relativos às amostras dos arguidos, até então não constava no enquadramento legal português.

Os critérios para a eliminação dos perfis de DNA, foram atualizados com a aprovação da Lei n.º 90/2017 (artigo 26.º). A atualização da lei veio atestar que a eliminação do perfil de DNA já não se encontra dependente do cancelamento do registo criminal, passou a ser realizada em consonância com os anos de pena concreta que foi decretada à pessoa condenada (n.º 3 do artigo 26.º da Lei 90/2017). Pelo que, quanto maior a pena concreta aplicada ao indivíduo, maior será o tempo de retenção do perfil e das informações pessoais na base de dados de perfis de DNA. A eliminação dos perfis obtidos através das amostras-problema é realizada se se verificar a sua identificação pelo perfil de uma pessoa condenada ou, caso não haja identificação, vinte anos após a sua inserção na base de dados. A alteração dos critérios de eliminação dos perfis das pessoas condenadas veio mudar o paradigma inicial da base de dados neste tópico. Inicialmente a remoção do perfil de DNA era realizada em simultâneo com o cancelamento do registo criminal para que a pessoa condenada pudesse ingressar novamente na sociedade sem o estigma de que tinha cometido um crime (Machado et al., 2013, p. 6; Machado et al., 2012, p. 180). Porém, atualmente, os critérios plasmados na Lei n.º 90/2017 vieram colocar pressão na chamada tradição humanista do sistema penal português (Machado et al., 2012; Moniz, 2009), pois os prazos de retenção dos perfis de DNA têm vindo a aumentar. Apesar da tendência da base de dados ser a da expansão, em Portugal, os juízes continuam a ser as figuras responsáveis pela construção da base de dados forense (Machado, 2016, p. 11). A opção do legislador pode ser vista sob o prisma da proteção dos direitos civis individuais. Deste modo, pretendeu-se a garantia dos direitos humanos fundamentais e a dissipação de potenciais maus usos e abusos de poder pelas entidades policiais no acesso e, consequente, utilização das informações que constam na mesma (*idem*).

A procura por uma base de dados protetora dos direitos dos cidadãos tem sido encarada como um obstáculo à própria investigação criminal. Primeiro, porque tem-se constatado que os juízes não têm ordenado com a frequência desejável a inserção de perfis

na base de dados (Machado, 2016, p. 11). Segundo, porque a informação que consta na base de dados não é comunicada diretamente ao Ministério Público ou às entidades policiais, inicialmente é comunicada ao juiz que decide, por meio de requerimento fundamentado, se é ou não importante transmitir a informação às entidades citadas (artigo 20.º da Lei n.º 90/2017). Sendo que, no entender das forças policiais a comunicação por intermédio do juiz dificulta o trabalho de investigação criminal que, por sua vez, limita as potencialidades da base de dados anunciadas publicamente (Costa, 2014; Machado & Costa, 2012, p. 67; Santos, Costa & Machado, 2012).

Sumariamente, em Portugal, o DNA pode ser utilizado em três vertentes, respetivamente, na identificação de suspeitos, na identificação de vítimas de crimes e no decurso de uma investigação de paternidade e/ou de maternidade (Machado, 2005, p. 4). A utilização de informação pessoal para fins de identificação no contexto da investigação criminal gera questões éticas, sociais e políticas diferentes das que são levantadas no âmbito da identificação civil. Por um lado, as bases de dados forenses de DNA são questionadas em torno do conceito de proporcionalidade e do equilíbrio entre as liberdades individuais e a necessidade de segurança coletiva. Em particular, “the proper balance between preventing, detecting and prosecuting crime and individual rights to liberty, autonomy and privacy” (Machado & Silva, 2010, p. 222; ver também Nuffield Council on Bioethics 2007). Por outro lado, a identificação civil através de uma base de dados de DNA é encarada, de modo generalizado, como uma prática desejável, pois vem possibilitar a identificação de indivíduos desaparecidos e de cadáveres (ou partes de um corpo) não identificados (Machado & Silva, 2010). Realce-se que a identificação nestes moldes só tem taxas de sucesso elevado se a base de dados for alimentada com os perfis genéticos da população em geral (familiares de pessoas desaparecidas, voluntários). Ambas as finalidades da base de dados forense de DNA, ainda que com níveis de aceitação pública diferentes, podem ser encaradas à luz da vontade Estatal relativamente ao controlo dos cidadãos através de uma monitorização física, moral e social dos seus corpos e comportamentos (Monahan, 2006).

Colocando em retrospectiva os aspetos elencados a respeito do enquadramento legal da base de dados forense de DNA constata-se que esta é uma das mais restritivas no seio da União Europeia (Machado, 2016, p. 11; Machado, Moniz, Santos, & Silva, 2011; Santos et al., 2013). Concretamente em relação aos critérios de inserção de perfis de DNA, à recolha de

amostras de DNA e aos critérios de eliminação dos perfis e de amostras de DNA. O caráter restritivo que lhe é atribuído pode ser entendido como uma vontade política de manter os direitos dos seus cidadãos protegidos (Dias, 2007). No entanto, a alteração à Lei n.º 5/2008 pode ser encarada como um esforço para expandir a utilização e a dimensão da base de dados que se deu através da revisão dos prazos de eliminação dos perfis de DNA e da simplificação do procedimento de inserção de perfis na base de dados. Anteriormente eram necessários dois requerimentos por parte do juiz: o primeiro para solicitar a recolha da amostra para obtenção do perfil de DNA e o segundo para pedir a sua inserção na base de dados. Na Lei n.º 90/2017 o pedido do juiz para a recolha de amostra e a inserção do perfis de DNA é realizado no mesmo requerimento. Esta mudança legal é a materialização daquilo que Machado e Silva (2008b) tinham previsto através do seu trabalho, onde especialistas legais e cientistas forenses defendiam que a utilização da bases de dados forense de DNA iria aumentar ao longo dos anos.

Lacunas e incertezas sobre a Lei n.º 5/2008 – Lei n.º 90/2017

Alguns trabalhos realizados na época da criação da primeira lei da base de dados forense de perfis de DNA portuguesa dão-nos conta de perspetivas aparentemente contraditórias (Machado & Silva, 2010). Se por um lado, se verificava existir consenso quanto ao caráter restritivo da base, que, por sua vez, poderia condicionar a eficácia da mesma. Por outro lado, observaram-se expectativas elevadas, por parte dos especialistas entrevistados no âmbito desses estudos, em relação à capacidade da base de dados enquanto ferramenta fundamental para a identificação de pessoas que cometeram crimes (*idem*; Williams et al., 2004, p. 12). A base de dados forense de perfis de DNA em Portugal foi criada num clima particular, onde o consenso partidário foi um dos fatores mais relevantes para a sua criação. Deste modo, tentou redigir-se um documento que não levantasse demasiadas objeções quanto à reflexão a respeito dos direitos individuais dos cidadãos portugueses (Machado & Silva, 2010, p. 226). Ainda que isso incluísse a criação de uma lei mais conservadora quanto à inserção e eliminação de informações na base de dados. Acreditando-se que, sendo esta uma lei restritiva, com o tempo e as mudanças sociais portuguesas, pudesse adquirir um caráter mais expansivo que lhe permitisse aumentar a sua dimensão à semelhança dos restantes Estados-Membros (*idem*).

A regularização do Conselho de Fiscalização da base de dados continua, mesmo após a alteração de 2017, a deixar questões em aberto. Tal como supramencionado esta entidade é responsável por supervisionar as atividades da base de dados e deve anualmente redigir um relatório público para apresentar ao parlamento português. O modo de nomeação dos elementos constitutivos do Conselho carece de regras mais claras a este respeito. Em particular, não foi realizado um aprofundamento daquilo que é o conceito de idoneidade, nem quais os critérios que devem ser tomados em consideração no momento da escolha da pessoa. Pelo que deixa à subjetividade um número desconhecido de elementos/critérios que podem ou não ser equacionados no momento da nomeação dos elementos do Conselho de Fiscalização.

O Conselho de Fiscalização tem sido assegurado, na sua maioria, por pessoas com formação académica em direito, existindo ainda alguns elementos, em menor número, com formação académica em áreas das ciências naturais e exatas. Neste sentido, Machado e Silva (2010) argumentam que o Conselho de Fiscalização não deveria limitar os elementos a pessoas com formação específica, pois, no seu entender, qualquer cidadão poderia integrar este órgão fiscalizador (p. 227). Complementam que seria através da nomeação de pessoas da sociedade civil que se conseguiria promover uma maior transparência e prestação de contas tanto ao Parlamento como à sociedade em geral no que remete para as atividades da base de dados forense de perfis de DNA (*idem*; Williams et al. 2004, p. 63). As autoras realçaram ainda a importância de se avançar com uma campanha de clarificação e sensibilização sobre a base de dados forense tanto ao nível nacional, como transnacional (Machado & Silva, 2010, p. 228; Murtuja et al. 2008). No entanto, passados dez anos não se verificou nenhuma iniciativa nacional suficientemente relevante a este respeito.

A base de dados forense prevê desde a sua primeira lei a recolha de amostras em voluntários para posterior inserção do perfil de DNA na base (artigo 6.º da Lei n.º 90/2017). No entanto, não foram apresentados os motivos pelos quais os cidadãos se deveriam voluntariar, ou quais as situações em que poderia ser útil constar na base de dados (por exemplo, em caso de desastre, profissões de risco). A opção de permitir a inserção de um perfil de DNA de um voluntário não foi problemática considerando que a proposta inicial era a da criação de uma base de dados universal que não viu a sua conclusão devido, essencialmente, ao dispêndio elevado de recursos (Machado, et al., 2012, p. 183). No entanto, a expectativa de que os cidadãos se iriam voluntariar para a base de dados forense

era demasiado baixa (Machado & Silva, 2010, p. 228). Esta situação veio a confirmar-se com o reduzido número de voluntários, dados do CFBDP ADN de junho de 2018 comprovam que entre o período de 2013 e 2018 apenas foram inseridos quatro perfis de voluntários³⁶ (desde 2013 que não se procede a nenhuma nova inserção). No entender de alguns especialistas a opção de se criar uma entrada voluntária na base de dados teve como objetivo dissipar as preocupações que certos políticos foram levantando a respeito dos direitos civis dos cidadãos portugueses (Machado & Silva, 2010, p. 228). Num plano macro do planeamento legal e político, foi representado um imaginário de que a base de dados é uma ferramenta útil e benéfica para a sociedade. Num plano micro, o discurso dos especialistas e o reduzido número de voluntários vêm contrariar o aparente otimismo em relação à base de dados.

Quanto à amostra de DNA do voluntário, esta só pode ser recolhida após o seu consentimento livre, informado e escrito (n.º 1 do artigo 6.º da Lei n.º 90/2017). Previamente ao consentimento, o cidadão que esteja interessado em ser inserido na base de dados “deve endereçar, por escrito, o seu pedido de recolha de amostras às entidades competentes para a análise laboratorial” (n.º 2 do artigo 6.º da Lei n.º 90/2017). Dito isto, Machado e Silva (2010) argumentam que esta disposição legal possui uma conotação simbólica pois maximiza o valor da escolha e da responsabilidade que os cidadãos possuem na manutenção da ordem e segurança pública através da doação da amostra genética ao Estado (p. 229). Nesta ótica o bom cidadão, o cidadão cumpridor da lei, tem o dever de doar uma amostra de DNA a favor do bem-coletivo (Rose & Novas, 2005, p. 440). O argumento por de trás da noção de que o bom cidadão coopera com o Estado pode colocar tensão acrescida ao caráter voluntário deste tipo de prática. Pois pode tornar implícita a obrigação daquela que é uma opção voluntária para o reconhecimento da categoria de bom cidadão (Marx, 2006). Em particular, potencia a criação de uma hierarquia social entre ‘criminosos’ e cidadãos cumpridores da lei. Sendo que esta diferenciação social assenta no princípio da obrigatoriedade implícita da partilha voluntária de informações e do perfil de DNA. Pois a decisão de não partilhar informações pessoais pode conduzir à suspeição do indivíduo em causa.

³⁶ Disponível em <https://www.cfbdadosadn.pt/pt/bdpadn/sobreabd/Paginas/ConteudoFicheiros.aspx>. Acesso a 12 de maio de 2020.

Na primeira versão da lei, os perfis de DNA resultantes das amostras recolhidas aos voluntários podiam ser cruzados com todos os perfis inseridos na base de dados (n.º 3 do artigo 20.º da Lei n.º 5/2008). No entanto, em 2017, esta disposição sofreu alterações significativas. Segundo a nova lei, os voluntários da base de dados forense apenas estão isentos do pagamento dos custos de obtenção do perfil de DNA se autorizarem o cruzamento do seu perfil para efeitos de investigação criminal (n.º 4 do artigo 6.º da Lei n.º 90/2017). Desta forma, pode entender-se esta alteração segundo dois prismas. Primeiro, dar ao cidadão a oportunidade de não ter o seu perfil de DNA cruzado com outros perfis para fins de investigação criminal veio acrescentar uma alínea na proteção dos seus direitos individuais. Segundo, isentar os cidadãos que autorizem o cruzamento do seu perfil no âmbito da investigação criminal dos custos pode ser entendido como uma forma de recompensar aqueles que auxiliam o Estado a zelar pelo bem-coletivo. Esta alteração veio colocar uma maior responsabilização no cidadão em relação à sua opção, pois com a nova reconfiguração legal é o cidadão que decide se quer ou não ver o seu perfil cruzado para fins de investigação criminal.

Cooperação internacional e Portugal

A criação da base de dados forense em Portugal resultou em grande medida da transposição do Tratado de Prüm para a lei da União Europeia em 2008 – Decisões Prüm. Após o ano de 2008 todos os Estados-Membros foram obrigados a criar uma base de dados forense de perfis de DNA com vista à cooperação transnacional para fins de investigação criminal. A cooperação obrigou a um certo nível de estandardização dos protocolos de obtenção de perfis de DNA por parte dos laboratórios. Contudo, existem vários aspetos que são reveladores das diferenças estruturais locais entre Estados-Membros, por exemplo, ao nível da disponibilidade de recursos, do enquadramento legal, do sistema judicial e da própria investigação criminal.

Portugal tem-se consolidado como um dos países com a legislação mais restritiva da União Europeia em relação à inserção, retenção e eliminação de informação relativa aos perfis de DNA (Machado, 2016, p. 11; Machado et al., 2011; Santos et al., 2013). No entanto, a pressão ao nível externo, de sistemas como o de Prüm tem conduzido a alterações na lei procurando a maximização da sua eficácia e o aumento do número de perfis de DNA na base. A este respeito, Machado e Silva (2010) referem no seu trabalho que

o Governo português possui uma narrativa que vai no sentido de “acompanhar a evolução dos outros países” (p. 233), justificando as alterações legais em relação à base de dados de perfis de DNA.

Denote-se que as alterações efetuadas à Lei n.º 5/2008 pretenderam diluir os obstáculos causados à inserção de perfis de DNA na base de dados. Deste modo, verificou-se um esforço no sentido de se aumentar o número de perfis resultantes de amostras-problema dos locais de crime. A nova versão da lei veio permitir a inserção de perfis de amostras-problema por parte de outra entidade para além do INMLCF, no caso, o Laboratório da Polícia Judiciária (alínea a do n.º 3 do artigo 17.º e n.º 4 do artigo 18.º da Lei n.º 90/2017). Relativamente à inserção de perfis de DNA resultantes de amostras-referência verificou-se também a simplificação do processo de autorização para inserção na base de dados. Sob a alçada da Lei n.º 5/2008 eram necessários dois despachos de um juiz para permitir a inserção dos perfis de DNA na base de dados. No primeiro despacho era ordenada a recolha da amostra de DNA ao indivíduo e só no segundo despacho era ordenada a sua inserção na base de dados. No novo contexto legal apenas é requerida a realização de um despacho que ordena que a “recolha de amostra em arguido condenado por crime doloso com pena concreta de prisão igual ou superior a 3 anos (...) com a consequente inserção do respetivo perfil de DNA na base de dados, é sempre ordenada na sentença” (n.º 2 do artigo 8.º da lei 90/2017).

4.1.2 Reino Unido

No Reino Unido tem-se assistido a um longo percurso quanto à recolha de material genético para posterior armazenamento numa base de dados de perfis de DNA para fins de identificação criminal. O armazenamento forense de perfis de DNA em bases de dados é realizado em todas as Nações constituintes do Reino Unido, no entanto as bases de dados são independentes e, consequentemente, os enquadramentos legais são diferentes (Amankwaa, 2018, p. 458; Johnson & Williams, 2004, p. 2). A primeira base de dados foi criada em 1995 pela Inglaterra e o País de Gales – *National DNA Database* NDNAD (Amankwaa, 2018, p. 455) e a sua gestão está, desde outubro de 2012, ao encargo do *Home Office*³⁷ encontrando-se sob custódia policial (Home Office, 2017). A NDNAD é a base de

³⁷ Ministério do Interior (*Home Office*): ministério responsável pela imigração, segurança, lei e ordem.

dados forense de perfis de DNA mais antiga do mundo e com um maior número de população inserida (Downey et al., 2012; Johnson & Williams, 2007). Segundo o relatório anual do *NDNAD Strategy Board*³⁸ apenas trinta funcionários do ministério possuem autorização de acesso completo à base de dados, por sua vez, as forças policiais têm acesso aos perfis de DNA e a notificações de correspondências (*hits*) entre perfis (Home Office, 2017). Devido à ampla dimensão e à sua utilização por parte da investigação criminal, a base de dados de perfis de DNA tem estado constantemente no centro de várias controvérsias éticas devido às consequências sociais que derivam das práticas de inserção e retenção de perfis de DNA (Human Genetics Commission, 2009; Nuffield Council on Bioethics, 2007; Skinner, 2013).

A base de dados Escocesa de perfis de DNA tem a sua manutenção à responsabilidade da *Police Forensic Science Laboratory Dundee*³⁹ (PFSLD) e é financiada por um conjunto de três forças policiais (*Tayside, Fife e Central Scotland*). Apesar de se apresentar como uma base de dados independente, são enviadas regularmente cópias dos seus perfis de DNA para a NDNAD (Johnson & Williams, 2004, p. 2). A base de dados forense de DNA da Irlanda do Norte está a cargo da *Forensic Science Northern Ireland*⁴⁰ (FSNI) e a sua custódia pertence às forças policiais nacionais. Neste caso, também se verifica a exportação de ficheiros de perfis de DNA para a NDNAD (Amankwaa, 2018). Tal como Johnson e Williams (2004) realçam, o recurso às bases de dados em todas as jurisdições do Reino Unido para auxílio na investigação criminal dá-se através de acordos bilaterais que permitem a partilha de dados relativos a perfis de DNA para fins de investigação forense.

Base de dados forense nacional – Contextualização da criação e do panorama político

A NDNAD foi criada sob a ótica que o recurso à genética na investigação criminal seria um passo fundamental para o aumento da eficácia na deteção e detenção do crime. Ao modo como a polícia e o Governo, à data da sua criação, entenderam o potencial da genética em meio policial é denominado de ‘imaginário forense’ (Williams, 2010). Sendo que, a base de dados forense, de forma semelhante às restantes bases de dados de material

³⁸ Entidade responsável pela governação e supervisão da NDNAD

³⁹ Laboratório de Ciências Forenses da Polícia Dundee (*Police Forensic Science Laboratory Dundee*): fundado em 1989. Possui 4 departamentos: biologia, química, base de dados de DNA e qualidade/administração.

⁴⁰ Ciência Forense da Irlanda do Norte (*Forensic Science Northern Ireland*): entidade afeta ao departamento da Justiça; tem como missão o fornecimento de apoio e aconselhamento científico imparcial, para melhorar o Sistema de Justiça Criminal. Disponível em <https://www.justice-ni.gov.uk/articles/about-forensic-science-northern-ireland>. Acesso a 12 de maio de 2020.

biológico, é apreendida enquanto ‘objeto promissor’ cujo valor potencial se situa no plano futuro ao invés do presente (Brown, Kraft, & Martin, 2006; Tutton & Levitt, 2010). Os argumentos que motivam a criação destas bases de dados focam-se na identificação das capacidades futuras destas ferramentas mitigando possíveis análises de custo-benefício no presente. Um aspeto revelador do imaginário futuro é o aumento do número de perfis de DNA na NDNAD ocorrer em paralelo com a diminuição das taxas de criminalidade, ainda que o medo do crime e a resposta policial/judicial ao mesmo se revelasse mais intensa (McCartney et al., 2010; Skinner, 2013, p. 978).

Os discursos políticos em torno da NDNAD podem dividir-se em dois intervalos de tempo (Downey et al., 2012, p. 445). O primeiro, situado nos anos anteriores a 2006, onde a base de dados era encarada enquanto ferramenta fundamental para o ‘combate’ ao crime. O segundo, nos anos que procederam 2006, onde esta começou a ser entendida como um potencial perigo para as liberdades civis dos cidadãos britânicos (*idem*). A clivagem nos imaginários a respeito da base de dados forense está intimamente relacionada com o contínuo aumento da inserção de perfis de DNA de pessoas inocentes, situação que gerou tensão na relação de confiança entre o Estado e os cidadãos (*idem*). Vozes críticas do funcionamento da base de dados já se tinham feito ouvir em 2001 (por exemplo, através da Ministra Ann Widdecombe). Contudo, só em 2006 ocorreu uma maior expressão destas preocupações por parte da comunicação social e da comunidade política (*idem*, p. 446).

As preocupações elencadas em relação ao funcionamento da bases de dados vão além da inserção e retenção indiscriminada de perfis de DNA de pessoas inocentes e da presença de perfis de DNA de crianças/menores. Skinner (2013) dá-nos conta de que a “ethnicity plays a ambiguous but highly significant part in the operation and outcomes of the NDNAD” (p. 981). A sobrerrepresentação de homens negros considerados inocentes (em tribunal) na base de dados tem gerado intenso debate em torno da problemática do racismo institucionalizado das forças policiais (Downey et al., 2012, p. 449). Em números, cerca de um terço da população negra e três quartos dos jovens negros têm o seu perfil de DNA inserido na base de dados (*idem*). Devido à sobrerrepresentação de pessoas negras na NDNAD tem-se gerado uma intensa discussão em torno das questões de raça, etnicidade e racismo. A título de exemplo seguem algumas das entidades que se têm dedicado à produção de relatórios e debates em torno da temática: *Human Genetics Commission*, *Commission for Racial Equality*; *Equality and Human Rights Commission*; *Nuffield Council on*

Bioethics, Black Mental Health, Liberty, GeneWatch, Privacy International, No2ID, Runnymede Trust (Skinner, 2013, p. 982).

A manutenção da NDNAD tem sido realizada a par de desafios de ordem operacional, ética e legal (*idem*, p. 980). Ao nível operacional é necessário compreender se o alto investimento de recursos nesta ferramenta resultou no aumento das taxas de deteção do crime (McCartney, 2006b). Ao nível ético, a expansão generalizada das bases de dados forenses tem colocado tensões sobre a proporcionalidade dos critérios de inserção, acesso e destruição dos perfis de DNA, a privacidade genética e a propriedade dos dados que constam na mesma (Hindmarsh & Prainsack, 2010). Ao nível legal, a NDNAD viu o seu enquadramento legal alterado no decorrer de uma decisão do Tribunal Europeu dos Direitos Humanos, em 2008, onde se decidiu que a retenção permanente de perfis de DNA de pessoas presas, mas não condenadas, não era proporcional (“Case of S. and Marper v. The United Kingdom” 2008).

Devido ao ‘imaginário forense’ (Williams, 2010) e aos imaginários sociotécnicos (Jasanoff & Kim, 2009) a respeito da base de dados, estudos mostram que, *grosso modo*, o público apoia a retenção a longo prazo/permanente de perfis de DNA de pessoas condenadas e de suspeitos (Amankwaa, 2018, p. 455). Também a retenção de perfis de todos ou parte dos detidos usufrui do apoio público. Contudo, um número elevado de pessoas opõe-se à retenção de perfis de DNA de inocentes devido a questões relacionadas com a privacidade e os potenciais usos desadequados da informação retida (*idem*). As perceções a respeito da retenção de perfis de DNA são diferentes consoante os seus grupos de pertença (*idem*, p. 460). Por um lado, os profissionais de justiça criminal tendem a defender a retenção permanente ou a longo prazo de toda a informação dos detidos. Por outro lado, os defensores dos direitos humanos e as pessoas sujeitas à recolha de amostras de DNA no ato da detenção tendem a apoiar a retenção temporária ou a não retenção dos dados das pessoas detidas. Genericamente, os argumentos a favor da retenção de perfis de DNA de detidos baseiam-se na possibilidade da futura deteção de crimes graves; na noção de que o cidadão cumpridor da lei não tem nada a esconder (Crossman, 2008); e no aumento da celeridade da investigação por ser mais fácil a eliminação de pessoas inocentes (Amankwaa, 2018, p. 460). Por sua vez, os argumentos desfavoráveis à retenção de perfis de DNA de detidos estão relacionados com a criminalização de pessoas inocentes (presunção de inocência); a sobrerrepresentação de certos grupos étnicos na base de dados (Skinner,

2013) e a desconfiança em relação aos procedimentos de retenção e utilização dos perfis de DNA (Amankwaa, 2018, p. 460).

Base de dados forense nacional – Funcionamento, supervisão e estatísticas

A base de dados forense nacional armazena dois tipos de registos de perfis de DNA. Um dos registos é relativo aos perfis de DNA de pessoas identificadas cuja amostra é, geralmente, recolhida pela polícia no ato da sua detenção (Home Office, 2017, p. 1). Neste caso, a amostra de DNA é recolhida através de um esfregaço bucal (técnica mais comum) e, posteriormente, enviada para um laboratório forense acreditado que faz parte do *Forensic Service Provider*⁴¹ (FSP). O perfil de DNA obtido através da amostra é inserido na base de dados e pode ser utilizado para procurar correspondências com perfis de DNA recolhidos em cena de crime. Através do perfil só é possível discernir o sexo do indivíduo, pelo que não é identificável qualquer característica física do mesmo. O segundo registo remete para perfis de DNA obtidos através de amostras recolhidas pela polícia científica (*Crime Scene Investigators*) em locais onde ocorreu um crime (Home Office, 2017, p. 2). Quando ocorre um crime podem ser deixados vestígios de DNA em objetos do local, pelo que a avaliação de uma cena de crime engloba a procura de objetos com maior probabilidade de conter DNA da pessoa que o cometeu. Os objetos são enviados para os laboratórios supramencionados para confirmação (ou não) da existência de DNA para produção de um perfil que será, posteriormente, inserido na base de dados.

A supervisão da base de dados é realizada por quatro entidades constituídas por pessoas de diversas áreas de formação. O *National DNA Database Strategy Board*⁴² é responsável pela manutenção e supervisão das atividades da NDNAD e da base de dados nacional de impressões digitais. O *National DNA Database Ethics Group*⁴³ está encarregue de fornecer aconselhamento ético independente em questões relacionadas com a base de dados. O *Biometrics Commissioner*⁴⁴ tem como função supervisionar a retenção e a utilização de amostras de DNA, perfis de DNA e impressões digitais por parte das forças

⁴¹ Serviço de ciência forense (*Forensic Service Provider*) prestado ao sistema de justiça criminal cujas normas de funcionamento obedecem a um regime de qualidade assegurado por um conjunto de *standards* científicos.

⁴² Disponível em <https://www.gov.uk/government/groups/national-dna-database-strategy-board>. Acesso a 12 de maio de 2020.

⁴³ Esta entidade foi substituída pelo *Biometrics and Forensics Ethics Group*. Disponível em <https://www.gov.uk/government/organisations/national-dna-database-ethics-group>. Acesso a 12 de maio de 2020.

⁴⁴ Disponível em <https://www.gov.uk/government/organisations/biometrics-commissioner>. Acesso a 12 de maio de 2020.

policiais. O *Forensic Science Regulator*⁴⁵ tem como objetivo assegurar que a prestação de serviços de ciência forense se encontra de acordo com o regime de standardização que visa a qualidade científica do trabalho oferecido.

Em março de 2016 a base de dados continha cinco milhões oitocentos e sessenta mil e seiscentos e quarenta e dois (5 860 642) registos de perfis de pessoas conhecidas e quinhentos e dezanove mil e seiscentos e setenta e oito (5 196 78) registos de perfis recolhidos em cenas de crime (Home Office, 2017). Contudo, estima-se que doze por cento (12%) dos perfis de DNA sejam duplicados devido à inserção de perfis de DNA de indivíduos que já constam na mesma, mas com um nome diferente. Considerando a estimativa de duplicados, o valor aproximado de perfis de DNA na base de dados é de cinco milhões cento e cinquenta e seis mil e duzentos e sessenta e oito perfis (5 156 268) (Home Office, 2017). Em relação à probabilidade de se verificar uma correspondência entre um perfil de DNA de um indivíduo e um perfil de DNA de uma cena de crime, o relatório anual do *Strategy Board*, refere que é de aproximadamente sessenta e três por cento (63%). O documento refere que o “match rate has increased year on year as the Database grows more effective” (Home Office, 2017, p. 13). Denote-se que a entidade responsável pela redação do relatório encara o crescimento da base de dados como eficiente. Entre os anos de 2015 e 2016 foram encontradas 440 correspondências entre perfis de DNA de indivíduos com perfis presentes em cenas de crime. Desses números, 63 perfis diziam respeito a homicídios e 83 perfis a violações (*idem*, p. 14)

Dado o tempo de vida da base de dados de DNA nacional (25 anos) compreende-se a importância atribuída à prova genética na resolução de crimes no Reino Unido. No entanto, a dificuldade de se recolherem provas biológicas nos locais onde ocorreu um crime encontra-se plasmada nos escassos 11% dos casos em que é possível proceder à sua recolha (*idem*, p. 17). As cenas de crime mais prováveis de conterem vestígios de DNA são as que dizem respeito a homicídios, violações, roubos e assaltos a habitações. Entre 2015 e 2016 os dados mostram que dos perfis encontrados em cena de crime e inseridos na NDNAD apenas cerca de 50% deram origem a uma correspondência positiva (*idem*, p. 17). Esclareça-se que uma correspondência positiva não origina por si só uma condenação, esta pode não

⁴⁵ Disponível em <https://www.gov.uk/government/organisations/forensic-science-regulator>. Acesso a 12 de maio de 2020.

corresponder ao indivíduo que perpetuou o crime, mas antes a uma pessoa que esteve no mesmo local noutra altura e noutro contexto.

Para o funcionamento eficiente da NDNAD procedeu-se, desde abril de 2015, à criação de uma base de dados de eliminação da polícia (*Police Elimination Database* - PED). A PED é constituída por registos de perfis de DNA recolhidos às forças policiais e aos seus funcionários com o objetivo de facilitar a identificação de contaminações nas cenas de crime e/ou durante a cadeia de custódia das provas (Police Staff Council, 2018). De modo completar existem para efeitos de eliminação a *Medical Examiners Elimination Database*⁴⁶ (MedExD) e a *Manufacturers Elimination Database*⁴⁷ (MED) (Forensic Science Regulator, 2014, p. 17). Quando se verifica a ocorrência de uma situação de contaminação é obrigatório reportar o incidente. Atualmente, a *National DNA Database Delivery Unit*⁴⁸ (NDU) encontra-se a desenvolver uma base de dados de eliminação centralizada – *Centralised Elimination Database* (CED) de modo a tornar a verificação de contaminações na NDNAD mais eficiente (Home Office, 2017, p. 22). Quando ocorre uma correspondência entre a CED e a NDNAD deve proceder-se, após verificação, à eliminação do perfil de DNA da NDNAD. De forma a mitigar potenciais erros por não conformidade com os *standards* científicos, os laboratórios (FSP) que pretendam realizar o processamento de amostras/perfis de DNA para a NDNAD têm obrigatoriamente de ser aprovados tanto pela NDU como pelo NDNAD *Strategy Board*. Em março de 2016, os serviços de ciência forense autorizados a inserir perfis de DNA na base de dados nacional perfaziam um total de 13 entidades (*idem*, p. 27).

Caso de S. e Marper versus Reino Unido e ‘Protection of Freedoms Act 2012’

A 16 de agosto de 2004, S.⁴⁹ e Michael Marper apresentaram no Tribunal Europeu dos Direitos Humanos um pedido relativo à retenção, por parte do Reino Unido, das suas impressões digitais, material celular e perfil de DNA (“Case of S. and Marper v. The United Kingdom” 2008, p. 2). Os requerentes consideraram que não existiam fatores que justificassem a retenção, pois os processos que foram movidos contra ambos encontravam-

⁴⁶ Nesta base de dados constam todos os funcionários médicos: médicos legistas, médicos associados ao Centro de Agressão Sexual, patologistas e médicos, direta ou indiretamente, envolvidos na recolha de vestígios em vítimas de crime (vivos ou mortos) e de suspeitos detidos.

⁴⁷ Nesta base de dados constam os funcionários diretamente envolvidos na construção e montagem de consumíveis utilizados na recolha, preservação e processamento de perfis de DNA.

⁴⁸ Departamento do Ministério do Interior responsável pela administração da NDNAD.

⁴⁹ S., o primeiro requerente, solicitou ao tribunal a não divulgação do seu nome no acórdão por ser menor de idade.

se encerrados (*idem*, p. 3). O primeiro requerente (S.), em 2001, teve as suas impressões digitais e amostras de DNA recolhidas no âmbito de uma detenção por tentativa de assalto, sendo absolvido no mesmo ano. O segundo requerente (Marper) foi preso com recolha da mesma informação, também em 2001, devido a acusações de assédio ao seu parceiro. No mesmo ano, reconciliaram-se e o mesmo desistiu da queixa, sendo o caso formalmente descontinuado.

No seguimento das decisões dos seus processos em tribunal, ambos requereram à polícia a destruição dos registos relativos às impressões digitais e às amostras de DNA. Face ao pedido, a polícia recusou a eliminação dos dados recolhidos a S. e a Marper e novo pedido foi remetido, em 2002, para o Tribunal Administrativo onde foi novamente recusada a eliminação dos dados (*idem*, p. 3). O pedido foi, posteriormente, apresentado ao Tribunal Europeu dos Direitos Humanos que, em 2008, confirmou que ocorreu uma violação do artigo 8.º da Convenção Europeia dos Direitos Humanos⁵⁰. O Tribunal decidiu que a retenção de perfis de DNA por tempo indefinido de pessoas condenadas e não condenadas é uma medida desproporcional. As repercussões desta decisão levaram à alteração das leis que regulavam a recolha, utilização e retenção de DNA forense no Reino Unido através do *Protections of Freedoms Act 2012* (PoFA) implementado em outubro de 2013 (Protection of Freedoms Act, 2012).

Amankwaa e McCartney (2018) analisaram vários dos relatórios redigidos pelas entidades responsáveis pela supervisão das atividades da NDNAD pós PoFA e exploraram os aperfeiçoamentos e potenciais riscos da sua implementação. De modo geral, os relatórios mostram que com o PoFA se verificou um aperfeiçoamento do desempenho da base de dados, bem como um reforço da privacidade genética dos cidadãos britânicos. Quanto aos riscos, foi enfatizada a possibilidade de ocorrer a eliminação de perfis de DNA que poderiam ser úteis para a identificação de pessoas que cometeram crimes (*idem*, p. 117).

O regime de retenção de perfis de DNA na NDNAD sofreu quatro alterações ao longo dos anos. O primeiro documento intitulado de *Criminal Justice and Public Order Act*, data de 1994 e baseava-se num regime de retenção restritivo (1995-2001) (Amankwaa, 2018, p. 458). Neste enquadramento, o perfil de DNA de condenados por qualquer tipo de crime era retido indefinidamente na base de dados, mas o perfil de DNA de pessoas não condenadas

⁵⁰ Artigo 8.º - Direito ao respeito pela vida privada e familiar

era eliminado da base de dados findada a investigação criminal (Amankwaa & McCartney, 2008, p. 118). Mais tarde, através do *Criminal Justice and Police Act (2001)* e do *Criminal Justice Act (2003)* a retenção de perfis passou a caracterizar-se pelo seu regime expansivo (2001-2013) (Downey et al., 2012, p. 442). Os perfis de DNA de condenados continuavam a ser retidos indefinidamente na base de dados e o mesmo acontecia com os perfis de DNA recolhidos no âmbito de uma investigação criminal mesmo que o processo terminasse com a exoneração da pessoa em questão. A escassa limitação imposta ao regime de retenção indefinida dos perfis de DNA foi criticada com base no argumento de que se estaria a colocar em causa o direito à presunção de inocência, bem como existia o perigo de se transformar a sociedade britânica numa ‘sociedade suspeita’ (Amankwaa, 2018, p. 456; McCartney, 2004). Para além dos argumentos mencionados, McCartney (2012) refere ainda a escassez de dados que comprovem a necessidade e as vantagens de manter perfis de DNA de pessoas inocentes na base de dados forense (*idem*). O terceiro documento a este respeito surge em 2010 com o *Crime and Security Act*, porém nunca chegou a ser aplicado devido à revogação assente em críticas remetidas aos dados estatísticos utilizados para a sua fundamentação (Amankwaa & McCartney, 2018, p. 119; Downey et al., 2012).

Atualmente, desde 2012, a retenção de perfis de DNA é caracterizada por um regime semi-restritivo através do PoFA. *Grosso modo*, o documento veio autorizar a retenção indefinida de perfis de DNA na NDNAD de todos os indivíduos condenados; bem como a retenção limitada de perfis de menores em situação de primeira condenação e de perfis de inocentes. Deste modo, a retenção ilimitada de perfis de inocentes deixou de ser possível à luz da nova regulação. A implementação do PoFA levou à eliminação de aproximadamente 1.7 milhões de perfis de DNA que perteciam a pessoas não condenadas e à destruição de cerca de 7.7 milhões de amostras de DNA após recolha do respetivo perfil (Amankwaa & McCartney, 2018, p. 119). Os relatórios analisados por Amankwaa e McCartney (2018) realçam que existe uma maior aceitação deste regime devido à proporcionalidade entre o direito à privacidade e o interesse público (p. 120). O valor da taxa de correspondências aumentou desde o PoFa, sendo um dos mais elevados ao nível europeu. Pode supor-se que a eliminação dos perfis de pessoas inocentes não afetou significativamente o desempenho da base de dados, verificou-se, pelo contrário, uma melhoria do mesmo (*idem*). Um outro benefício que pode advir da implementação do PoFA tem que ver com a diminuição dos

custos associados ao armazenamento de perfis de DNA que, com o novo regime, são em menor número (*idem*).

O PoFA tem gerado vários desafios ao nível da sua implementação. Uma das medidas adotadas passa pela eliminação dos registos biométricos, por parte da polícia⁵¹, de acordo com os novos critérios de retenção de perfis de DNA. No entanto, este é um processo informaticamente complexo que pode proporcionar a retenção errada de dados biométricos de pessoas que deveriam ter sido excluídas da base de dados (Amankwaa & McCartney, 2018, p. 121). Outro aspeto periclitante tem que ver com o fraco envolvimento das forças policiais no novo regime. Esta situação pode decorrer de vários aspetos. Primeiro, devido à necessidade de disponibilidade de recursos humanos e financeiros. Segundo, pelo facto de alguns profissionais não concordarem com as opções legislativas do novo regime de retenção de perfis de DNA. Terceiro, tem-se verificado dificuldades na compreensão das circunstâncias em que se deve proceder à retenção dos registos biométricos (*idem*). Por fim, a situação dos voluntários na base tem sido questionada. Inicialmente os perfis dos voluntários eram retidos indefinidamente na NDNAD, podendo dissuadir esta prática. Após a implementação do PoFA a retenção dos perfis de DNA dos voluntários começou a obedecer às mesmas regras que os restantes. Contudo, um dos grupos responsáveis pela supervisão da NDNAD – o *Ethics Group* – realça que o consentimento informado ainda não é satisfatório em matéria de clarificação do sistema de retenção, bem como na proteção dos direitos individuais dos voluntários (*idem*, p. 122).

Os órgãos que supervisionam a NDNAD têm exposto os vários riscos que podem decorrer do novo regime de retenção. Sendo este um sistema mais complexo no que concerne à retenção de perfis de DNA de pessoas que foram ilibadas em tribunal, pode verificar-se a eliminação de registos biométricos que deveriam continuar na base de dados (*idem*, p. 123). Do mesmo modo, pode ocorrer a retenção de perfis de DNA na base de dados sem o devido enquadramento legal originando uma violação da privacidade da pessoa envolvida no processo (*idem*). Consequência direta desta situação, é a possível correspondência de um perfil ilegalmente retido com um perfil legalmente inserido na base de dados. Deste modo, a retenção de perfis de DNA de pessoas não condenadas é realizada através de um pedido específico que é avaliado caso-a-caso. No entanto, os indivíduos cuja

⁵¹ Através do *Police National Computer* (PNC) que contém os dados de todos os indivíduos detidos no decorrer de atividades policiais

retenção dos dados é solicitada não são informados nem do pedido de retenção, nem das razões que motivaram o procedimento, pelo que esta situação pode configurar-se complexa em questões de privacidade e proteção de dados (*idem*). Por fim, os não condenados revelam diferentes hierarquias de inocência, de acordo com os critérios de retenção dos perfis de DNA. Esta situação decorre do modo discriminatório com que os indivíduos que são detidos com base em alegações de crimes graves são tratados em relação aos restantes detidos por alegações de crimes menos graves e voluntários. No primeiro grupo, o consentimento informado não é obrigatoriamente requerido, pelo que se colocam questões de proporcionalidade do PoFA no que concerne à retenção de dados de pessoas inocentes (*idem*, p. 124).

Cooperação transnacional – Decisões Prüm

As negociações que envolveram o Tratado de Lisboa (2009) incluíram a inserção de um artigo (artigo 10.º do protocolo 36⁵²) que concedia ao Reino Unido um período de cinco anos para decidir se continuava ou não a fazer parte cooperação policial e judicial, bem como das medidas de reconhecimento mútuo pré-tratado. O Partido Trabalhista (social-democrata de centro-esquerda) mostrou-se mais favorável à saída do Reino Unido do pacote de medidas de modo a ganhar tempo para pensar nas implicações que a permanência poderia trazer ao nível nacional (McCartney, 2013, p. 547). Em particular, a continuidade obriga a que o Reino Unido se encontre sujeito ao Tribunal de Justiça da União Europeia (TJUE)⁵³ e possa ser penalizado pela Comissão em caso de infração às normas europeias (*idem*). Sendo que, McCartney (2013) denota que existe uma certa confusão, no Reino Unido, entre o Tribunal Europeu dos Direitos Humanos (responsável pela decisão de *S. & Marper*) e o Tribunal de Justiça da União Europeia (p. 547). A este respeito, o Tratado de Lisboa realça que o TJUE não pode interferir com as operações de segurança levadas a cabo, ao nível nacional, pelas polícias e pelas instituições responsáveis pela aplicação da lei (*idem*, p. 548). Em contexto nacional ambos os Tribunais são criticados com base no poder que podem exercer sobre as leis nacionais em matéria de direitos humanos e lei criminal.

⁵² Disponível em <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008M/PRO/36:EN:HTML>. Acesso a 12 de maio de 2020.

⁵³ Disponível em https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_pt Acesso a 12 de maio de 2020.

Encontra-se presente no discurso político esta ideia de controlo por parte da União Europeia sendo que, Theresa May, *Home Secretary*⁵⁴ (2010-2016), referiu numa intervenção que:

I mentioned the European Court of Justice. I also want to refer to the European Court of Human Rights, which contradicts laws passed by our Parliament, overrules judgments made by our courts, and interprets the articles of the original convention on human rights in an expansionist way. That is totally unacceptable. I therefore believe that we also have to consider very carefully this country's relationship with Strasbourg as well as our relationship with Brussels (House of Commons Hansard Debates 2013).

No excerto apresentado, Theresa May demonstra a sua posição contra ambos os tribunais por considerar que os mesmos vão contra a soberania do Reino Unido. Theresa May realça também o facto de o Tribunal Europeu dos Direitos Humanos contrariar as leis britânicas, sendo esta uma situação 'inaceitável'. No entanto, ao longo do relatório "EU police and criminal justice measures: The UK's 2014 opt-out decision" várias vozes discordaram da narrativa de perda de soberania em matéria de lei criminal (House of Lords, 2013). Em particular, John Spencer do *Centre for European Legal Studies* referiu no documento que o reconhecimento mútuo veio assegurar a existência e respeito pelos contextos legais dos diferentes países (ponto 78.). No mesmo relatório, Spencer acrescentou que "there was no evidence of the CJEU attempting to interfere in domestic law" (House of Lords, 2013, ponto 88.). Nesta linha, McCartney (2013) refere, no seu trabalho, que as medidas associadas ao Tratado de Lisboa não versam sobre a cedência do controlo nacional às instituições europeias. Pois, através do reconhecimento mútuo é possível permitir que os sistemas judiciais nacionais não sejam necessariamente iguais, mas em simultâneo, garantir que consigam cooperar entre si (*idem*, p. 550). A não adesão ao Tratado, apesar das salvaguardas feitas por John Spencer e outros académicos, foi encarada como uma forma de reaver da União Europeia os poderes estatais retirados ao Reino Unido (*idem*, p. 549). Os poderes que a ala conservadora pretendia recuperar remetiam para a lei criminal, o policiamento e a condenação em tribunal (*idem*).

⁵⁴ A *Home Secretary* é responsável pelos Assuntos Internos de Inglaterra e do País de Gales e pela Imigração e Nacionalidade no Reino Unido

Situação igualmente complexa foi a de optar por fazer parte das Decisões Prüm, obrigatórias para os Estados-Membros da União Europeia. O Governo do Reino Unido, em 2013, entendeu que, sendo o país com a maior base de dados forense de perfis de DNA, iria ficar à mercê de um número desproporcional de pedidos de informação (segundo passo do sistema Prüm) por parte dos restantes países (*idem*, p. 555). No entanto, não se compreende se esta apreensão verte de dificuldades técnicas ou de outro tipo de problema. McCartney (2013) dá-nos conta de algumas incongruências no decorrer das conversações a respeito das Decisões Prüm (pp. 555-558). Primeiro, em 2007, o Governo considerou que os recursos financeiros necessários à implementação do sistema Prüm (cerca de £ 31 milhões) eram adequados tendo em consideração os benefícios de um sistema desta natureza. Contudo, em 2013, o novo Governo voltou atrás e referiu não estar preparado para avançar com uma implementação desta amplitude com valores monetários tão elevados, pelo que não se verificou qualquer tipo de medida para avançar com o sistema Prüm. Segundo, não foram feitos esclarecimentos sobre o modo como foram calculadas as estimativas dos gastos da implementação do sistema Prüm, sendo que o valor se revelou substancialmente mais alto do que o que foi estimado por outros Estados-Membros. Terceiro, apesar de o parlamento e especialistas em ética realçarem a importância de se garantir a privacidade dos cidadãos na partilha transnacional de informação pessoal, foram as questões económicas que assumiram um papel determinante nesta decisão. Acrescente-se que as atividades no sistema Prüm não usufruem da mesma supervisão que as atividades da base de dados forense nacional.

A decisão de não fazer parte deste sistema, em 2014, foi contra aquela que era a lógica de cooperação entre Estados-Membros. Cooperação essa que pretendia ir além fronteiras com o objetivo de aumentar a segurança e a identificação de potenciais perigos (exemplo, terrorismo) para a União Europeia e os seus cidadãos. Garantir a segurança nacional sem investir na cooperação policial transfronteiriça torna-se uma tarefa mais complexa e pode potenciar situações de insegurança. Nas palavras de McCartney (2013):

The UK cannot isolate itself from policing and security challenges across the EU and internationally. The use of the opt-out is a significant backward step in ensuring effective policing cooperation. (p. 559)

O Conselho da União Europeia, a 3 de fevereiro de 2017, publicou um relatório que dava conta da avaliação do Reino Unido em relação à partilha transnacional de dados (Council of the European Union, 2017). No documento constavam as respostas fornecidas pelo Reino Unido aos questionários acerca da proteção de dados, partilha de dados de DNA e a avaliação dos Países Baixos (país nomeado para ajudar e testar a implementação do sistema Prüm). Foram feitas várias recomendações, principalmente, relacionadas com o número de marcadores dos perfis de DNA a serem disponibilizados. Em particular, durante a avaliação, o Reino Unido indicou que apenas perfis com 10 ou mais *loci* seriam comparados ao nível internacional. No entanto, a equipa de avaliação recomendou a inclusão de perfis com 6, 7, 8 e 9 *loci*, pois estes também poderiam originar correspondências importantes para a investigação criminal. Posteriormente, o Reino Unido atualizou o seu processo para cumprir esta recomendação (Council of the European Union, 2017, p. 2).

No decorrer da mesma avaliação, o país referiu que apenas procederia à partilha de dados pessoais com correspondências entre perfis com 10 ou mais *loci*. Neste sentido, a equipa dos Países Baixos recomendou que se baixasse o número de *loci*, pois uma correspondência com menos *loci* pode ser igualmente valiosa em termos de prova na investigação criminal. Porém, a equipa de avaliação reconheceu que esta opção pode potenciar o número de falsos positivos, recomendando a utilização da *Random Match Probability* para evitar a partilha de dados com base em falsas correspondências. Tendo em consideração as recomendações, o Reino Unido decidiu que para correspondências com 10 ou mais *loci* procederia ao envio das informações pessoais de modo rotineiro. Contudo, nas que se verificassem menos do que 10 *loci* o envio seria decidido caso-a-caso (*idem*, p. 3).

Findada a avaliação, a equipa designada para o efeito declarou que, em relação à partilha de dados de perfis de DNA, o país implementou corretamente as Decisões Prüm (*idem*, p. 4). Dito isto, em 2017, o Reino Unido encontrava-se preparado para começar a ficar operacional com os restantes países da União Europeia. Na avaliação participaram as seguintes entidades britânicas: *Forensic services Metropolitan Police Services* (MPS); *DNA intelligence analyst Metropolitan Police Authority* (MPA); *DNA Services Manager MPS*; *Information Law Strategy*; *Data Protection Officer*; *Freedom of Information Office MPS*; *G5 Officer*; *Casework Co-ordination Unit MPS*; *Policy lead for Prüm, Home Office*; *National Crime Agency* (NCA) (*idem*, p. 5).

A 12 de abril de 2018 foi publicado um novo relatório pelo Conselho da União Europeia que clarificava questões levantadas pelos Estados-Membros ao Reino Unido em relação aos perfis de DNA (Council of the European Union, 2018b). A primeira questão teve que ver com a inclusão de perfis de DNA de pessoas não condenadas na base de dados forense nacional. O Parlamento britânico referiu que apenas seriam disponibilizados os perfis de DNA de pessoas condenadas, consequência da alteração legislativa que decorreu do caso S. e Marper. A segunda pergunta remeteu para o modo como se procederia a partilha de dados em perfis com 10 ou mais *loci* e entre 6 e 9 *loci*. No primeiro caso, o Reino Unido reiterou que a partilha de informação seria automática. O segundo caso é mais complexo, pelo que se a correspondência fosse confirmada proceder-se-ia à partilha da informação, mas se não fosse o suficiente para confirmar a correspondência, o pedido de informação deveria seguir pela Interpol. Por fim, a terceira questão pedia esclarecimentos sobre proteção de dados. O país clarificou que iria adotar a nova legislação europeia em matéria de proteção de dados (GDPR), bem como os restantes documentos que dizem respeito à proteção de dados em matéria de cooperação e investigação policial.

Com base nos relatórios “Prüm/DNA data exchange evaluation of United Kingdom (UK)” e “Clarification on DNA concerns raised at previous DAPIX meetings” confirmou-se a intenção do Reino Unido em fazer parte das Decisões Prüm e de participar na cooperação transnacional. No dia 6 de junho de 2019, o Conselho da União Europeia efetivou a participação do Reino Unido no sistema Prüm quanto à partilha transnacional de dados genéticos (Council of the European Union, 2019a). Oficialmente, o início da partilha de dados genéticos através do sistema Prüm iniciou-se no dia 14 de junho de 2019, sendo que o Reino Unido deve prestar esclarecimentos até junho de 2020 a respeito da exclusão dos perfis de DNA de suspeitos da partilha automática. A decisão de (não) partilhar dados de suspeitos tem sido um dos pontos de tensão quanto à entrada do país no sistema Prüm. Neste seguimento, no dia 17 de julho de 2019, o *European Scrutiny Committee* do Parlamento britânico considerou ser necessário um pedido de esclarecimento de modo a compreender se “excluding the DNA profiles of criminal suspects from the Prüm data exchange mechanism is ‘in conformity’ with the Prüm Decisions”⁵⁵. No entanto, o referendo

⁵⁵ Parecer publicado no site do parlamento britânico: <https://publications.parliament.uk/pa/cm201719/cmselect/cmeuleg/301-lxx/30106.htm>.

Acesso a 12 de maio de 2020.

que ditou a saída do Reino Unido na União Europeia (*Brexit*), realizado em 2016 e a confirmação oficial coloca a entrada no sistema Prüm em causa.

4.2. Perspetivas de geneticistas forenses e *stakeholders*

4.2.1 Portugal

O presente subcapítulo empírico irá versar sobre as entrevistas semiestruturadas que foram aplicadas a geneticistas forenses e aos *stakeholders* em Portugal, no âmbito do sistema Prüm e da base de dados forense de perfis de DNA. Foram realizadas um total de vinte e sete entrevistas, sendo que os/as entrevistados/as enquadram-se em diferentes perfis profissionais. Deste modo, os/as entrevistados/as foram agregados/as nas seguintes categorias: geneticistas forenses (14 entrevistas); membros de entidades de supervisão e regulação (4 entrevistas); membros de órgãos de investigação criminal (3 entrevistas); e por fim, Professor(a) Universitário(a)/Investigador(a) (6 entrevistas: 2 entrevistados/as com formação em biologia e 4 com formação em direito)

Contexto legal da base de dados forense de perfis DNA

As entrevistas do presente estudo foram realizadas num contexto de instabilidade legal, na medida em que estavam a ser revistas e votadas as propostas à alteração da Lei n.º 5/2008. Portanto, quando os/as entrevistados/as foram questionados/as acerca da base de dados forense de perfis de DNA as suas perceções basearam-se tanto no balanço da eficácia da base de dados, como na pertinência das alterações à lei nesta matéria realçando, em diversos momentos, os pontos que consideraram fulcrais.

Apenas uma parte diminuta dos/as geneticistas forenses entrevistados/as no âmbito do estudo encaram a base de dados sob a lente do positivismo político que precedeu a sua criação (Machado, 2011; Machado & Silva, 2010). Os imaginários que compreendem as narrativas que enfatizam o bom funcionamento da base de dados focam-se, em grande medida, nas características técnicas e científicas da mesma. No entanto, como está demonstrado no extrato apresentado, a reduzida dimensão da base de dados forense portuguesa (Reed & Syndercombe-Court, 2016) é um dos aspetos menos favorável ao seu desempenho. Isto porque a sua eficácia em termos de utilidade, segundo o/a entrevistado/a, depende do aumento da dimensão da base de dados. De modo implícito

encontra-se plasmada na sua reflexão a diferenciação entre a dimensão técnico-científica e a dimensão político-social (Dyer, 1997) da base de dados forense, sendo estas as características centrais destas tecnologias de vigilância. Por um lado, elencando que tecnicamente todas as salvaguardas estão a ser cumpridas de modo a assegurar os critérios de qualidade. Por outro lado, referindo que para que a função social e política da base de dados seja cumprida, ou seja, a identificação de pessoas que tenham cometido crimes, é necessário aumentar a inclusão de perfis de DNA.

“O balanço é positivo, penso que a nossa base está a funcionar muitíssimo bem (...) temos uma série de mecanismos para prevenir erros, para que tenhamos a certeza que tudo está exatamente conforme os melhores critérios de qualidade. Mas o único problema que eventualmente a base poderá ter é ser uma base com um número muito reduzido de perfis, porque a função de uma base será tanto mais concretizada quanto maior for a sua dimensão (...). Agora relativamente a todo o funcionamento, todas as regras de qualidade são cumpridas, a nossa base acho que está a funcionar muito bem.” [N24-geneticista forense]

Na grande maioria dos/as geneticistas forenses entrevistados/as observa-se uma postura mais crítica em relação ao desempenho da base de dados forense no contexto nacional. Posto isto, um dos pontos elencados remete para certas incongruências que se encontravam na lei orgânica em relação à entidade responsável pela supervisão da mesma. O extrato apresentado demonstra o conflito de interesses que inicialmente caracterizava a supervisão das atividades da base de dados forense, na medida em que, o orçamento do órgão de supervisão (CFBDP ADN) se encontrava, numa primeira versão da lei (Lei n.º 40/2013⁵⁶), dependente da entidade fiscalizada, o INMLCF. Em termos éticos, o grau de dependência da entidade supervisão em relação à entidade a ser fiscalizada apresenta-se como um obstáculo no desempenho das suas funções, pois devido à sua natureza exige-se um certo grau de independência que não estava adequadamente assegurado nestes moldes. O/a mesmo/a entrevistado/a refere ainda a elevada proximidade física e espacial das duas entidades supracitadas. Atualmente, as instalações do Conselho de Fiscalização

⁵⁶ Lei de organização e funcionamento do conselho de fiscalização da base de dados de perfis de ADN

continuam a permanecer no mesmo edifício do Instituto de Medicina Legal e Ciências Forenses.

“Na lei, a grande crítica é o facto de a autoridade de supervisão (...) não ser suficientemente independente da entidade que possui a custódia da base de dados. Formalmente, parece não haver problema, mas depois repara-se que há demasiada [interferência]. (...) Mesmo fisicamente, nas infraestruturas, no pessoal, entre outros.” [N01-geneticista forense]

Grosso modo, as insuficiências apontadas pelos geneticistas forenses como impedimentos ao bom funcionamento da base de dados forense portuguesa derivam do enquadramento legal que motivou a sua criação, nomeadamente, a Lei n.º 5/2008. De modo consensual, os/as participantes elencam que o contexto legal se apresentou como uma das dificuldades mais prementes para o aumento da inserção de perfis de DNA na base de dados forense. Em particular, um/a dos/as geneticistas forenses argumenta que a base de dados nacional é ‘demasiado exigente’ e burocrática nos critérios administrativos, pois depende excessivamente da figura do tribunal e do juiz para a retificação de dados pessoais e processuais na própria base. Os procedimentos morosos necessários à alteração de informação na base de dados podem condicionar a celeridade na retificação dos dados pessoais que constam na mesma. Em última análise, esta situação é problemática em relação ao direito que os cidadãos possuem de retificação dos seus dados nas várias plataformas institucionais (al. d do n.º 1 do artigo 5.º; artigo 16.º do Regulamento (UE) 2016/679). Ainda que o Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) exclua o tratamento de dados no âmbito da esfera criminal (artigo 2.º), não deixa de ser um documento fundamental para a identificação de boas práticas no tratamento de dados pessoais. Esta crítica encontra-se em linha com outros trabalhos académicos que demonstram que as forças policiais também encaram a centralidade do juiz como problemática para o bom funcionamento da base de dados (Costa, 2014; Machado & Costa, 2012, p. 67; Santos et al., 2012)

“É muito complicada [a base de dados] em termos administrativos. E é demasiado exigente, porque se não [se] tem o número do processo temos que pedir

ao tribunal que retifique, se não tem isto, voltamos a pedir ao tribunal que retifique.” [N15-geneticista forense]

As bases de dados forenses de perfis de DNA enquanto “instrumentos contemporâneos da biopolítica” (Pugliese, 2012, p. 2) têm como função basilar a identificação de pessoas que cometeram crimes. Em contexto nacional estas permitem encontrar ligações entre casos arquivados e cenas de crime; identificar delinquentes e perpetradores de crimes (através de correspondências com a base de dados); garantir a identificação mais célere de ofensores e, por conseguinte, dissuadir potenciais atividades criminosas, entre outros (INTERPOL, 2009). No entanto, as perspetivas dos/as entrevistados/as revelaram-se críticas em relação à gestão da base de dados forense nacional. O extrato de um/a dos/as geneticistas forenses demonstra que o modo como o enquadramento legal foi concretizado tem vindo a condicionar o número de amostras, principalmente, de amostras-problema na base de dados. Por esse motivo, o/a entrevistado/a considera, inclusivamente, que os condicionamentos legais impostos pelo legislador português desempenham um papel prejudicial para a própria investigação criminal que não consegue usufruir em pleno das potencialidades deste tipo de base de dados biométrica.

“É um balanço um bocadinho negativo porque a legislação não permite que de facto haja uma evolução da base de dados, o que eu acho que é prejudicial para a investigação e para a resolução da criminalidade, não é? Temos muito poucas amostras de vestígios biológicos (...).” [N06-geneticista forense]

Face às críticas generalizadas ao modo como a lei portuguesa da base de dados foi pensada depreende-se que os participantes do estudo, em particular, geneticistas forenses, defendem que ao nível nacional não se está a retirar da base de dados forense todo o seu potencial utilitário. Neste sentido, no excerto, encontra-se presente o argumento de que a lei portuguesa apresenta fortes carências no domínio da ciência por parte do legislador. Refere-se, inclusivamente, que uma otimização da base de dados forense passa por uma melhor integração entre a ciência e a lei (Jasanoff, 1995, 2006) de modo a alcançar um

documento que permita mais correspondências, mas que continue, em simultâneo, a salvaguardar os direitos civis à privacidade e proteção de dados.

“Porque é um tema que é muito específico, é evidente que quem legisla não domina, e se calhar não há aquela ligação que devia haver entre a ciência e quem legisla para que se conseguisse chegar a uma lei mais justa para toda a gente e conservadora q.b. e tudo isso, mas que conseguisse fazer com que isto tudo valesse mais a pena. Porque a base de dados hoje em dia, infelizmente, ainda não tirámos dela o potencial que poderíamos tirar.” [N08-geneticista forense]

Denote-se que as alterações efetuadas à Lei n.º 5/2008 pretenderam diluir os obstáculos causados à inserção de perfis de DNA na base de dados identificados como um dos fatores debilitantes. Deste modo, verificou-se um esforço no sentido de se aumentar o número de perfis resultantes de amostras-problema dos locais de crime que, segundo os/as entrevistados/as, eram até à data em número muito reduzido. Deste modo, a nova versão da lei veio permitir a inserção de perfis de amostras-problema por parte de outra entidade para além no INMLCF, respetivamente, o Laboratório da Polícia Judiciária (al. a do n.º 3 do artigo 17.º e n.º 4 do artigo 18.º da Lei n.º 90/2017) de modo a fomentar um aumento do número de amostras-problema constantes na base de dados.

Relativamente à inserção de perfis de DNA resultantes de amostras-referência verificou-se também a simplificação do processo de autorização para inserção na base de dados. Sob a alçada da Lei n.º 5/2008 eram necessários dois despachos de um juiz para permitir a inserção dos perfis de DNA. No primeiro despacho era ordenada a recolha da amostra de DNA e só no segundo despacho era ordenada a sua inserção na base de dados. No novo contexto legal procede-se à realização de um despacho que ordena que a “recolha de amostra em arguido condenado por crime doloso com pena concreta de prisão igual ou superior a 3 anos (...) com a consequente inserção do respetivo perfil de DNA na base de dados, é sempre ordenada na sentença” (n.º 2 do artigo 8.º da lei 90/2017). Esta alteração pretendeu evitar a não inserção de um perfil de DNA devido ao não preenchimento de um segundo requerimento que poderia, por motivos vários, não ser realizado.

A maioria dos/as geneticistas forenses mostram-se favoráveis às alterações legais por considerarem que estas podem ajudar a mitigar as vulnerabilidades associadas à

pequena dimensão da base de dados forense. Nos extratos apresentados, ambos os/as entrevistados/as realçam que a simplificação dos passos processuais exigidos para a inserção de perfis de DNA na base de dados forense veio permitir o aumento da inserção de perfis de amostras-referência, bem como de amostras-problema. Pois, a redução para um só requerimento do juiz para o pedido de inserção do perfil de DNA de um condenado na base de dados tem vindo a materializar-se no aumento de amostras-referência na mesma. Na mesma ótica, a autorização para que uma segunda entidade insira perfis de DNA de amostras de cenas de crime, nomeadamente, o Laboratório da Polícia Judiciária, tem, igualmente, contribuído para o aumento da inserção de amostras-problema na base de dados forense. No primeiro extrato, o/a geneticista forense, realça, para além do já referido, o contributo fundamental da sua categoria profissional para a sensibilização da classe dos juízes relativamente à importância dos pedidos de inserção de perfis de DNA na base de dados forense.

“A nova lei também faz com que se calhar aumente o número de condenados [inseridos na base de dados]. (...) Em termos de tribunais isso será uma forma mais automática (...). E assim como com os condenados houve uma evolução, mais juízes a solicitarem a inserção de perfis de condenados, com as amostras-problema também tem estado a acontecer isso. Um bocadinho com insistência da nossa parte, a questionar se pretendem [a inserção do perfil], e as pessoas que trabalham nessas áreas começam a ficar sensibilizadas para aquilo.” [N07-geneticista forense]

“(...) É a verdadeira função da base de dados, só que havia muitas restrições até então, a antiga lei implicava muitas restrições, tinha de ser sempre com uma ordem judicial, colocar questões. Portanto burocratizavam muito o processo, e agora pode eventualmente ficar um pouco mais facilitado” [N22-geneticista forense]

Os/as entrevistados/as pertencentes à entidade de supervisão e regulação da base de dados forense portuguesa mostram posições algo opostas quanto ao balanço que fazem das atividades e do enquadramento legal da mesma. Por um lado, sob uma ótica otimista, parte dos elementos da entidade de supervisão faz uma avaliação positiva em relação à sua progressão no que diz respeito ao aumento da inserção de perfis de DNA. No extrato,

refere-se que o facto de a base de dados portuguesa ser recente não permite uma avaliação completa do seu desempenho, contudo, é revelada satisfação com o seu desenvolvimento.

“[E]u acho que a base tem progredindo positivamente. (...) Mas enfim, as coisas têm o seu tempo, a base também ainda não existe há tanto tempo quanto isso, acho que a avaliação que eu posso fazer, genérica, é que tem progredido positivamente.” [N18-entidade de supervisão/regulação]

Num tom notoriamente mais crítico e revelador de desconforto quanto ao modo como a base de dados entrou em funções, um/a dos/as entrevistados/a, pertencente à entidade de supervisão, realça dois aspetos que considera serem de extrema relevância na avaliação que faz da base de dados. Primeiro, começa por revelar que, na sua perspetiva, um dos pontos mais comprometedores da criação da base de dados forense portuguesa foi precisamente o ‘desinteresse’ político neste tópico. Esta constatação parece contrariar a aura de positivismo que revestiu o discurso político da criação da base de dados como uma ferramenta que iria ajudar a resolver o crime com maior celeridade e eficácia no país através da ciência forense (Lentzos, 2006; Machado, 2011; Machado & Silva, 2010).

“Do meu ponto de vista uma das grandes questões emergentes das bases de dados é o desinteresse absoluto da Assembleia da República, e deve dizer-se, do Governo, dos Governos sucessivos.” [N11-entidade de supervisão/regulação]

Segundo, realça que a independência da entidade de fiscalização, no seu início de atividade, foi largamente condicionada por critérios legais desadequados. Tal como anteriormente referido por um/a dos/as geneticistas forenses, no seguinte excerto, o/a participante, explica a dependência financeira do Conselho de Fiscalização em relação ao instituto detentor da custódia da base de dados forense, respetivamente, o INMLCF. Nas suas palavras, esta situação apresentava-se como bastante problemática, sendo mais tarde retificada através da lei orgânica do Conselho de Fiscalização (artigo 3.º da Lei n.º 40/2013).

“O Conselho de Fiscalização da base de dados de perfis de ADN é um órgão administrativo independente, que só está relacionado com a Assembleia da

República, e o seu orçamento depende do orçamento da Assembleia da República. E agora a grande pergunta: ‘Quem é que gere o orçamento que o Conselho tem?’ Quem fazia a gestão do orçamento era o Instituto de Medicina Legal (...). Isto é a maior barbaridade que alguma vez se pode imaginar.” [N11-entidade de supervisão/regulação]

Relativamente às alterações propostas à Lei n.º 5/2008 materializadas na Lei n.º 90/2017, todos os membros da entidade de supervisão e regulação entrevistados demonstram estar de acordo com a necessidade de renovar certos aspetos legais da base de dados forense. No entanto, reconhecem que, apesar dos esforços, a inserção dos perfis de DNA na base de dados continua a ser um ponto debilitante no seu funcionamento. No primeiro extrato, o/a entrevistado/a tece críticas à (in)capacidade interpretativa dos juízes portugueses relativamente às normas processuais que, no seu entender, obrigam à inserção consecutiva de perfis de DNA de condenados, por crime doloso, a penas de prisão efetiva igual ou superior a três anos. Na sua perspetiva, o carácter facultativo na ordenação da inserção do perfil de DNA na base de dados, por parte do juiz, não está a ser corretamente interpretado, sendo que esta imprecisão continua por resolver com a entrada em vigor da nova lei. No segundo extrato, de um membro da entidade de supervisão e regulação, é reforçada a premissa de que é possível, ao nível legal, fazer novos ajustes no sentido de melhorar o funcionamento da base de dados. No entanto, alerta para o facto de que se este processo for demasiado rápido pode encontrar demasiada resistência política. No mesmo excerto, denota-se, de modo semelhante ao anterior, que é dada demasiada margem legal e interpretativa aos juízes no que concerne à decisão de ordenarem ou não a inserção de um perfil de DNA na base de dados forense.

“Primeiro problema gravíssimo do meu ponto de vista, e que não foi resolvido agora de modo nenhum, se for ao Código de Processo Penal não tem uma única norma sobre prova genética. (...) Porque a lei 5/2008 tem normas processuais, que não têm de estar ali (...). Os juízes têm uma tendência extraordinária em não ver as normas processuais penais, quando não estão no Código de Processo Penal, e não as interpretar como sendo normas processuais penais. De maneira que, do meu ponto de vista, fazem barbaridades. Dizer: ‘Ah, não é obrigatório mandar’ [ordenar a

inserção do perfil de DNA]. Não! É obrigatório, está lá que é obrigatório.” [N11-entidade de supervisão/regulação]

“Acho que (...) há coisas que ainda podem ser alvo de correção na legislação. Mas não sei também se nós estamos preparados para ir muito além, muito rápido. (...) Eu acho que a lei continua a deixar uma margem considerável naquilo que é a possibilidade de se inserir ou não inserir o perfil. (...) Acho que continua a não ser muito afinada nesse sentido e, portanto, acho que aí ainda há caminho a fazer.” [N25-entidade de supervisão/regulação]

Como se pode observar, no excerto supramencionado, o/a entrevistado/a refere que o facto de as alterações à lei da base de dados serem insuficientes teve que ver com a potencial resistência, por parte de alguns atores políticos, se fossem propostas alterações legais mais significativas. Portanto, depreende-se que, apesar de ainda não serem suficientes, as alterações efetuadas no enquadramento legislativo da base de dados forense tiveram como objetivo permitir uma maior eficácia da base de dados relativamente à sua utilidade para a investigação criminal. Neste sentido, no extrato a seguir apresentado, o/a entrevistado/a refere que não se pretendeu ferir o ‘paradigma conservador’ (N03) característico da base de dados portuguesa, nem colocar o equilíbrio entre a proteção de dados pessoais e a necessidade de resolução de crimes em situação de tensão. Sendo que, a tentativa de conservar este paradigma pode ter sido uma das principais causas para os poucos ajustes legais da base de dados.

“Tentou-se, sem mudarmos este paradigma conservador ou contido da nossa lei na relação, ou na tensão entre proteção de dados pessoais, direitos fundamentais *versus* interesses e eficácia da investigação. Pretendeu-se (...) introduzir algumas alterações com vista a conseguir eventualmente alguns ganhos de eficácia na investigação. Facilitando um pouco alguns aspetos da inserção de perfis de amostras-problema.” [N03-entidade de supervisão/regulação]

Na generalidade, os/as entrevistados/as pertencentes a órgãos de investigação criminal fizeram um balanço pouco positivo em relação às atividades da base de dados

forense portuguesa. Uma das vulnerabilidades mais elencada por estes profissionais é a falta de perfis na base de dados para a obtenção de correspondências úteis para a investigação criminal (Machado, 2016, p. 11; Machado, et al., 2011; Santos et al., 2013). Deste modo, compreende-se que, na perspetiva dos/as participantes, a utilidade da base de dados encontra-se explicitamente dependente da sua capacidade de gerar correspondências que possam auxiliar os investigadores na resolução de crimes, como se pode observar no seguinte extrato:

“A nossa base de perfis de ADN é uma base reduzida, tem poucos perfis. (...) Mas continuo a dizer, as bases de dados só dão aquilo que lá têm. E mais, não dão em definitivo, sugerem.” [N19-órgão de investigação criminal]

A expansão generalizada da base de dados forense a toda a população portuguesa é considerada, por parte de um/a dos/as entrevistados/as desta categoria profissional, como uma medida eminente que a longo prazo poderá tornar-se obrigatória. Apesar da sua formação ser em direito, a racional que conduz a argumentação deste/a participante está intimamente relacionada com as funções de investigação policial que desempenha ao nível profissional. Observa-se, portanto, um ‘imaginário forense’ (Williams, 2010) que equaciona a base de dados forense de acordo com as suas capacidades promissoras de identificação que aumentam com a expansão dos critérios de inserção na mesma (Brown et al., 2006; Tutton & Levitt, 2010). No entanto, não existe uma reflexão sobre o seu potencial no tempo presente, nem o custo económico que uma decisão desta amplitude implicaria para o país. Sendo que um dos argumentos para a não aprovação de uma base de dados universal em Portugal no início da sua discussão se pautou precisamente pelos elevados custos económicos da mesma (Machado et al., 2012, p. 183).

“Mais tarde ou mais cedo, quando fizermos um cartão cidadão, (...) eu acredito que o perfil genético será recolhido. (...) Quanto mais a base de dados estiver preenchida, mais possibilidade de comparação teremos, se for recolhido um vestígio biológico e em muitos crimes é fácil a recolha de vestígios biológicos, temos a probabilidade de ter logo o suspeito. Se não tivermos perfis inseridos, de que é que adianta ter uma lei? Isso é importantíssimo.” [N28-órgão de investigação criminal]

Critério de inserção do perfil de DNA na base de dados forense

No decorrer das entrevistas foi solicitado aos/às participantes do presente estudo que refletissem sobre um dos critérios de inserção de perfis de DNA na base de dados forense portuguesa. Concretamente, o que diz respeito à inclusão de arguidos condenados por crime doloso, com pena concreta de prisão igual ou superior a três anos, por ordem do juiz (n.º 2 do artigo 8.º da Lei n.º 90/2017).

A discussão em torno deste critério de inserção de perfis de DNA na base de dados, por parte dos entrevistados pertencentes à categoria de entidade de supervisão/regulação, remeteu para questões associadas à proporcionalidade relativamente ao critério do limite mínimo de três anos de pena efetiva. Na sua grande maioria, os/as entrevistados mostram-se críticos da opção tomada pelo legislador na Lei n.º 5/2008. Dito isto, no extrato apresentado, são elencados três pontos de reflexão acerca desta medida. Primeiro começa-se por referir que a base de dados deveria incluir todas as pessoas condenadas por um crime, em linha com critérios mais expansivos característicos de outros Estados-Membros (Santos et al., 2013). Segundo, elenca-se a discrepância entre os crimes que mais contribuem para a base de dados, sendo que podem estar a deixar-se de fora crimes que, por não permitirem uma moldura penal acima dos três anos de pena efetiva, são excluídos da base de dados. Terceiro, reforça-se a vontade da construção de uma base de dados mais ampla que, deste modo, não deveria depender da ordem judicial para a inserção do perfil de DNA na base de dados. Denota-se, através das palavras do/a entrevistado/a, uma vontade explícita de instrumentalizar a base de dados portuguesa numa racional que denuncia a pretensão por uma ferramenta de carácter mais expansivo do que o que está transposto na lei (*idem*). Sendo que, esta posição vem contrariar por completo a tradição jurídica conservadora dos direitos humanos que está implícita na lei que deu origem à criação da base de dados (Machado et al., 2012; Moniz, 2009).

“Eu acho que não devia ser preciso sequer que as pessoas tivessem de ter uma pena de um determinado número de anos, isso para mim, a questão do ADN tem de ser uma questão universalizada, pronto. Mas tendo em conta o que está descrito na legislação (...) há determinados crimes que de uma forma mais geral têm essa tipologia de pena, superiores a 3 anos, e, portanto, contribuem mais para a base, quando há outros crimes, de natureza diferente, que podem ter um valor

inferior a esse que está estipulado para entrar na base, e portanto que ficam de fora. (...) Tendo em conta a forma como eu vejo a base, eu acho que [a inserção] devia ser quase automática, não acho que devesse ficar dependente de uma instrução de um juiz.” [N25-entidade de supervisão/regulação]

Um/a outro/a entrevistado/a, também crítico/a do critério do limite mínimo de três anos de pena concreta para ordenação da inserção de perfil de DNA na base de dados, reconhece que o legislador pretendeu englobar neste critério a discussão em torno da proporcionalidade desta prática. A este respeito, a literatura dá-nos conta de que a proporcionalidade dos critérios de inserção de indivíduos nas bases de dados forenses tem sido largamente discutida em torno do balanço entre os direitos individuais e a necessidade de garantia do bem comum da sociedade (Bigo, 2008; Cavoukian, 2001; Heinemann et al., 2012; Toom et al., 2016; Tseloni & Pease, 2010). O/a entrevistado/a prossegue a sua reflexão referindo que, mesmo tendo em consideração o debate em torno da proporcionalidade, seria mais prudente adicionar um outro critério material à inserção do perfil. A sua opção por um critério misto teve como principal enfoque evitar que indivíduos condenados por certos crimes, com moldura penal inferior a três anos, não pudessem ser inseridos na base de dados devido ao critério escolhido pelo legislador.

O/a entrevistado/a refere também que, do mesmo modo que podem existir indivíduos que deveriam constar na base de dados e não constam, também se pode verificar a inserção de indivíduos condenados (com pena superior a três anos) que podem não ter um perfil de interesse para a investigação criminal. Neste caso, depreende-se que a solução sugerida por este/a profissional é uma tentativa de tornar os critérios de inserção de perfis de DNA mais proporcionais. Pois, a adição de um novo ponto poderia, por um lado, evitar que indivíduos que não tenham um perfil de interesse para a base de dados fossem inseridos na mesma. Por outro lado, potenciar uma construção mais eficaz da base de dados com perfis que entende serem mais adequados para a resolução do crime.

“Eu percebo que a intenção do legislador foi essa ideia de proporcionalidade. Tendo a achar que esse critério dos 3 anos é um critério um pouco cego. (...) Eu não sei se não devíamos misturar, ou ter aqui um critério material. Como a lei fala em 3 anos, há muitos crimes que são punidos com penas inferiores a 3 anos relativamente

aos quais se calhar se justificaria ser colhida uma amostra e depois analisada e inserida na base. E se calhar em relação a outros crimes punidos com pena de prisão superior a 3 anos, são perfis que lá ficam e que se calhar nunca vão ser utilizados.” [N18-entidade de supervisão/regulação]

A par das características restritivas dos critérios de inserção de perfis de DNA na base de dados forense em Portugal (Machado, 2016, p. 11; Machado et al., 2011; Santos et al., 2013), um/a dos/as entrevistados/as refere que a opção plasmada na lei revela um carácter conservador. No extrato, esta percepção encontra-se implícita no argumento de que ao garantir um ‘consenso’ para a criação da base de dados, se tenham colocados limites que condicionam a própria investigação de âmbito criminal. O culminar de uma lei de carácter restritivo em relação à metodologia de inserção de perfis de DNA na base de dados teve como justificação a necessidade de se chegar a um consenso político aquando da discussão em torno das medidas a adotar (Machado & Silva, 2010, p. 226). Pois, certos partidos políticos, mostraram-se receosos quanto aos riscos que a utilização de amostras biológicas e dados genéticos para fins de investigação criminal poderiam implicar para os direitos civis. Em Portugal, o debate político que acompanhou a proposta da construção de uma base de dados universal (Machado & Silva, 2010, p. 218; Machado & Silva, 2008b) culminou na criação de um dos enquadramentos legais mais restritivos no seio da União Europeia.

“Eu acho que é uma solução que pretendeu de alguma forma assegurar, digamos, um certo, não sei se consenso (...). Digamos que se terá sempre manifestado alguns receios, precisamente, quanto aos perigos e aos riscos que a utilização das amostras biológicas e dos dados genéticos para fins de investigação criminal podem acarretar. (...) Portanto, eu acho que isso acaba por, pronto, condicionar bastante, como é evidente a nossa opção é uma opção, nesta perspetiva, conservadora.” [N03-entidade de supervisão/regulação]

A perspetiva dos entrevistados que fazem parte de órgãos de investigação criminal foca-se nas vantagens que Portugal poderia obter ao possuir uma base de dados forense com critérios mais abrangentes para a inserção de perfis de DNA. A necessidade de resolver crimes e deter comportamentos criminosos através de métodos expansivos de vigilância

biométrica (Chow-White & Duster, 2011; Duster, 2004, 2006; Machado et al., 2010) encontra-se explicitamente plasmada na narrativa do/a entrevistado/a cujo extrato se encontra abaixo apresentado. Esta intenção é velada pelo repúdio do critério escolhido pelo legislador, pois, no seu entender enquanto investigador/a criminal, o mais adequado seria a inserção do perfil de DNA de todos os arguidos e condenados por qualquer tipo de crime na base de dados forense. Numa perspetiva policial, a racional em relação à expansão das bases de dados forenses em termos de critérios de inserção passa precisamente pela sua capacidade em resolver crimes hediondos através de correspondências com perfis inseridos por ofensas menores. Portanto, no extrato constata-se a não concordância com o enquadramento legal atual das diretrizes para a inserção de perfis de DNA, bem como a vontade do/a entrevistado/a em relação à adoção de uma base de dados de carácter mais expansivo que, segundo o/a mesmo/a, permite uma melhor e mais eficaz deteção do crime.

“Quem trabalha na área policial constata uma coisa, o ser humano é um animal de hábitos. E isso reflete-se na nossa vida, a nossa tendência a seguir os estudos numa área específica, isto vai acompanhar-nos ao longo da vida, o criminoso é a mesma coisa. (...) Será que o legislador não está a pôr a malha da rede muito larga, e vamos só penalizar aqueles que são condenados de 3 anos para cima, porque não todos os arguidos, seja ele qual for na área criminal? (...) Nós nunca sabemos, por exemplo, há cá *serial killers* registados que foram apanhados por uma simples infração de trânsito. Uma coisa simples, que vai resolver o crime bárbaro.” [N28-órgão de investigação criminal]

De modo geral, os profissionais desta categoria situam as suas narrativas num plano que privilegia a capacidade de produção de inteligência através da base de dados forense (Bigo, 2006; Innes et al., 2005). Sendo que o aumento no número de perfis de DNA nesta infraestrutura encontra-se implicitamente associado a uma maior eficácia na produção de inteligência. Porém, mostra-se redutor cingir o aumento da capacidade de produção de inteligência à expansão dos critérios de inserção (Santos et al., 2013) na base de dados portuguesa, pois é igualmente importante o tipo de perfil dos indivíduos que constam na mesma. Como se observou, por exemplo, no Reino Unido, a eliminação de perfis da base de dados por ordem judicial não afetou o número de correspondências positivas, pois estes

não eram relevantes do ponto de vista da investigação criminal (Amankwaa & McCartney, 2018, p. 120).

O/a único/a entrevistado/a da categoria Professor(a)/investigador(a) que elaborou comentários acerca desta questão possui formação em direito e mostra-se igualmente crítico do modelo de inserção de perfis de DNA seguido pelo legislador português. Em particular, no excerto abaixo representado, denota que, apesar de se considerar pessoalmente um/a defensor/a dos direitos humanos, a marca dos três anos é demasiado elevada para os objetivos que a base de dados forense se propõe a cumprir. Depreende-se que, mesmo numa perspetiva que englobe os direitos humanos, o critério em utilização revela-se demasiado protetor dos indivíduos responsáveis por certos crimes. Isto porque o limite escolhido pelo legislador português pode, em última análise, jeopardizar o direito à restituição da justiça por parte das vítimas e das suas famílias quanto aos crimes que lhes causaram danos físicos, morais e/ou psicológicos.

“A minha primeira reação, apesar de eu me considerar como defensor/a dos direitos e liberdades das pessoas acima de tudo, a minha primeira reação é que de facto é um regime, este de só permitir a recolha (...) de amostras a condenados por crimes a mais de 3 anos que é, eventualmente, demasiado protetor. (...) Não é que eu tenha uma alternativa a propor, mas parece-me exigente.” [N17-Professor(a)/investigador(a)]

Apesar de a vontade política ter ditado que Portugal se apresentasse como um dos países com a lei da base de dados forense mais restritiva de toda a União Europeia, as respostas dadas pelos participantes demonstram que a sua grande maioria não concorda com o critério adotado. Os/as entrevistados/as da categoria entidade de supervisão/regulação apontam as suas respostas para uma nova interpretação da proporcionalidade desta prática, por considerarem o critério de inserção demasiado lato para ser útil e eficaz na investigação criminal. A sua (re)interpretação do conceito de proporcionalidade culminou na sugestão da inclusão de critérios mistos na inserção de perfis de DNA na base de dados com o objetivo de filtrar de forma mais adequada os indivíduos que devem constar na mesma. Portanto, *grosso modo*, a proporcionalidade entre os direitos civis, como a privacidade e a proteção de dados, e o bem comum assegurado

através da restauração da segurança pública foi reavaliada no sentido de dar mais poder aos órgãos de investigação criminal.

Relativamente à categoria dos órgãos de investigação criminal assiste-se a uma instrumentalização completa das capacidades da base de dados forense. Numa ótica que deixa completamente de parte o equilíbrio entre o bem comum e os direitos individuais por se assumir que a diminuição das taxas de criminalidade e a resolução de crimes são objetivos por si só justificativos da supressão de direitos em prol da segurança. Numa perspetiva de carácter policial, um crime menos grave que dê origem à inserção de um perfil de DNA na base de dados forense pode levar a uma condenação num crime mais grave no futuro (Santos et al., 2013, p. 8). Toda esta retórica teve por base uma premissa que assenta na reincidência quase certa das pessoas que cometem crimes. Por fim, na categoria professor(a)/ investigador(a), numa perspetiva voltada para os direitos humanos, é referido que um critério tão alto para a inserção de perfis de DNA pode colocar em causa os direitos das vítimas de crimes que, em última instância, podem não ver os prejuízos/danos sofridos pelos crimes restabelecidos.

Vantagens e desafios do sistema Prüm⁵⁷

A criação do sistema Prüm deu-se devido à necessidade de se otimizarem as ferramentas para o policiamento e captura das pessoas responsáveis pela perpetuação de crimes transnacionais (Amankwaa, 2019; Sallavaci, 2017; Santos, 2017; Santos & Machado, 2017). Como tal, o objetivo deste sistema passa pelo controlo do crime organizado e do terrorismo no seio da União Europeia. Sumariamente, o sistema Prüm, começou por existir enquanto Tratado de Prüm que foi assinado em 2005 por um número restrito de países pertencentes à União Europeia. Mais tarde, em 2008, foi transposto para a lei da União, passando a adotar um carácter obrigatório. Esta decisão obrigou a que todos os Estados-Membros possuissem bases de dados de perfis de DNA operacionais que permitissem o aumento da partilha de informações de carácter policial e judicial no Espaço Schengen. A iniciativa da criação de uma ferramenta com estas características teve como objetivo a aproximação da União Europeia ao que tinha sido estabelecido no Programa de Haia, isto é, o fluxo livre de informações relacionadas com a aplicação da lei entre Estados-Membros –

⁵⁷ Sistema Prüm engloba tanto o Tratado de Prüm como as Decisões Prüm, pois os/as entrevistados/as não fizeram essa diferenciação no âmbito das suas respostas.

ou ‘princípio da disponibilidade’ (McCartney, 2014b, p. 4). O resultado do cumprimento do programa passará pela existência de “uma base de dados virtual da UE para efeitos de aplicação da lei, onde a inserção de informações numa base de dados forense em qualquer Estado-Membro se encontre disponível para os restantes” (Human Genetics Commission, 2009, para 5.10)

O sistema Prüm regula que, num primeiro momento, a pesquisa de informação seja realizada num sistema de *hit/ no hit*. Só depois de findado este processo de confirmação da correspondência é que se procede à partilha de dados através dos canais de assistência mútua dos países envolvidos na pesquisa. Portanto, o segundo passo depende dos enquadramentos legais nacionais dos Estados-Membros, pelo que pode ou não ocorrer a partilha de dados demográficos dos cidadãos (McCartney, 2014b, p. 4). Tendo em consideração o carácter transnacional que envolve a partilha de dados no âmbito da investigação criminal, torna-se essencial que, em particular nos perfis de DNA, existam regras estandardizadas que garantam a harmonização científica entre Estados-Membros (Bowker & Star, 1999; Goos et al., 2015; Lampland & Star, 2009; Prainsack & Toom, 2010, 2013).

Uma das dimensões do guião de entrevista aplicado no decorrer do presente estudo teve por base questões relacionadas com o papel de Portugal no sistema Prüm e vice-versa. Neste sentido, pretendeu-se compreender quais as perspetivas dos entrevistados quanto às motivações que levaram Portugal a entrar no sistema Prüm, quais as vantagens associadas a esta ferramenta, bem como os desafios que se podem enfrentar neste contexto de cooperação policial e judiciária.

A maioria dos geneticistas forenses entrevistados no âmbito do presente estudo revelam, a par com a literatura, que a criação de sistemas de partilha de informação para fins de investigação criminal foi um passo fundamental para permitir acompanhar a nova realidade no espaço europeu (Amankwaa, 2019; Santos, 2017; Santos & Machado, 2017). O novo contexto teve que ver essencialmente com a adoção do Tratado Schengen⁵⁸ que teve como principal ambição a promoção da livre circulação de pessoas entre Estados-Membros. Contudo, a abertura das fronteiras internas da União Europeia veio, por sua vez, aumentar os desafios destes países em relação à segurança nacional que veio acompanhada de

⁵⁸ Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:l33020>. Acesso a 12 de maio de 2020.

discursos políticos “contra o terrorismo e o crime organizado” (Hert, 2005). Portanto, a simplificação da circulação dos cidadãos europeus entre Estados-Membros trouxe vantagens no plano económico, mas também permitiu que o crime se transformasse num fenómeno transnacional através da circulação de indivíduos que cometem crimes. O extrato apresentado, demonstra explicitamente um entendimento claro em relação aos ‘problemas comuns’ da União Europeia, numa perspetiva claramente europeísta que reproduz os argumentos basilares à criação do sistema Prüm.

“Prüm não é mais do que exatamente a partilha de informação entre os vários países. Ora se nós sabemos que nos movemos cada vez com mais facilidade, um indivíduo está aqui e pode ir praticar um crime noutro país. Portanto é importantíssimo que haja essa troca de informação. Estamos numa Europa comum com problemas comuns.” [N06-geneticista forense]

Para além da simplificação no processo de identificação de pessoas que cometem crimes no espaço interno da União Europeia, alguns entrevistados, como se observa no extrato, referem que o sistema Prüm também é relevante para a criação de inteligência sobre as trajetórias criminosas de certas pessoas e grupos de criminalidade organizada. Neste sentido, sendo o sistema Prüm uma ferramenta de verificação da identidade de pessoas que cometeram crimes, pode revelar-se igualmente útil para a investigação criminal pois permite também a identificação subjetiva através do ‘intelligence-led policing’ (Bigo, 2006; Williams & Johnson, 2004b). Implicitamente, o reconhecimento dos padrões de atividade criminal em vários países veio permitir que os indivíduos que perpetuam esses mesmos atos possam ser responsabilizados nos vários Estados-Membros.

“Eu acho que é fundamental porque pode até não permitir que se apanhe um criminoso, mas conseguir até definir o trajeto que a pessoa tem feito. Por exemplo, se houver um *hit* a nível de Prüm de amostras-problema, consegue-se definir que aquela pessoa já fez um crime num país e já passou por outro e até pode ajudar também na investigação.” [N07-geneticista forense]

A implementação das Decisões Prüm apoiou-se numa lógica de harmonização e estandardização técnico-científica que pretendeu mitigar e ultrapassar as diferenças legais, culturais e políticas dos Estados-Membros (Lampland & Star, 2009; Prainsack & Toom, 2010, 2013). Sendo que a partilha e o fluxo de dados pessoais neste contexto só foram possíveis com a criação de *standards* que pretenderam tornar compatíveis sistemas (bases de dados forenses) *a priori* incompatíveis (Balzacq et al., 2006; Bigo, 2008; De Hert & Gutwirth, 2006; McCartney 2014a, 2014b). Enquanto tecnologia de vigilância, o sistema Prüm, usufruiu do aumento da amplitude da regulação transnacional quanto à gestão de tecnologias em vários setores de atividade, como na investigação criminal e no controlo do crime (Djelic & Sahlin-Andersson, 2006; Hallström & Boström, 2010; Timmermans & Epstein, 2010). Sendo que a governação transnacional do sistema Prüm veio reiterar a noção de que as fronteiras físicas de um país não se circunscrevem necessariamente às fronteiras regulatórias, citando, “[n]ational regulatory patterns can quickly get transnationalized and transnational initiatives are having a local impact” (Djelic & Sahlin-Andersson, 2006, p. 2).

Alguns dos geneticistas forenses entrevistados vão ao encontro da literatura supracitada e realçam o papel fundamental que a estandardização de procedimentos e a harmonização legal pode desempenhar numa situação de cooperação transnacional como a que se observa com o sistema Prüm. Pode observar-se no extrato que o/a entrevistado/a considera a existência de documentos formais, produzidos pela União Europeia para a partilha de dados ao nível transnacional, como um aspeto muito relevante para o garante das boas práticas de partilha de dados.

“O papel de Prüm é importante, têm de existir tratados, tem de haver regras para os países saberem como é que se podem orientar e têm de haver regras comuns a todos.” [N20-geneticista forense]

Relativamente à estandardização de procedimentos e práticas científicas, os restantes geneticistas forenses enfatizam a necessidade de acreditação dos laboratórios forenses que fazem perícias de DNA no contexto da investigação criminal. Esta creditação vem garantir que tanto os dados pessoais transmitidos como os dados pessoais que os países recebem de terceiros são cientificamente legítimos e validados. Nesta ótica, um/a destes/as profissionais considera que com o sistema Prüm se verifica uma maior

responsabilidade por parte dos órgãos responsáveis pelos laboratórios e pelos dados partilhados (McCartney, 2014b). A argumentação dos entrevistados subjacente à acreditação dos laboratórios forenses pauta-se pelos princípios da confiança na utilização de dados genéticos para fins de investigação criminal, nomeadamente, pela utilização de métodos ‘rigorosos, transparentes e auditáveis’, bem como através de procedimentos standardizados (McCartney et al., 2011, p. 306). Tendo em consideração o processo de acreditação e as medidas implementadas para o estímulo da confiança nos resultados laboratoriais, os geneticistas forenses apresentam uma perspetiva em relação aos laboratórios que coincide com os princípios da objetividade e standardização (Lynch, 2002; Machado & Granja, 2018).

“A necessidade desta partilha acabou por obrigar as diferentes entidades competentes a acreditarem os seus laboratórios, e a terem cuidado com todos os perfis que saem, as análises que fazem, a maneira como os resultados são expostos, precisamente para não haver qualquer tipo de dúvidas porque a responsabilidade é ainda maior. Portanto eu diria que ajuda no sentido de melhorar bastante na informação, não só que é obtida, como também que é transmitida para outros indivíduos.” [N21-geneticista forense]

No âmbito do guião da entrevista, os/as geneticistas forenses entrevistados/as foram convidados/as a refletir sobre os desafios mais prementes do sistema de Prüm. Novamente, as respostas recaem sobre a harmonização inerente a ferramentas que operam ao nível transnacional. Como já referido a standardização técnica parece ter alcançado um nível satisfatório para os entrevistados/as. Contudo, não deixam de enfatizar que as legislações nacionais em torno da cooperação policial e judicial também necessitam de um maior empenho na harmonização dos seus padrões de atuação (Prainsack, 2010, p. 22; Prainsack & Toom, 2013), conforme se pode observar no extrato abaixo apresentado. A posição dos/as entrevistados/as é reveladora das tensões locais e globais sentidas pelos países na procura pela harmonização das regulações nacionais (Hoeyer et al., 2016). Dito isto, o sistema Prüm enquanto agente de standardização da vigilância genética na União Europeia tem encontrado vários desafios. Pois, esta cooperação transnacional encontra-se embebida num contexto de diversidade política e legal, de diferentes tradições em relação

às tecnologias biométricas forenses, bem como diferentes expectativas e percepções em relação ao impacto societal operado pela vigilância. Entendendo-se que tem sido mais fácil atender aos critérios técnicos e científicos deste sistema do que às salvaguardas éticas, por exemplo, sobre privacidade e proteção de dados na partilha transnacional.

“Os principais desafios são, se calhar, termos alguma harmonização de legislação que permita que aquilo que a parte técnica já resolveu possa também concretizar-se a nível de pressupostos legais para a troca de informação. Ou seja, que se consiga com segurança, que algumas restrições legais possam ser levantadas.” [N02-geneticista forense]

O mecanismo de cooperação policial em dois passos foi um dos aspetos referidos pelos/as entrevistados/as no âmbito dos desafios do sistema Prüm. De modo geral, os/as geneticistas forenses mostram-se satisfeitos com o primeiro passo do sistema Prüm no contexto nacional. Sendo que a standardização técnica dos laboratórios e das infraestruturas exigida à implementação parece cumprir os requisitos impostos pelas Decisões Prüm (Lampland & Star, 2009, pp. 4-5; Prainsack & Toom, 2010, 2013). No entanto, a par das críticas já supramencionadas, consideram que o segundo passo tem-se demonstrado de maior complexidade quando se chega ao momento da partilha dos dados demográficos dos indivíduos com países terceiros. A complexidade do passo 2 identificada na narrativa dos/as participantes encontra-se em grande medida relacionada, num primeiro ponto, com o carácter restritivo da base de dados forense portuguesa (Santos et al., 2013; Machado, 2011, p. 157; Machado & Silva, 2010, p. 218). Num segundo ponto, com a alçada da base de dados forense, pois, em Portugal, a custódia pertence ao Ministério da Justiça. Neste caso a complexidade deve-se ao facto de as autoridades judiciais possuírem processos de partilha de informações tendencialmente mais morosos do que os dos órgãos policiais (Machado & Granja, 2019, pp. 11-12). Posto isto, os/as entrevistados/as referem que os pontos supramencionados se têm apresentado enquanto obstáculos à cedência de dados pessoais de nacionais a outros Estados-Membros no âmbito da investigação criminal, como se pode observar no excerto.

“Em termos de ligação do nosso país a vários outros, tem corrido bem do ponto de vista técnico. (...) No que se refere ao tal *second step* ou a partilha de dados pessoais, aí já tem havido alguma dificuldade. Portanto quando nós precisamos, tem havido algumas informações que têm vindo para cá. O inverso, isso já não tem acontecido tanto porque a nossa legislação é restritiva. (...) Tem havido *hits*, mas depois os dados pessoais não os temos enviado por falta desta solicitação de um juiz.” [N02-geneticista forense]

Decorrente do modo de implementação do sistema Prüm em contexto nacional, os/as geneticistas forenses indicam que o segundo passo condiciona a velocidade e o fluxo de dados genéticos entre os Estados-Membros em matéria de cooperação transnacional. Neste sentido, o peso burocrático elencado pelos/as entrevistados/as ao nível do sistema Prüm encontra-se intimamente relacionado com as características procedimentais que obrigam a que a partilha de dados pessoais compreenda os princípios da lei de Proteção de Dados nacionais, bem como os critérios mínimos estabelecidos pela Comissão Europeia para a proteção de dados (Machado & Silva, 2010; McCartney et al., 2011; Prainsack, 2010; Prainsack & Toom, 2010).

“O principal desafio neste momento ainda é a velocidade com que circula a informação. Depois da ocorrência de *hits*, acho que ainda há algumas burocracias que poderão atrasar certo tipo de procedimentos. O principal desafio seria tentar minimizar ao máximo essas burocracias que ainda limitam a brevidade com que deveria ser tomada uma determinada ação.” [N07-geneticista forense]

Um último tópico sobressaiu da narrativa dos/as geneticistas forenses e remete para a problemática da soberania dos Estados na cooperação transnacional para fins de investigação criminal. Neste sentido, a harmonização da regulação dos procedimentos legais da partilha de dados pessoais no plano transnacional tem sido difícil de alcançar, principalmente, devido à resistência na cedência de certos poderes de soberania dos Estado-Membros em matéria criminal (Hufnagel, 2012). A par desta situação, um/a dos/as entrevistados/as refere que um dos desafios do sistema Prüm advém do excesso de proteção dos Estados em relação aos seus cidadãos. Este ponto é revelador da possível falta

de confiança entre os países da União Europeia (Hufnagel & McCartney, 2015) que, devido a *standards* de proteção de dados diferenciados, podem considerar que os países terceiros não oferecem as proteções necessárias para se proceder à partilha de informação.

“Talvez hajam países que tentem proteger demasiado a entidade dos seus cidadãos, e não partilhar essa informação por isso.” [N20-geneticista forense]

Os membros de entidades de supervisão/regulação partilham a mesma posição em relação às motivações associadas à criação e implementação do sistema Prüm no seio da União Europeia (Amankwaa, 2019; Santos, 2017; Santos & Machado, 2017). A globalização trazida pelo desenvolvimento tecnológico e pela livre circulação de pessoas e bens dentro do espaço europeu trouxe consigo a vontade política de responder aos desafios impostos pela abertura de fronteiras. Neste sentido, encarando os ‘mecanismos de troca de informações’ (N25) enquanto tecnologias de vigilância, compreende-se que a sua criação e tendencial expansão é justificada por argumentos associados à gestão do risco (Bogard, 2007). Neste pano de fundo, os ataques terroristas de 11 de setembro de 2001 e, mais recentemente, em várias cidades europeias vieram reforçar a expansão de biotecnologias, como as bases de dados forenses. Contudo, vários autores têm reiterado que é necessária uma reflexão acerca da potencial ameaça e supressão da autonomia e da privacidade enquanto valores democráticos, bem como do (des)equilíbrio entre os direitos humanos e a segurança pública (Heinemann et al., 2012; Toom et al., 2016; Wayman & Nuger, 2005). No extrato apresentado, o/a entrevistado/a refere, de modo semelhante, que o sistema Prüm foi criado devido à necessidade de se acompanharem os avanços sociais associados à mobilidade na União Europeia. A argumentação subjacente a esta legitimação está intimamente relacionada com questões de segurança nacional e pública, sendo que o sistema Prüm veio suprir a necessidade de garantir maior segurança nas fronteiras e de facilitar a aplicação da lei (Hert, 2005; Liu 2013, p. 103).

“Eu acho que no mundo globalizado, se queremos estar dentro daquilo que é a esfera global, temos de estar alinhados com mecanismos de troca de informações a todos os níveis com outros países, seja na União Europeia, seja com países de língua portuguesa. E eu diria que foi esse o esforço que foi feito (...). Eu diria que terá

sido essa a motivação, pelo menos na minha cabeça faz sentido.” [N25-entidade de supervisão/regulação]

No entanto, um/a dos entrevistados/as foi particularmente crítico/a da passividade de Portugal na implementação do sistema Prüm referindo que todo o processo não foi mais do que uma adequação burocrática ao mesmo. A passividade enunciada por este/a profissional encontra-se em linha com o discurso político à data da criação da base de dados forense, onde foi realçado que Portugal deve esforçar-se por estar a par dos parceiros europeus. Deste modo, conseguiria seguir o exemplo dos países mais desenvolvidos em relação à utilização de dados genéticos para fins de investigação criminal, como também na adesão de sistemas de cooperação transnacional que estimulem a promoção de políticas de ‘combate’ ao crime (Machado & Silva, 2010, p. 219; Machado, 2006, p. 12). Da narrativa do/a entrevistado/a depreende-se que a vontade política de acompanhar os países mais desenvolvidos pode colocar em causa a capacidade de questionamento que a implementação de um sistema desta dimensão pode implicar para o contexto nacional. Em última análise, a frase do/a participante ‘metemo-nos na fila e lá fomos’ (N11) é a representação metafórica da falta de debate nacional no momento da implementação do sistema de Prüm. No segundo excerto, o/a entrevistado/a é ainda mais explícito/a quanto à vontade do Estado português em aderir a todos mecanismos de controlo da criminalidade que partem de iniciativas da União Europeia.

“O Instituto de Medicina Legal (...) fez os testes de compatibilidade, cumpriu os critérios e foi só burocraticamente que se fez a aproximação. Por parte da tutela não houve qualquer atitude proactiva, nem passiva. (...) Foi burocrática, exclusivamente burocrática. (...) Portanto não houve declaração, não houve adesão, não houve nada, pronto, metemo-nos na fila e lá fomos.” [N11-entidade de supervisão/regulação]

“Normalmente somos sempre muito bons alunos nessas coisas, aderimos a tudo. Eu acho que é um estado português, não tem a ver com esta matéria. Normalmente aderimos, assinamos. (...) É claro que racionalmente eu acho que foi

uma boa decisão. Mas o que pesou é, vamos nessa, é uma coisa nova, vai ser bom.”
[N18-entidade de supervisão/regulação]

A falta de regulamentação de âmbito transnacional que contemple todas as diretrizes sobre os modos de partilha de dados genéticos entre países é um dos desafios expressos pelos entrevistados desta categoria profissional. Do ponto de vista ético, garantir que a partilha ocorra mediante os mesmos *standards* de privacidade e proteção de dados é uma das formas de tornar esta prática transparente e de acordo com os direitos civis dos cidadãos europeus. Neste sentido, segundo o/a participante, a criação de um ‘manual de partilha de dados’ é um passo que deve ser tomado para a concretização da harmonização legal. Pois, deste modo, obter-se-ia a mitigação das diferenças entre enquadramentos jurídicos (Lampland & Star, 2009; Prainsack & Toom, 2010, 2013) podendo, inclusivamente, tornar todo o sistema mais automático. Associada à automatização sugerida, surge a noção de que a confiança entre Estados-Membros pode ser alcançada através da certificação dos procedimentos legais (Hufnagel & McCartney, 2015) de modo semelhante ao que se verifica nos processos de standardização obrigatórios ao nível técnico e científico do sistema Prüm.

“Eu acho que o problema está em não haver uma regulamentação para todos os países aderentes que obriga a que todos cumpram determinados parâmetros para incluir a base, estando esse caminho verificado a cooperação tem de ser, eu diria, quase automática. Porque se os sistemas são ‘certificados’, se todos os países membros confiam, existe a garantia de que toda a informação que foi incluída cumpre (...) a legislação de cada país.” [N25-entidade de supervisão/regulação]

A implementação do sistema Prüm em Portugal é entendida pelos entrevistados como um processo demasiado moroso que obrigou à procura de opções para que se conseguisse colmatar a impossibilidade de partilhar dados pessoais para fins de investigação criminal. As dificuldades técnicas sentidas tiveram que ver com o facto de a base de dados forense demorar demasiado tempo a ficar completamente operacional. Pois, a lei que permitiu a sua criação data de 2008, contudo, no site do Conselho de Fiscalização, os primeiros dados a respeito da inserção de perfis de DNA na base de dados portuguesa são

de 2013⁵⁹. Sendo que, em 2012, numa apresentação oral acerca da base de dados forense, Francisco Corte-Real deu conta de que até ao dia da conferência, constavam na base de dados 481 perfis de DNA retirados maioritariamente de amostras-referência em condenados (Conselho Nacional de Ética para as Ciências da Vida, 2012, p. 66). Uma das formas de colmatar as dificuldades na partilha de informação passou pelo recurso à lei da cooperação judiciária internacional em matéria penal (Lei n.º 115/2009) com o objetivo de tentar satisfazer os pedidos feitos por parte dos parceiros europeus.

“As decisões [Prüm] são fundamentais, é pena que não estejam devidamente implementadas, e o tempo que demorou no que diz respeito ao ADN... Nós durante muito tempo mediávamos a questão usando as leis da cooperação judiciária. (...) Esticávamos ao máximo a cooperação judiciária para abranger todos os pedidos que vinham.” [N11-entidade de supervisão/regulação]

A argumentação em torno da legitimação do sistema de Prüm segue os mesmos contornos dos restantes aparelhos tecnológicos de vigilância, pois recorre ao discurso sobre a necessidade de combater o terrorismo como forma de justificar o (re)equilíbrio da liberdade e da privacidade com a segurança coletiva (Bigo, 2008, p. 92; Hert, 2005). Denote-se que o sentimento de insegurança em relação ao terrorismo tem sido disseminado à luz de processos culturais que dão voz às ‘inseguranças modernas’ devido ao carácter imprevisível desta tipologia de crime (Monahan, 2010). Apesar da conjuntura de insegurança, a proteção dos direitos e liberdades civis em causa com a partilha transnacional de informações pessoais para fins de investigação criminal é uma das preocupações mais elencadas pelos entrevistados desta categoria profissional. Como se pode observar no seguinte excerto representativo desta narrativa:

“É a proteção dos direitos, não é? Temos de acautelar sempre que não há excessos. E isto é muito importante, mas relativamente a fenómenos como o terrorismo que é um fenómeno europeu, é uma preocupação europeia, esta cooperação é fundamental.” [N18-entidade de supervisão/regulação]

⁵⁹ Disponível em <http://www.cfbdadosadn.pt/pt/bdpadn/sobreabd/Paginas/ConteudoFicheiros.aspx>. Acesso a 12 de maio de 2020.

Em relação aos entrevistados dos órgãos de investigação criminal, estes são unânimes quanto à capacidade de produção de inteligência forense através das correspondências no sistema Prüm (Bigo, 2006). No excerto selecionado, o/a participante reitera e reproduz uma racional característica das entidades policiais (Innes et al., 2005) para referir que a centralização estimulada pelo sistema Prüm permite chamar a atenção para associações que até então poderiam passar despercebidas aos operacionais no terreno, principalmente, devido à fragmentação das informações.

“As perguntas não se satisfazem apenas com as suas respostas, o facto de existir a pergunta já leva a perceber que existiu a dúvida. E às vezes saber-se que existiu a dúvida é importante para outro tipo de coisas, de onde a centralização permite criar alguma inteligência, permite criar aquilo que nós chamamos de inteligência forense (...) no contexto das situações concretas. E Prüm obrigou-nos a uma reorganização.” [N19-órgão de investigação criminal]

No plano dos desafios trazidos pelo recurso a um sistema de grande escala de partilha transnacional de dados pessoais no âmbito da investigação criminal, os entrevistados demonstram estar a par da possibilidade de ocorrerem falsos positivos (McCartney, 2014a; Kierkegaard, 2008; Prainsack & Toom, 2010; Santos & Machado, 2017; Toom, 2018; Van der Beek, 2011). No extrato, esta preocupação encontra-se plasmada no reconhecimento da importância de organismos transnacionais que colmatem a necessidade de se cumprirem determinados passos no decorrer da recolha da prova. Sendo esta uma medida que pode permitir a redução de situações em que certos indivíduos possam ver os seus direitos fundamentais diminuídos com base em provas não legítimas. Neste sentido, a ocorrência de um falso positivo pode ter origem na contaminação de amostras na recolha das provas em cena de crime, onde a formalização dos procedimentos da cadeia de custódia da prova poderia ser uma das soluções a adotar (Krimsky & Simoncelli, 2011; McCartney, 2004, 2006b; Murphy, 2007, 2018; Toom, 2018). O objetivo seria, mais uma vez, o da mitigação das diferenças entre países nesta matéria (Lampland & Star, 2009; Prainsack & Toom, 2010, 2013).

“Tem de haver entidades internacionais que promovam a certificação sobre determinado tipo de passos, e esses passos têm de ser cumpridos religiosamente, como por exemplo, a cadeia de custódia na prova, é importantíssimo, para a salvaguarda dos tais princípios de defesa do arguido.” [N28-órgão de investigação criminal]

Numa perspetiva semelhante à apresentada pelos participantes pertencentes a entidades de supervisão/regulação, os elementos de órgãos de investigação criminal referem que Portugal possui uma cultura europeísta que se sustenta no princípio da reciprocidade entre Estados-Membros (Hufnagel & McCartney, 2017; McCartney, 2017) como premissa justificativa para a adesão ao sistema Prüm. Esta observação encontra-se em linha com a vontade política, demonstrada por Portugal, em acompanhar os países mais desenvolvidos em matéria de investigação criminal (Machado & Silva, 2010, p. 219; Machado, 2016, p. 12). Como se pode observar no extrato, o/a entrevistado/a realça o carácter vanguardista nacional na ratificação de acordos com outras comunidades.

“É no âmbito do princípio da reciprocidade, e é algo cultural, digamos assim. Portugal normalmente está na vanguarda dos países que normalmente tem tendência a ratificar os acordos com outras comunidades.” [N28-órgão de investigação criminal]

Por fim, um último desafio apontado pelos entrevistados em relação à implementação do sistema Prüm tem que ver com o equilíbrio entre o princípio de disponibilidade de informação (McCartney, 2014) e a salvaguarda da soberania nacional em matéria de lei criminal (Hufnagel, 2012; Zaiotti, 2007). Neste sentido, é referido que medidas demasiado restritivas em relação à informação partilhada no sistema Prüm podem conduzir ao aumento de obstáculos no segundo passo (Santos et al., 2013; Machado & Silva, 2010; Prainsack, 2010). Dito isto, ambos os extratos apresentados encetam uma narrativa que realça que o excesso de medidas protetoras da privacidade dos cidadãos se encontra relacionada com a dificuldade demonstrada pelos Estados em abdicar de certos aspetos da sua soberania nacional.

“Respeito pela soberania e reciprocidade. (...) Eu julgo que não se pode é frustrar a celeridade da capacidade de pesquisa nas bases com questões muito limitativas na partilha da informação no chamado *second step*. Mas por outro lado, também não se pode desrespeitar os tais princípios da soberania. E, portanto, também temos que ter aqui um balanço e um equilíbrio entre uma coisa e outra.” [N19-órgão de investigação criminal]

“Os estados têm dificuldade a abdicar de parte da sua soberania, e uma delas é a componente da segurança. (...) De momento a cooperação tem funcionado razoavelmente bem, poderia obviamente trabalhar otimamente se os estados abdicassem um bocado da sua soberania, e não tivessem tanto problema com que os seus poderes fossem afetados.” [N28-órgão de investigação criminal]

Em linha com o enunciado pelas categorias profissionais já analisadas em relação às motivações da criação de uma tecnologia de controlo com as características do sistema de Prüm, os profissionais da categoria de Professor(a)/investigador(a) remetem as suas reflexões para a elevada mobilidade dos cidadãos europeus. Da leitura do extrato compreende-se que o/a entrevistado/a, formado/a em biologia e campos relacionados, considera que a circulação livre de pessoas no espaço da União Europeia foi responsável pela (re)configuração das fronteiras nacionais que teve como objetivo a promoção de uma melhor integração continental (Zaiotti, 2007). Sendo que o regime Schengen pode ser apontado como uma das plataformas que proporcionou o desenvolvimento de sistemas de controlo e gestão de fronteiras no seio da União Europeia (*idem*). Deste modo, como se observa no extrato, a procura por novas medidas de segurança dos Estados-Membros e a simplificação da partilha de informação a esse respeito (Hert, 2005; Liu 2013, p. 103) culminaram na criação do sistema Prüm.

“Nós estamos num mundo global. É completamente diferente a situação de hoje e de há 10 anos atrás, um indivíduo está aqui hoje, amanhã está noutro sítio (...). Portanto, obviamente que tem que haver partilha de dados. As fronteiras não são estanques, não há nada disso.” [N05-Professor(a)/investigador(a)]

O sistema Prüm encontrou na estrutura de dois passos a solução para a proteção das informações pessoais que constam nas bases de dados forenses (Prainsack & Toom, 2010). No entanto, no plano local, a implementação das bases de dados para fins de investigação criminal tem gerado debate sobre os desafios éticos, sociais e políticos em relação à salvaguarda da privacidade e da proteção de dados (Machado et al., 2012; McCartney, 2014a; McCartney et al., 2011; Toom, 2018). Neste sentido, um/a dos participantes, formado/a em direito, realça que, em termos de proteção de dados, Portugal é um dos países mais seguros do sistema Prüm. Primeiro, devido ao caráter restritivo da lei portuguesa quanto ao tipo de informações pessoais inseridas na base de dados forense (Santos et al., 2013). Segundo, porque a infraestrutura informática nacional possui várias medidas que visam proteger os dados a serem inseridos na plataforma.

“Portugal, o exemplo de Portugal, é que propôs algumas alterações no Prüm. Quanto à separação das informações. O sistema português é o mais seguro de todos os países.” [N09-Professor(a)/investigador(a)]

Os entrevistados desta categoria, principalmente, os que têm formação em direito, referem que é necessário assegurar que a partilha de dados realizada através de Prüm não é um atentado à dignidade humana e aos direitos civis dos cidadãos. Sendo que se mostram particularmente preocupados com a instrumentalização política do medo do terrorismo para justificar a aplicação de medidas que não respeitem e suprimam as liberdades civis. Pois, o aproveitamento político que tem sido feito dos atentados terroristas tem sido responsável pelo pânico moral desenvolvido pelos cidadãos em torno do tema (Cohen, 2002; Garland, 2008; Goode & Ben-Yehuda, 1994). Neste sentido, como o extrato demonstra, defende-se que devem existir mecanismos de supervisão das atividades de cooperação mais eficazes, com o objetivo de evitar comportamentos abusivos por parte das autoridades policiais que possam suprimir desproporcionalmente os direitos dos indivíduos (Amankwaa, 2018; McCartney, 2014a).

“É que sob o objetivo estratégico de combate ao terrorismo tem-se cometido muitos atropelos aos direitos fundamentais, à liberdade das pessoas. (...) Acho que a União Europeia até devia ter aqui mecanismos de fiscalização mais fortes (...). Só

pode ser por aí, quer dizer, de facto percebe-se que é importante partilhar informação nesta área, mas é preciso de facto cuidado com essa partilha de informação.” [N26-Professor(a)/ investigador(a)]

Privacidade e proteção de dados na base de dados forense

No que concerne às medidas adotadas para a proteção da privacidade e proteção de dados em contexto forense nacional os geneticistas forenses não identificaram nenhum ponto controverso (Latour, 1987b) constatando-se que a discussão em torno destas questões é permeada de certezas quanto à segurança dos dados. Nesta linha, os entrevistados, como se observa no extrato apresentado, elencam que a segurança informática, através da encriptação, é uma das formas de garantir que nenhuma informação pessoal seja do conhecimento de pessoas sem a devida autorização. Posto isto, a circulação de dados pessoais e perfis de DNA por meio das tecnologias de informação veio conferir um carácter neutro e objetivo aos mesmos que relega para o plano invisível uma reflexão mais aprofundada sobre os dilemas éticos da partilha de dados (Derksen, 2010, p. 224; Machado & Granja, 2018, p. 254). Sendo que garantir a privacidade e a proteção de dados dos cidadãos num contexto forense não deve realizar-se apenas pela segurança informática na partilha das informações, mas também pelo tipo de dados que lhes são recolhidos, pela correção de incongruências, pela garantia de não ocorrerem falsos positivos, entre outros.

“Os ficheiros que são enviados do laboratório para o ficheiro intermédio, do ficheiro intermédio para as equipas são sempre ficheiros encriptados. Mesmo que alguém abra ou recebesse um email erradamente nunca conseguiria, não haveria hipótese. Depois, entretanto, a equipa dos perfis recebe esses ficheiros, e tem que desencriptar obviamente (...).” [N07-geneticista forense]

A segunda medida que, no entender dos geneticistas forenses, veio garantir a privacidade genética das pessoas que constam na base de dados tem que ver com a natureza das análises à região não-codificante do DNA que não permitem o acesso a informação sensível relacionada com dados de saúde e características físicas (Benecke, 2002; McCartney, 2014b). A simplificação da proteção de dados através do *black boxing* da privacidade (Machado & Granja, 2018) demonstram que o questionamento relacionado

com os direitos humanos e os riscos éticos das bases e dados forenses foram encarados, pela maioria dos participantes, enquanto incertezas resolvidas (Latour, 1987b). A sua posição encontra-se em linha com a carência generalizada de discussões mais amplas quanto aos significados das premissas acerca da proteção da privacidade supramencionadas (Jasanoff, 2011; Nuffield Council on Bioethics, 2007). Em particular, a natureza sensível dos dados genéticos, o uso perverso dos dados pessoais e a ocorrência de incriminações (através de vestígios biológicos) e falsos positivos (Gamero et al., 2008; Liu, 2013, p. 13; Wallace et al., 2014, p. 58). Esta narrativa pode encontrar-se no excerto abaixo apresentado:

“Não há absolutamente risco nenhum. Porque as partes dos genes que são usados hoje, para identificação criminal ou civil (...), são anónimas no nosso genoma, não codificam nada (...). Não têm interesse em termos de saúde, psiquiatria, etc. Portanto, não apresentam problemas.” [N01-geneticista forense]

Numa posição substancialmente residual observa-se um posicionamento mais crítico em relação à necessidade de se garantir a privacidade e proteção de dados pessoais dos cidadãos num contexto forense. Neste sentido, um/a dos/as geneticistas forenses refere que a resolução de um crime e a restituição da justiça às vítimas deve estar acima de qualquer outro direito do indivíduo que perpetuou o crime. Observa-se, no extrato selecionado, uma narrativa que coloca sobre o bom-cidadão a obrigação moral de contribuir para o bem-comum e a responsabilidade social (Machado & Silva, 2008b, p. 161; Marx, 2006, 2008; Rose, 2008) ao permitir a supressão do seu direito à privacidade. Sendo que a defesa da premissa de que ‘quem não deve, não teme’ (N16) pode conduzir à erosão de direitos como a presunção de inocência (Kreissl et al., 2015; Marx, 2006, p. 5) e a dúvida razoável (Lyon, 2014, p. 10) numa lógica que entende o direito à privacidade e a criminalidade como sinónimos (Crossman, 2008, p. 116).

“Eu entendo que se deve defender a privacidade das pessoas e alguns direitos das pessoas. Mas não consigo conceber quando estamos a falar de crimes. Quando estamos a falar de crimes há outros direitos. O direito à vida da pessoa que morreu

acho que é maior do que o outro. E sempre disse, quem não deve, não teme. Agora, quem deve, deve ter algum receio, isso é.” [N16-geneticista forense]

Este tipo de narrativa diverge da anterior relativamente à tónica que é colocada na privacidade e na proteção de dados na investigação criminal. De modo geral, no primeiro grupo, as questões de privacidade são resolvidas pelo facto de que cientificamente o perfil de DNA forense não permite a intrusão do Estado e da polícia nas informações sensíveis dos cidadãos. De certo modo, estes entrevistados cingem a discussão ao carácter estritamente técnico sem que se foquem necessariamente nas implicações que esta situação pode ter para o indivíduo. No segundo grupo, ainda que menos expressivo, diminui-se a questão técnica e verifica-se um aprofundamento da questão social, onde a reflexão incide maioritariamente na figura da vítima e do seu direito à restituição da justiça. Porém, apesar do reconhecimento do direito da vítima, esta narrativa não incorpora os prejuízos que uma pessoa pode sofrer na sua vida devido a uma suspeita errada com base no perfil de DNA. Posição que cria uma linha muito ténue entre aquilo que é a garantia da privacidade e a culpa pela prática de um crime.

As narrativas dos entrevistados de entidades de supervisão e regulação demonstram que esta categoria profissional também entende que ao nível nacional existem medidas eficientes para a proteção de dados e da privacidade genética no âmbito forense. Relembre-se, que o reduzido número de proporção populacional inserida na base de dados nacional associado às opções tomadas pelo legislador levaram à inclusão de Portugal num conjunto de países que são denominados de restritivos (Santos et al., 2013). De modo genérico, países com estas características possuem critérios de inserção de perfis na base de dados que não permitem a inclusão de pessoas inocentes e/ou não condenadas em processo (*idem*, p. 8). Relativamente aos critérios de exclusão dos perfis de DNA também se verifica uma tendência para a retenção temporalmente limitada (*idem*). Posto isto, considera-se que países com características restritivas são mais protetores dos direitos de privacidade e proteção de dados plasmados na Declaração Universal dos Direitos Humanos através de critérios restritos na gestão da base de dados. Neste sentido, a maioria dos participantes, com formação em direito, realçaram que na Lei n.º 5/2008, responsável pela criação da base de dados forense, foram explícitas as preocupações com os direitos humanos fundamentais, como se pode observar no extrato seguinte:

“Sendo esta uma área onde se colocam à partida questões sensíveis ligadas à proteção dos dados pessoais daqueles cujos perfis depois acabam por ficar na base de dados, acho que houve de facto uma preocupação grande desde o início, e a lei de 2008 reflete isso, com o assegurar destes direitos fundamentais.” [N03-entidade de supervisão/regulação]

No espírito da proteção de direitos humanos fundamentais, um dos entrevistados referiu que Portugal é um país que tem como tradição jurídica a salvaguarda dos direitos e liberdades civis dos seus cidadãos, ressalvando que os dados enviados para os restantes países são limitados. No extrato, a preocupação em relação à privacidade dos dados genéticos foi enquadrada no momento em que os dados fluem do contexto nacional para o transnacional. Portanto, o funcionamento e o enquadramento legal português da base de dados não são encarados como um fator que potencia a supressão desproporcional destes direitos. Esta questão coloca-se quando os dados saem do país, ou seja, no tipo de medidas protetoras da privacidade que os outros países dispõem. De modo implícito, este tipo de narrativa avança com uma transferência de responsabilidade quanto à proteção dos dados pessoais partilhados. Através das palavras do/a entrevistado/a constata-se, a par da literatura, que a supervisão internacional dos fluxos de informação realizados no âmbito do sistema Prüm pode ser insuficiente (McCartney, 2014a) para conseguir garantir a idoneidade e transparência da utilização dos dados partilhados.

“Porque nós somos o paraíso dos direitos. (...) E por acaso até somos. Portanto nós não fazemos mal nem provocamos mal. Agora o que é que eles podem fazer de mal com os dados que nós damos? Agora nós também damos muito pouca coisa, não é? (...) São os dados de identificação.” [N11-entidade de supervisão/regulação]

A fiscalização obrigatória das atividades da base de dados forense plasmada tanto na Lei n.º 5/2008, como na Lei n.º 90/2017 foi um dos pontos mais mencionado pelos entrevistados como protetor da privacidade de quem consta na mesma. Em Portugal, o órgão responsável pela fiscalização é, como já mencionado, o Conselho de Fiscalização da

Base de Dados de perfis de ADN, sendo que, sempre que necessário deve recorrer à Comissão Nacional de Proteção de Dados para o esclarecimento de eventuais situações. Na mesma linha, no extrato que se segue, a fiscalização operada ao nível interno é novamente encarada como eficiente, mas implicitamente é perceptível que o/a entrevistado/a considera que é fundamental que os mecanismos de controlo externo sejam eficazes.

“Eu acho que sim, que a legislação acompanha e protege. Aliás há uma série de comissões que tratam, de conselhos que tratam de ser o garante desse cumprimento.” [N25-entidade de supervisão/regulação]

Constatou-se que os entrevistados desta categoria profissional consideram que a legislação é uma das formas mais eficazes de garantir a privacidade e proteção de dados dos cidadãos cujos perfis de DNA se encontram na base de dados forense. Na perspetiva dos participantes a supervisão realizada em contexto nacional não apresenta problemas significativos, pelo que se verificou um consenso geral em relação à adequabilidade das medidas de proteção de dados e da privacidade no contexto forense, em Portugal.

A criação da base de dados forense nacional foi acompanhada do debate acerca das preocupações com a manutenção e utilização da mesma. Nesta linha, as tecnologias biométricas ao serviço do aparelho Estatal de vigilância apresentam-se como potenciais supressoras das liberdades e direitos civis dos cidadãos (Clarke, 2001). As vulnerabilidades mais prementes deste tipo de biotecnologia de vigilância e controlo do corpo dos cidadãos (Aas, 2006, p. 144) têm que ver com as salvaguardas adotadas em relação à proteção de dados e privacidade dos indivíduos com dados genéticos inseridos nestes sistemas (Mostert et al, 2017; Wayman & Nuger, 2005). No extrato apresentado, o/a entrevistado/a, a desempenhar funções num órgão de investigação criminal, refere que a base de dados forense portuguesa se encontra informaticamente muito bem protegida do acesso externo. Segundo a sua perspetiva a gestão informática da base de dados cumpre os princípios de *privacy by design* (Jones & Raab, 2015; Schaar, 2010) para a construção de sistemas de informação. Uma das salvaguardas informáticas mais utilizada é, respetivamente, a criação de registos individuais que mapeiam e registam todos os acessos à base de dados forense.

“Porque as bases de dados policiais são estanques, ninguém pode entrar (...). Os próprios administradores informáticos dizem que o sistema é extremamente forte e a nível de segurança tem um patamar de segurança quase excelente. (...) Mais, a utilização de dados por parte da polícia é facilmente verificável, porque cada vez que eu entro com a minha *password*, fica latente no sistema (...)” [N28-órgão de investigação criminal]

De modo semelhante aos geneticistas forenses, nesta categoria profissional, a reflexão a respeito da privacidade e proteção de dados cingiu-se ao papel central das tecnologias de informação para a garantia da proteção das infraestruturas digitais e físicas da base de dados. Assumindo-se, deste modo, que garantir a segurança da base de dados contra ataques ou acessos não autorizados é a única dimensão da proteção da privacidade dos indivíduos que constam inseridos na mesma.

As perspetivas da categoria profissional Professor(a)/ investigador(a) a respeito da privacidade e proteção de dados em contexto forense encontra-se em linha com uma narrativa otimista demonstrada pelos entrevistados das outras categorias profissionais. No extrato apresentado, um dos entrevistados que teceu comentários a este respeito considerou que o equilíbrio entre os direitos individuais e a segurança coletiva é adequado em Portugal. Esta posição vem contrariar a preocupação generalizada acerca da reflexão sobre as ameaças à supressão de direitos fundamentais com o recurso a bases de dados forenses em investigação criminal (Heinemann et al., 2012; Toom et al., 2016; Wayman & Nuger, 2005). No entanto, o/a entrevistado/a admite que o equilíbrio entre o bem-comum e a proteção da segurança pública pode configurar-se complexo se se continuarem a viver episódios de terrorismo na União Europeia. Pois, nas suas palavras, quando existem acontecimentos frequentes que levam as populações a sentirem-se inseguras é possível que se verifique o reforço de medidas que visam a segurança em detrimento da privacidade e proteção de dados dos cidadãos. O terrorismo enquanto fator do (des)equilíbrio enunciado pelo entrevistado encontra-se a par com a literatura que chama a atenção para o facto de que este tem sido a justificação para a adoção de medidas mais restritivas das liberdades civis (Bigo, 2008, p. 92; Hert, 2005).

“Do ponto de vista legal acredito que a legislação de facto seja sempre uma legislação de equilíbrio. Porque há realmente valores de referência, de estado de direito. Agora eu acho que isso também vai depender muito da própria evolução do combate ao terrorismo. Quer dizer, se nós passarmos a viver sob um medo constante de ações terroristas é natural que haja uma maior tendência para ser menos exigente do ponto de vista da segurança e dos direitos.” [N26-Professor(a)/ investigador(a)]

Colocando em retrospectiva os pontos elencados nesta secção constata-se que, mesmo com diferentes níveis de reflexão ética sobre utilização de uma base de dados forense, todas as categorias profissionais entendem que em Portugal a proteção de dados é realizada de modo a dar primazia à privacidade. Sendo que se identificam, genericamente, duas dimensões justificativas para a neutralização dos riscos decorrentes desta utilização ao nível nacional. A primeira é a dimensão tecnológica que remete para a criação de salvaguardas ao nível técnico para a proteção da base de dados contra o acesso não autorizado das informações pessoais que nela constam. A segunda dimensão é a legal, sendo que as narrativas analisadas revelam uma confiança generalizada na adequabilidade do enquadramento legal da base de dados que favorece, pelos seus critérios de inserção de perfis de DNA, o equilíbrio entre o bem-comum e a segurança coletiva.

Interoperabilidade entre bases de dados forenses e biobancos

A criação das infraestruturas das bases de dados forenses de perfis de DNA e dos biobancos para fins de investigação médica usufruiu do desenvolvimento tecnológico generalizado. Os três fatores preponderantes para o seu sucesso e consecutiva expansão foram, nomeadamente, a maior capacidade de armazenamento de dados informáticos, o aumento substancial do fluxo de informações entre sistemas e, por fim, a simplificação dos processos envolvidos no cruzamento de dados através da standardização tecnológica (Goos et al, 2015; Mostert et al, 2017; Nissenbaum, 2010).

As perspetivas dos geneticistas forenses e *stakeholders* em relação à interoperabilidade entre bases de dados forenses e biobancos serão novamente analisadas tendo como base a categorização já enunciada neste estudo (página 120). Relembrando, a categorização decompõe-se em quatro categorias analíticas, nomeadamente, a ‘negação

técnico-legal’, a ‘interoperabilidade pela excecionalidade’, a ‘negação pela finalidade’ e, por fim, a ‘interoperabilidade pela expansão’.

Na categoria dos geneticistas forenses, apenas um/a dos/as entrevistados/as considera que a interoperabilidade entre bases de dados forenses e biobancos não é uma prática aceitável, como se pode observar no excerto. O argumento de que se serve para justificar a sua perspetiva está associado aos diferentes enquadramentos éticos que permeiam as atividades das duas utilizações dos dados genéticos. Portanto, o seu posicionamento demonstra que considera a utilização de biobancos para o auxílio na investigação criminal um desvirtuamento do princípio da finalidade da utilização dos dados (Brown, 2009; European Data Protection Supervisor, 2006; Gamero et al., 2008; Gonçalves & Jesus, 2012, 2013; Harbo, 2010; Hert, 2005; Hoven, 2001; IRISS, 2012). De modo genérico, a finalidade das bases de dados forenses está relacionada aos princípios de segurança e da identificação suspeitos de crimes, ao passo que os biobancos remetem para a salvaguarda da saúde pública (Gaskell et al., 2013; Machado & Silva, 2015a, p. 820).

“Não deve ser utilizado porque o consentimento dado pelos cidadãos para se criar um banco de fins genéticos clínicos, não inclui investigação criminal. E tal como o contrário também é verdadeiro. Entendo também que amostras que estejam na área forense não deverão ser utilizadas para fins clínicos. Portanto entendo que deve haver uma separação entre uma área e a outra área.” [N02-geneticista forense]

No entanto, verificou-se, através das entrevistas, que os restantes geneticistas forenses não descartam a hipótese de existir uma interconexão entre bases de dados forenses e biobancos. Esta situação vem confirmar a tendência para a intensificação da vigilância através da identificação do corpo humano (Aas, 2006, p. 144). Sendo que a digitalização e o desenvolvimento tecnológico supramencionados têm permitido a criação de redes de vigilância tecnológica em massa cada vez mais interoperáveis e interconectadas em torno das sociedades contemporâneas (Gilliom, 2007, p. 114). Contudo, os participantes denotam que a interoperabilidade nestes termos necessitaria de um enquadramento regulatório forte que fosse responsável pela determinação dos critérios legais para o acesso às plataformas. Nesses critérios, de modo protocolar e estandardizado, deveriam estar

plasmadas as situações em que o acesso seria permitido, quem teria acesso aos dados médicos ou forenses, bem como os mecanismos de supervisão para este tipo de práticas.

“De facto tenho que admitir que esse cruzamento poderia ser feito. Agora tem que haver mecanismos de controlo sobre como é que isso seria feito, sobre que situações, sobre que contextos e que regras e quem o poderia fazer. Não pode ser é uma selva. (...) Isso é que não.” [N04-geneticista forense]

A grande maioria dos geneticistas forenses remete a interpretação da questão sobre a interoperabilidade entre bases de dados numa lógica assente no acesso forense a bases de dados médicas, sendo que a situação inversa foi menos referenciada. Neste sentido, no extrato seguinte, o/a entrevistado/a assume uma postura cautelosa em relação à legitimação deste tipo de práticas no âmbito da investigação criminal. Na sua perspetiva, o acesso forense a um biobanco poderia ser do interesse público para efeitos de resolução de um crime, contudo a permissão para aceder a dados médicos deveria ser realizada numa ótica de caso-a-caso. Deste modo, as narrativas destes entrevistados revelam a tensão entre os ideais que movem a criação de ambos os tipos de bases de dados devido aos mecanismos sociais responsáveis pela sua concretização. Por um lado, a restituição da ordem pública e da justiça. Por outro lado, a salvaguarda da saúde pública. Neste sentido, a discussão ética em torno do acesso forense a biobancos não se cinge à disponibilidade dos dados, pois o fluxo de informações sensíveis é condicionado pelas expectativas dos cidadãos em relação a determinada prática (Hoeyer et al., 2016). Sendo que as relações de confiança entre o Estado e os seus cidadãos também pode ser um constrangimento a este tipo de atividades devido a receios relacionados com práticas policiais desadequadas, fugas negligentes de informação, entre outros.

“Eu acho que poderia ser interessante e poderia ajudar a resolver alguns casos, mas acho que isso teria de ser visto base a base porque depende do tipo de informação que contém. E do tipo de resposta que poderia dar. (...) Acho que é um bocado caso a caso.” [N23-geneticista forense]

O extrato seguinte é igualmente representativo dos receios dos geneticistas forenses quanto a uma utilização forense dos biobancos. Neste caso em particular, o/a participante reconhece a utilidade que a legitimação do acesso a biobancos pode trazer no contexto da investigação criminal, nomeadamente, levar à justiça pessoas culpadas de crimes. No entanto, mostra-se preocupado/a com situações em que o acesso policial pode levar à suspeição de um indivíduo que não contribuiu em nada para o crime a ser investigado. Pois, este tipo de situação colocaria em causa o direito à proteção de dados e à privacidade dos cidadãos pois ‘estar no sítio errado à hora errada’ (N20) poderia conduzir ao escrutínio da sua vida privada de modo desproporcional e irremediável.

“Se eu estivesse a fazer investigação criminal, gostaria de ter acesso a essa informação, porque o bem da justiça é superior ao bem individual do criminoso. (...) Colocando-me na parte de um suspeito inocente, é um bocado mau. Se fosse na parte de um suspeito culpado, pronto olha, azar, isso é contribuir para a justiça. (...) Porque não é que eu tenha algum problema em ser vigiada ou controlada, mas a dada altura pode acontecer uma situação da pessoa estar no sítio errado à hora errada, ser apanhada no meio de uma situação para a qual nada contribuiu, mas ser apanhada por causa dos seus dados estarem nestas bases de dados todas.” [N20-geneticista forense]

Tendo por base a análise dos extratos acima apresentados, as narrativas dos geneticistas forenses enquadram-se, maioritariamente, no que é denominado no presente estudo como ‘interoperabilidade pela excecionalidade’. Neste sentido, o acesso forense a biobancos é compreendido como tendo um potencial valor investigativo. No entanto, este só deverá ocorrer se se estabelecerem previamente um conjunto de condições cujo objetivo seja o de evitar que esta prática lese injustificadamente os direitos civis das pessoas envolvidas.

Relativamente à categoria profissional entidade de supervisão/regulação, a narrativa mais dominante encontra-se em desacordo com a prática da interoperabilidade entre bases de dados forenses e biobancos. Em particular, no extrato, encontra-se realçado o carácter voluntário dos biobancos (Machado & Silva, 2015a), bem como o perigo da confusão entre as finalidades de bases de dados com objetivos distintos, como já referido. Posto isto, o

desvirtuamento da finalidade da salvaguarda da saúde pública no acesso forense a um biobanco poderia, nas palavras do/a entrevistado/a, colocar *a priori* todos os cidadãos voluntários numa situação de desconfiança e suspeição. Sendo que, em última análise, a abertura deste precedente poderia colocar em causa a solidariedade (Chadwick & Berg, 2001; Prainsack & Buyx, 2016) característica dos biobancos e a confiança que os dadores depositam nas instituições, sejam elas médicas ou policiais. Esta reflexão encontra-se em linha com a literatura sobre os princípios pelos quais um biobanco deve ser regido, respetivamente, a voluntariedade, o altruísmo e a solidariedade do dador (Bexellius et al., 2007; Forsberg et al., 2009; Gamero et al., 2008; Machado & Silva, 2015a; Wilson-Kovacs et al., 2012).

“Porque abre a porta a uma confusão de finalidades e de objetivos, até de alguma legitimidade de utilização (...) porque desde logo introduziria um fator de desconfiança que penso que levaria ao fracasso de um [bio]banco, assente no voluntariado. E ser imposto acho que isso é perfeitamente inaceitável.” [N03-entidade de supervisão/regulação]

Sumariamente, os/as participantes que desempenham funções em entidades de supervisão/regulação balizam o seu posicionamento na categoria ‘negação pela finalidade’. Sendo que a reflexão ética e os dilemas referidos no decorrer das entrevistas decorrem, em grande medida, das características deste grupo. Pois, ao nível profissional e enquanto membros de entidades de supervisão realizam atividades fortemente guiadas pelo questionamento ético.

Na categoria órgão de investigação criminal a posição dos entrevistados foi antagónica. Por um lado, um/a dos/as entrevistados/as, investigador/a criminal com formação em direito, defendeu a existência da interoperabilidade entre as duas infraestruturas. Por outro lado, outro/a entrevistado/a, a desempenhar um cargo administrativo e com formação em direito, revelou-se completamente contra o acesso forense a biobancos. A discrepância destas narrativas, considerando que possuem a mesma formação académica e pertencem à mesma categoria profissional, pode estar relacionada com o tipo de funções desempenhadas no seio do órgão de investigação criminal. Ao passo que o/a primeiro/a entrevistado/a desempenha funções mais associadas à investigação

criminal no plano prático. O/a segundo/a participante tem a seu encargo funções administrativas que não estão diretamente associados com o trabalho no terreno. Posto isto, observa-se, no extrato, de modo latente uma racionalidade objetiva que contribui para a instrumentalização dos biobancos em prol do cumprimento dos objetivos da garantia da segurança e da restituição da ordem pública. Em particular, são mitigados quaisquer riscos de desvirtuamento da utilização dos dados partindo do princípio que os órgãos de investigação são revestidos de total transparência.

“Para investigação criminal sempre fantástico. Temos um vestígio biológico de determinado indivíduo que está propenso a uma determinada doença, que pode permitir até facilmente o identificar (...). Estas bases de dados biomédicas devem estar perfeitamente acessíveis à polícia, a polícia não está preocupada se tu tens (...) uma doença degenerativa, a polícia não pretende isso, pretende unicamente a segurança.” [N28-órgão de investigação criminal]

O segundo extrato é representativo de uma posição completamente oposta, como já referido, onde é enfatizada, mais uma vez, que as bases de dados forenses e os biobancos possuem finalidades diferentes de acordo com as suas funções. Nesta perspetiva, argumenta-se que é mais relevante possuir uma base de dados forense de dimensão considerável com perfis de DNA de condenados e/ou arguidos do que prosseguir com o acesso a um biobanco que contém informação sobre pessoas à partida inocentes. O argumento apresentado vem contrariar parcialmente a tese de que para a maximização da eficácia da vigilância as tecnologias necessitam obrigatoriamente de se tornar mais intrusivas para os cidadãos em geral (Haggerty & Ericson, 2007, p. 17). Deste modo, os esforços para melhorar a resposta da investigação criminal devem ser canalizados para o aperfeiçoamento da base de dados forense ao nível nacional. Por oposição a um avanço que visa a intrusão de uma ‘realidade distinta’ como o campo da investigação médica.

“Penso que não deve haver. Nós temos em Portugal um dos maiores biobancos (...) temos uma recolha do teste do pezinho para fins epidemiológicos. (...) Portanto o que eu gostaria é ter uma grande base de dados de perfis de condenados ou de arguidos, onde possa fazer uma pesquisa e tenha resultados. A outra situação

para efeitos epidemiológicos é (...) no domínio da saúde. (...) Não vejo como possa ser possível ou como possa ser desejável cruzar realidades distintas.” [N19-órgão de investigação criminal]

Por fim, a posição dos entrevistados da categoria professor(a)/investigador(a) situou-se entre o repúdio à interoperabilidade e o acesso em circunstâncias excecionais a biobancos no âmbito da investigação criminal. No extrato apresentado, o entrevistado defendeu que este tipo de prática seria desproporcional e violaria o princípio da finalidade de recolha, uma vez que as autoridades estariam a recorrer a amostras recolhidas sob pretextos médicos para a resolução de crimes. Neste sentido, do ponto de vista ético, a solidariedade e o altruísmo implícitos na doação de tecidos biológicos para o auxílio na investigação médica devem ser os valores com maior peso na decisão (Bexellius et al., 2007; Forsberg et al., 2009; Gamero et al., 2008; Machado & Silva, 2015a; Wilson-Kovacs et al., 2012). Pois, segundo este/a, a verificar-se esta prática, as instituições estariam a comprometer a generosidade dos cidadãos que constam nos biobancos.

“Ainda por cima seria injusto. Quer dizer, também desse ponto de vista, as pessoas cedem, se cedem material biológico para efeitos de investigação, ainda que possam ser criminosos em outro contexto, que essa generosidade acabe por se virar contra eles. Acho que há ali problemas também do ponto de vista ético sensíveis e que me levarão a não encontrar nenhuma justificação para cruzar este tipo de informação.” [N17-Professor(a)/investigador(a)]

O extrato abaixo apresentado é representativo de uma perspetiva que favorece o acesso forense condicionado aos biobancos. Do ponto de vista ético, a opção por uma regulação que cinja o acesso aos biobancos de acordo com a gravidade do crime pode apresentar-se como uma das ferramentas para favorecer a prestação de contas aos cidadãos (Jasanoff, 2005). Dito isto, observa-se que a restrição da prática a crimes particularmente graves tem como objetivo a garantia da proporcionalidade na intrusão da privacidade genética dos cidadãos, bem como a mitigação dos riscos sociais subjacentes ao acesso a informações médicas sensíveis (Granja & Machado, 2019, p. 14). A proposta de uma regulação condicional no que toca ao acesso forense a dados médicos delimita os

“limits of privacy, confidentiality, equality, and (the presumption of) innocence within the bounds of a particular criminal case” (*idem*).

“É bastante problemático. Eu diria que é necessário fazer aqui uma ponderação, e eventualmente limitar a investigação criminal a determinados crimes particularmente graves, e não permitir um acesso completo. Eu diria que só em circunstâncias muito excepcionais é que eventualmente poderemos pensar numa interoperabilidade nesses termos. Mas não a rejeito em absoluto (...).” [N27-Professor(a)/investigador(a)]

Relativamente à última categoria profissional, as narrativas dominantes podem ser enquadradas nas categorias de ‘negação pela finalidade’ e de ‘interoperabilidade pela excepcionalidade’. Mais uma vez, assiste-se a uma reflexão que tem por base as distintas finalidades das bases de dados forenses e dos biobancos e o modo como o seu cruzamento pode ferir princípios como o de altruísmo associado à doação de material genético.

Direito ao apagamento dos dados - Artigo 17.º do Regulamento (EU) 2016/679

O direito ao apagamento dos dados também conhecido como direito a ser esquecido encontra-se plasmado no novo Regulamento Geral de Proteção de Dados (Regulamento (EU) 2016/679) no artigo 17.º. Este direito veio complementar os direitos de acesso e retificação dos dados que já constavam em documentos anteriores. Portanto, pelo artigo 17.º, qualquer cidadão da União Europeia possui o direito de “obter do responsável pelo tratamento, o apagamento dos seus dados pessoais, sem demora injustificada” nas seguintes situações: 1) quando os dados pessoais recolhidos deixam de ser necessários para a finalidade que motivou a recolha ou o tratamento dos mesmos (alínea a do n.º 1 do artigo 17.º); 2) quando é retirado o consentimento por parte do titular dos dados para o tratamento dos mesmos (alínea b do n.º 1 do artigo 17.º); 3) quando os dados foram tratados ilicitamente pelo responsável pelo tratamento (alínea d do n.º 1 do artigo 17.º). Contudo, estão previstas, no Regulamento, exceções ao apagamento dos dados quando é solicitado pelo titular (n.º 3 do artigo 17.º). Posto isto, o direito ao apagamento dos dados pode ser suprimido caso estes sejam necessários para o exercício da liberdade de expressão e de informação; para o cumprimento de uma obrigação legal relacionada com o exercício

de funções de interesse público ou da autoridade pública; por motivos de interesse público no domínio da saúde pública; para efeitos de declaração, exercício ou defesa de um direito num processo judicial, entre outros.

Uma parcela dos entrevistados pertencentes à categoria entidades de supervisão/regulação refere que apesar de o direito ao esquecimento ser pertinente e fundamental para os indivíduos, é necessário ter presente que existem situações em que deve ser suprimido em prol do bem comum. As perspetivas destes/as participantes quanto à limitação do direito ao esquecimento em determinados contextos acompanham a intenção expressa pelo legislador quando incluiu no Regulamento uma exceção à eliminação de informações no âmbito de processos judiciais. No excerto selecionado, é apresentada uma narrativa que se compactua com a tradição humanista do sistema judicial português (Machado et al., 2012; Moniz, 2009). Pois, defende explicitamente a reintegração social dos indivíduos que mudam de vida e não voltam a cometer atos ilícitos. No entanto, é salvaguardado que este não é um direito universal e aplicável a todos os contextos históricos e espaciais. No seu entender os crimes hediondos cometidos contra a humanidade não devem usufruir deste tipo de mecanismos legais, como por exemplo, os crimes de guerra.

“A pessoa pode ser lembrada para sempre por coisas completamente frívolas, mas que podem destruir. Efetivamente é inaceitável que uma pessoa fique marcada por períodos imaturos da sua vida, é insuportável. E o direito a ser esquecido é um direito real, (...) a pessoa resolveu mudar de vida legitimamente, e aquele período está completamente liquidado e esquecido. Agora isso não é válido para tudo e, portanto, é um direito que também ele próprio tem limitações. É importante que esteja compaginado com a tal imprescritibilidade dos crimes contra a humanidade.”
[N11-entidade de supervisão/regulação]

O tópico do direito que os cidadãos possuem ao apagamento dos seus dados volta a ser um ponto de discórdia entre os entrevistados a desempenhar funções nos órgãos de investigação criminal, possivelmente devido aos fatores, já mencionados, relacionados com a natureza das atividades que desempenham. Neste sentido, no primeiro extrato, o/a entrevistado/a enfatiza a mudança de paradigma da proteção de dados com o novo

Regulamento através da inculcação da temporalidade na retenção de dados pessoais. No seu entender, esta disposição legal usufrui da proporcionalidade entre os direitos humanos individuais de autonomia e privacidade e os direitos coletivos de segurança pública (Heinemann et al., 2012; Toom et al., 2016; Wayman & Nuger, 2005).

“De acordo com os princípios de proteção de dados europeus tem-se inculcado uma ideia de tempo, de temporário. (...) Eu julgo que as soluções têm sido equilibradas em termos legais. Não advogo também que coloquem o enfoque na questão exclusiva do direito individual porque acho que tem que haver um compromisso entre o direito individual e o direito coletivo, a sociedade também tem alguns direitos, e alguns passam por ter expectativas de segurança. Mas esses direitos de segurança não se podem impor eternamente a todos ou a uma minoria.” [N19-órgão de investigação criminal]

Numa perspetiva diametralmente oposta observa-se a narrativa do/a seguinte entrevistado/a. Em particular, considera que o direito ao apagamento dos dados não é adequado, sendo que existem, em contexto nacional, modos legalmente enquadrados que permitem aos cidadãos o acesso, a revisão e a retificação dos mesmos. Na sua perspetiva, a prática da eliminação de dados pessoais pode conduzir à não deteção de crimes, pois os indivíduos que praticaram os atos criminosos podem não ser identificados por estarem a usufruir de uma ‘não existência’ nas bases de dados. Observa-se, que o facto de o/a entrevistado/a ser um/a investigador/a criminal ativo/a no terreno contribui para uma retórica que visa a instrumentalização de todos os sistemas de informação disponíveis para a detenção e interceção de um crime ou de atividades criminosas.

O enfoque na restituição da justiça relega a dimensão ética do acesso a bases de dados fora do âmbito forense para um plano completamente invisível. Os pontos elencados no extrato reforçam a noção de que a dicotomia entre dados públicos e dados privados está a tornar-se cada vez mais obsoleta. Pois, o desenvolvimento dos sistemas tecnológicos tem vindo a permitir novas modalidades de obtenção de informação pessoal dos cidadãos que confluem com a expansão da vigilância e a recolha de dados em massa (Nissenbaum, 2010). Deste modo, os avanços no armazenamento, processamento e análise dos dados recolhidos

tem vindo a levantar questões sobre a necessidade de garantia e proteção da privacidade em público (Nissenbaum 1997, 1998).

“Eu acho que o cidadão não deve ter direito a ser esquecido, está no artigo 35.º da Constituição da República Portuguesa, nós temos acesso aos nossos dados, podemos junto do estado ou de entidades privadas, solicitar quais os dados que têm, e podemos mandar suprimir, retificar ou pronunciar sobre os nossos próprios dados. Então os criminosos, isto é uma maravilha: ‘deixe-me em paz, estamos esquecidos’. Isto não pode ser assim. Agora quem é que tem acesso a esses dados pessoais? Não podem ser entidades privadas, não pode ser qualquer entidade. A polícia que tenha acesso a estes dados, tudo bem. (...) está-se a borrifar para esse tipo de situações, não visa o lucro, a única ideia é sempre intercetar ou identificar determinada pessoa (...).” [N28-órgão de investigação criminal]

Os entrevistados da categoria professor(a)/investigador(a) demonstram perceções semelhantes às reveladas pelos participantes que se enquadram nas entidades de supervisão/regulação. No extrato seguinte, o/a entrevistado/a, com formação em direito, realça a importância de princípios legais como o da reinserção social como forma de sustentação da opção do legislador pelo direito ao esquecimento dos cidadãos. Neste seguimento, do ponto de vista ético e moral, o/a participante alerta para os danos psicológicos que a permanência de certas informações pessoais pode provocar ao indivíduo. Esta discussão em torno da disponibilidade dos dados em meio digital obrigou a que se movesse o referencial ético tradicional do plano físico para a integração de danos não palpáveis (Nissenbaum, 2010). O não apagamento de certos dados pode ter consequências graves relativamente ao seu impacto sobre a privacidade da informação, a discriminação baseada em dados (*data discrimination*), bem como os danos morais e psicológicos dos indivíduos cujos dados são públicos (Metcalf & Crawford, 2016). Em última instância pode ainda ficar em causa a capacidade de reinserção dos cidadãos que mudaram os seus hábitos de vida para modelos socialmente aceites.

“Uma pessoa que tenha um conjunto de dados na internet quando tem 20 e poucos anos. Quer dizer, vai passar toda a sua idade adulta com um conjunto de

informações, por mais que faça. Há pessoas que já fizeram outras coisas, muito mais relevantes do que aquela informação, mas porque fizeram qualquer coisa, eu googlei aquele nome e de facto o que aparece é logo aquilo à cabeça. Toda a outra informação é relegada lá para segundo plano (...). Eu acho que isto tem um impacto até na saúde mental das pessoas. É importante que os países e a União Europeia, trabalhem muito, para que seja um direito efetivo dos cidadãos.” [N26-Professor(a)/investigador(a)]

Decorrente da necessidade de encontrar mecanismos que permitam o cumprimento efetivo do direito ao apagamento dos dados, é também elencada a dificuldade de se conseguir proceder à eliminação completa dos mesmos. O desenvolvimento tecnológico ao nível dos sistemas de informação digitais tem potenciado várias mudanças estruturais em relação aos modos de acesso, processamento e troca de dados pessoais dos cidadãos (Dijck, 2014). Neste sentido, o contexto digital caracteriza-se pelo cruzamento de várias informações que podem ser descarregadas e copiadas; pela densidade das redes e pela possibilidade de criação de diversas cópias de segurança (Goos et al., 2015). Os avanços enunciados têm vindo a contribuir ativamente para o aumento das “capacities for storing, organizing, and retrieving great quantities of information” (Nissenbaum, 2010, p. 36). Portanto, devido à massificação do fluxo de informações em redes cada vez mais densas, os/as entrevistados/as, alertam para o facto de que podem verificar-se situações em que não seja possível garantir o usufruto em pleno do direito ao esquecimento (artigo 17.º do Regulamento (UE) 2016/679).

“Tem direito a um apagamento de dados, mas como é que consigo fazer isso num ambiente onde nós sabemos que os dados, verdadeiramente, nunca desaparecem. E, portanto, eu acho que é mais um direito em que não seja fácil, pelo menos, aceder a esses dados. Portanto, garantir que as pessoas tenham uma vida normal, sem serem prejudicadas por determinado tipo de informações, que até podem não ser factuais.” [N27-Professor(a)/investigador(a)]

Exceções ao direito do apagamento dos dados foram identificadas, por um/a dos/as entrevistados/as formado/a em direito, como estando associadas ao direito à liberdade de

imprensa e ao direito à informação. O argumento utilizado pelo/a entrevistado/a foi assente numa lógica que denunciou o (des)equilíbrio entre direitos comumente protegidos no seio da União Europeia que podem, em determinadas situações, ser concorrentes. Neste sentido, o artigo 17.º do Regulamento deve ser avaliado casuisticamente e em paridade com outros direitos em vigor que podem ser justificativos para a sua supressão. O/a participante defende que em situações concretas que envolvam o escrutínio público de certas pessoas influentes, como os decisores políticos, o que deve prevalecer é o direito à liberdade de imprensa de modo a permitir a denúncia de atividades ilícitas.

“Isto coloca-se essencialmente quando aqueles dados que querem ser apagados dizem respeito a questões que devem ser objeto de um debate público. O que é particularmente importante quando estão em causa, por exemplo, políticos. Isso coloca-se designadamente quando são dados que são obtidos até de forma ilícita, mas que são dados particularmente importantes para a comunidade, designadamente para efeitos de liberdade de imprensa. (...) E, portanto, nós temos aqui um choque entre por um lado o direito à privacidade, e por outro lado o direito à informação, e são 2 direitos protegidos, e nós temos de fazer na verdade uma análise casuística, para tentar perceber se naquela circunstância concreta vamos dar prevalência a um ou a outro.” [N27-Professor(a)/investigador(a)]

A confiança dos cidadãos nas instituições estatais e/ou organizações privadas que recolham, armazenem e partilhem dados é um dos fatores que pode condicionar e restringir o fluxo de dados por receios associados com a salvaguarda da privacidade e da proteção de dados (Hoeyer et al., 2016). Deste modo, o caso altamente mediatizado de Edward Snowden deu origem a várias tensões entre a confiança dos cidadãos nos Estados, mas também a confiança em empresas privadas que cederam dados pessoais dos seus utilizadores à NSA (Wright & Kreissl, 2015). As atividades das empresas e do Governo dos EUA contribuíram ativamente para uma rede contínua de vigilância em massa de pessoas que nunca tinham cometido crimes colocando sérios desafios à democracia e à transparência (Balzacq et al., 2006; Balzacq, 2005; Brown, 2009; Kietz & Maurer, 2006; Liu, 2013).

No extrato apresentado, o/a entrevistado/a constata que existiu um esforço real na manutenção dos direitos dos cidadãos, nomeadamente, o da proteção dos dados pessoais. Porém, este direito apela regularmente à autodefesa e à proatividade do próprio cidadão em questionar e solicitar ao controlador dos dados o apagamento dos mesmos. Sendo que, a tónica na proatividade implícita nos mecanismos de controlo pode, em casos mais extremos, atuar como fator de desresponsabilização das práticas de recolha de dados por parte das empresas e do próprio Estado.

“Entendo que a opção do legislador Europeu por introduzir este novo direito que constituiu uma forma de, por um lado, permitir que as instituições europeias venham dizer, os cidadãos podem estar descansados porque os seus direitos no contexto do novo regime de proteção de dados saem reforçados. (...) Ao mesmo tempo, o reforço dos direitos das pessoas, é de uma tendência para a autorregulação, ou autodefesa no caso dos cidadãos. Autorregulação por parte dos controladores de dados. Autodefesa na medida em que se remete para os indivíduos ao mesmo tempo uma responsabilidade de se defenderem.” [N17-Professor(a)/investigador(a)]

4.2.2. Reino Unido

A presente análise empírica irá versar sobre as 16 entrevistas semiestruturadas realizadas no Reino Unido. As entrevistas tiveram como objetivo apreender as perspetivas dos vários *stakeholders* (11) e dos geneticistas forenses (5) em relação ao sistema Prüm, questões de privacidade e proteção de dados da partilha de informações, à base de dados forense nacional e à interoperabilidade entre bases de dados forenses e biobancos. Os *stakeholders* encontram-se nas seguintes categorias profissionais: órgãos de investigação criminal (2); entidades de supervisão e regulação (5); organizações não governamentais de Direitos Humanos (2); empresas privadas (2).

À data das entrevistas, entre 2015 e 2019, o Reino Unido encontrava-se num período de instabilidade política fruto da votação do *Brexit*, em 2016. Atendendo a este contexto, é necessário ressaltar que este foi um dos fatores que influenciou as perspetivas dos/as entrevistados/as a respeito do sistema Prüm e do posicionamento político do país em relação à União Europeia.

Desafios éticos da utilização das bases de dados de perfis de DNA para fins forenses

Um dos objetivos do guião de entrevista foi compreender de que modo os geneticistas forenses e os *stakeholders* enquadram os desafios éticos presentes no recurso a bases de dados forenses para a deteção e detenção do crime. A sobrerrepresentação de certas minorias étnicas nas bases de dados forenses (Skinner, 2013, 2018; Van Camp & Dierickx, 2007), principalmente no contexto nacional do Reino Unido, foi um dos pontos éticos elencados pelos geneticistas forenses. Esta preocupação com o racismo institucional encontra-se a par com os trabalhos que têm abordado a sobrerrepresentação da população negra na NDNAD (Downey et al., 2012; Skinner, 2013) que tem gerado intenso debate em torno da problemática do racismo nas polícias. No extrato que se segue, o/a entrevistado/a denota que o facto de existirem grupos *a priori* em desvantagem por pertencerem a minorias étnicas é um desafio ético a ter em consideração na construção das bases de dados forenses.

“Penso que o maior desafio ético seria (...) a sobrerrepresentação de certos grupos étnicos na base de dados de DNA. (...) Obviamente o racismo institucional é um assunto que continua a ser falado na polícia Britânica. (...) Penso que isto é um problema, que tenhamos pessoas e grupos em desvantagem. Mas as pessoas vão contestar isto e dizer que não há razão, se não se estiver a fazer nada de errado não há problema. Mas, claramente, a pessoa está em desvantagem.” [D10-geneticista forense]

As bases de dados forenses são construídas com base em critérios discriminatórios, pois não possuem toda a população, na sua generalidade, os indivíduos que têm os seus perfis numa base de dados forense já tiveram contacto com as malhas da justiça. Dito isto, os critérios de inserção variam de acordo com o contexto nacional em que a base de dados forense se encontra. A possibilidade de construção de uma base de dados universal como fator de diluição dos desafios éticos associados à discriminação racial e étnica foi uma das soluções elencadas nas entrevistas. Sendo que as perspetivas acerca da expansão universal de bases de dados de perfis de DNA para a resolução do crime não são consensuais. Por um lado, um estudo a respeito das perspetivas de reclusos sobre bases de dados forenses mostrou que os participantes não apoiavam a criação de bases de dados universais para fins

de investigação criminal por não confiarem nas autoridades governamentais para a gestão e utilização justa dos seus dados (Machado & Prainsack, 2012, p. 172). Por outro lado, a construção de uma base de dados forense universal é encarada, por parte de vários autores, como uma opção que pode favorecer a privacidade dos envolvidos (Dedrickson, 2017), apresentando-se como um dos dilemas éticos deste tipo de infraestruturas. Dedrickson (2017) defende que a universalidade das bases de dados traria benefícios ao nível da resolução mais eficiente de crimes, da exoneração de inocentes e da redução de comportamentos racistas na aplicação da lei (p. 637). No entanto, o carácter universal traz consigo a necessidade de se implementarem medidas de proteção de dados e da privacidade complementares às já existentes (*idem*, p. 639). Neste sentido, a destruição de amostras de DNA é encarada como uma medida que promove a privacidade das pessoas que constam na base de dados universal (Dedrickson, 2017; Simoncelli, 2006; Smith, 2006). Como se pode observar no excerto abaixo apresentado, o/a entrevistado/a, geneticista forense, expressa o seu favorecimento pela existência de bases de dados universais. Os seus argumentos encontram-se em linha com os apresentados por parte dos autores que defendem esta prática como amenizadora dos desafios éticos relacionados com a privacidade e a sobrerrepresentação de minorias.

“Eu sou uma dessas pessoas peculiares que não se importa que todas as pessoas estejam na base de dados. De certo modo, o facto de todas as pessoas estarem nela mostra que a base de dados não é prejudicial para nenhum grupo em particular. (...) E há muitas razões diferentes para isso, uma delas é que um crime é um crime e não podemos deixar de investigar as pessoas porque podem ficar aborrecidas. E, indubitavelmente, ser difamado é uma consequência e uma questão social que precisa de ser resolvida (...). E eu também diria que é ingénuo supor que pessoas de minorias étnicas não querem que os crimes sejam investigados apenas porque é alguém da sua comunidade que está a cometer o crime.” [D11-geneticista forense]

Os geneticistas forenses entrevistados no âmbito do presente estudo elencam um último tópico como um desafio ético relativamente à utilização de prova genética no decorrer de uma investigação criminal. No extrato, o entrevistado refere que o modo como

a polícia avalia a prova genética pode apresentar-se como uma questão ética, pois, existe uma sobrevalorização da prova de DNA em detrimento de outras provas que são igualmente importantes para identificar a pessoa que perpetuou um crime (Lynch, 2013, p. 60). A perspectiva deste/a entrevistado/a enquadra-se no ‘pragmatismo biométrico’ (Williams & Johnson, 2004b) que se caracteriza pela reflexão a respeito da legitimidade da utilização da prova de DNA consoante o contexto em que esta se insere (p. 211; Machado et al., 2013; Matos, 2013).

Na narrativa do/a entrevistado/a as polícias gozam de um ‘entusiasmo tecnológico’ (Costa, 2017) que pode ter repercussões no modo como a prova genética é avaliada por estes profissionais. Neste sentido, a ‘visão profissional seletiva’ (*idem*) da utilidade do DNA na investigação criminal pode afetar significativamente a robustez de todo o processo. Parafraseando o/a entrevistado/a, se não existir prova biológica, a polícia considera que o caso não é possível de solucionar. A dimensão ética desta questão tem que ver com a não resolução de casos criminais, potencialmente com vítimas, devido ao mau julgamento das provas disponíveis por parte dos profissionais das polícias.

“Penso que um dos desafios éticos é compreender realmente que o DNA não é tudo, e que muitas vezes precisamos de outras provas para o corroborar. Pode ser um testemunho ocular... provas essenciais. Mas precisamos de alguma coisa mais para construir o caso. Então, o DNA não é só DNA. Penso que temos assistido a uma pequena revolução do DNA, se não houver DNA, a polícia dá o caso por encerrado, é um caso sem solução. Mas a situação não é realmente essa.” [D12-geneticista forense]

A necessidade da proteção dos dados dos indivíduos que constam nas bases de dados forenses de perfis de DNA foi um dos problemas éticos realçados pelos entrevistados a desempenhar funções em entidades de supervisão/regulação. No entanto, o/a entrevistado/a cujo extrato se encontra abaixo apresentado, considera que o direito à privacidade e proteção de dados se encontra melhor salvaguardado no âmbito forense do que em bases de dados com finalidades médicas (para um aprofundamento a respeito das perspetivas públicas em relação a biobancos e bases de dados forenses consultar Machado & Silva, 2014a, 2014b, 2015a, 2015b). O escândalo público em relação às atividades da NSA

através do testemunho de Edward Snowden, em 2013, revelou extensas atividades de vigilância sobre populações, líderes políticos internacionais e diversas empresas (Dijck, 2014; Wright & Kreissl, 2015, p. 6). A revelação dos documentos que comprovavam a vigilância massiva dos cidadãos gerou tensões entre os países envolvidos, como também conduziu à deterioração da confiança pública ao nível nacional por receio de estarem a ocorrer atividades de controlo semelhantes (Lyon, 2014). Dito isto, o/a entrevistado/a revela que, devido ao sucedido com a NSA, os Governos dos vários países têm procurado adotar medidas de transparência para que a confiança pública nos seus modos de atuação seja mais elevada. Entende-se que a preocupação com os níveis de confiança dos cidadãos no Estado pode conduzir a políticas mais protetoras dos dados pessoais das pessoas envolvidas nas bases de dados forenses.

O/a entrevistado/a realça um último ponto em relação à proteção de dados que é igualmente relevante no contexto do desenvolvimento tecnológico que permitiu a criação de bases de dados forenses e a recolha de informações em grande escala. Pelo que, a categoria de informação sensível sobre um indivíduo passa também pela potencial obtenção de demasiados dados a seu respeito. Neste sentido, defende que é necessário avaliar o dano através de uma lente diferente da que tradicionalmente tem sido utilizada pelos comités de ética (Metcalf & Crawford, 2016). A posição do/a entrevistado/a encontra-se em linha com o que a literatura tem vindo a abordar sobre a escassez de debate e a urgência na atualização do enquadramento ético da recolha de informações obtidas não só em bases de dados privadas, como também em bases de dados públicas. Segundo vários autores, os *standards* pelos quais a regulamentação ética se guia estão obsoletos, pois o desenvolvimento tecnológico veio permitir inferir associações até então impossíveis (Metcalf & Crawford, 2016; Nissenbaum, 2010), por exemplo, através de práticas de *Big Data*, como se verificou na NSA. Portanto, a reflexão ética tem de ir além da avaliação do dano físico na utilização das bases de dados para equacionar outras dimensões que englobam o impacto das práticas na privacidade, proteção de dados e discriminação através dos dados (*idem*).

“A questão da proteção de dados no domínio forense é vista como menos problemática porque os sistemas estão bem protegidos do acesso externo que, desde que não tenhamos razão para desconfiar do governo sobre estes dados, estão

muito mais seguros do que no campo médico. Acho que os governos, provavelmente, nas democracias liberais, são afetados pelo efeito da NSA. Não querem a sua reputação prejudicada se for vista como abusiva na utilização das informações confidenciais das pessoas. E informação sensível pode ser apenas muita informação sobre alguém (...). Então, acho que precisamos de uma melhor compreensão de dano.” [D06-entidade de supervisão/regulação]

Em relação aos desafios éticos da utilização das bases de dados de perfis de DNA para fins forenses, um/a dos/as entrevistados/as, a desempenhar funções numa ONG dedicada aos Direitos Humanos, aponta para o perigo da expansão constante das bases de dados forenses e a introdução consecutiva de novas tecnologias. O extrato abaixo apresentado denota explicitamente a apreensão deste/a entrevistado/a sobre os motivos comerciais subjacentes à motivação para a expansão destas ferramentas, ao invés de uma análise que permite discernir se a expansão das bases de dados forenses aumenta a capacidade de resolução do crime. Sendo que, a expansão das bases de dados forenses e o aumento da vigilância sobre os cidadãos pode conduzir à vulnerabilização de determinadas populações (Chow-White & Duster, 2011; Duster, 2004, 2006; Machado et al., 2010). A pressão comercial, referida pelo/a entrevistado/a, para a expansão e introdução de novas tecnologias para aplicação no campo forense nem sempre é útil para o controlo mais adequado do crime. Realçando-se que a comercialização dos serviços forenses os torna suscetíveis às variações do mercado (Lawless, 2011, p. 682), pelo que o investimento em novas tecnologias pode ocorrer devido aos imperativos de mercado. Neste sentido, também Roberts (1996) defendeu que a comercialização dos serviços forenses teria implicações a longo prazo na gestão da justiça criminal.

“Penso que [um dos desafios éticos] é a pressão para continuar a expandir as bases de dados já existentes e a introdução de novas tecnologias de modo a criar novos mercados. Por isso, acho que a criação de novos mercados é impulsionada por muitas mudanças que vêm de uma abordagem comercial e económica e não da tentativa de perceber qual é a melhor forma de resolver mais crimes.” [D05-ONG de direitos humanos]

Outro/a entrevistado/a de uma ONG de direitos humanos identifica a celeridade nas decisões políticas e o discurso assente no risco como um potencial desafio ético à utilização de bases de dados forenses. A criação e expansão de sistemas de vigilância, como as bases de dados forenses, são regularmente justificadas por discursos que versam sobre a importância da gestão do risco. O seu objetivo é precisamente eliminar a situação de risco, mesmo antes de este ocorrer (Bogard, 2007, p. 60). Subjacente ao discurso sobre o risco aparece o desenvolvimento do pânico moral (Cohen, 2002; Garland, 2008; Goode & Ben-Yehuda, 1994) nas sociedades europeias como resposta à possível deterioração das suas estruturas de valores. Sendo que, uma das consequências diretas do pânico moral na classe política passa pelo que o/a entrevistado/a identifica como uma linguagem de crise e urgência à qual se alia a rapidez na adoção de medidas políticas para o controlo do crime. Como se observa no excerto, a cúpula do perigo iminente deixa de parte várias considerações éticas a respeito da recolha crescente e do armazenamento de dados biométricos devido à pressão que os magistrados sofrem nesse sentido.

“As propostas são todas introduzidas num discurso de crise, urgência e de necessidade de fazer as coisas muito rapidamente, o que significa que estas podem não ser muito bem executadas. E (...) propondo introduzir novos métodos de recolha e armazenamento de dados biométricos, e recolha de informações de mais pessoas, sem ter a certeza de que há tempo para todas as considerações e debates, sem que os magistrados sejam pressionados o tempo todo por este sentido de urgência e crise, é potencialmente muito problemático.” [D16-ONG de direitos humanos]

Regime de retenção ‘Protection of Freedoms Act 2012’ na base de dados forense nacional

No que toca ao enquadramento legal da base de dados forense nacional, um dos pontos enfatizados pelos entrevistados tem que ver com o novo sistema de retenção de perfis e amostras de DNA. O novo sistema faz parte do documento *Protection of Freedoms Act 2012*, implementado no decorrer de uma decisão do Tribunal Europeu dos Direitos Humanos, referente ao caso de *S. and Marper versus The United Kingdom*. Como já supramencionado, uma das alterações estruturais aos critérios de retenção de perfis de DNA foi a restrição temporal imposta na retenção de perfis de pessoas detidas, mas não condenadas. Quanto aos perfis de DNA de pessoas condenadas continua a ser possível a sua

retenção por tempo ilimitado. Uma das questões que tem vindo a ser analisada é o possível impacto do novo regime de retenção, que obrigou à eliminação de um número avultado de perfis de DNA, na eficácia da base de dados. Os vários relatórios, redigidos pelos órgãos encarregues da supervisão das atividades da base de dados, mostraram que o PoFA veio aperfeiçoar o seu desempenho devido ao aumento do valor da taxa de correspondências (Amankwaa & McCartney, 2018). Dito isto, o extrato abaixo apresentado demonstra que o/a entrevistado/a, pertencente a um órgão de investigação criminal, partilha da mesma perceção em relação ao PoFA, referindo que a eliminação dos perfis de pessoas detidas (não condenadas) não afetou significativamente a prevenção e deteção do crime, logo a eficácia da base de dados.

“Tanto quanto eu sei, a percentagem de perfis de DNA de cenas de crime que corresponde a uma pessoa conhecida na base de dados nacional de DNA não se alterou, apesar da eliminação de um número significativo de perfis de detenção. Assim, parece que este processo (...) não teve um efeito significativo na prevenção e deteção do crime.” [D04- órgão de investigação criminal]

Outro/a entrevistado/a, membro de um órgão de investigação criminal dos Serviços Forenses, com formação em biologia e campos relacionados, partilha a mesma representação quanto ao impacto do novo regime de retenção de perfis de DNA. Pode constatar-se no extrato que o/a entrevistado/a não considera problemática a exclusão de amostras/perfis de DNA de pessoas inocentes na deteção e detenção de atividades criminosas.

“Na verdade, de acordo com a lei temos margem para reter uma amostra enquanto a investigação ainda está ativa. Mas tenho que ser honesto e dizer que não nos apercebemos de nenhum impacto com a destruição das amostras no Reino Unido. Não é que tenha causado grandes problemas nos tribunais, ou em termos de não se ser capaz de detetar (ou impedir) o crime.” [D01-órgão de investigação criminal]

Apesar dos entrevistados reconhecerem que o PoFA é um regime pertinente para a base de dados forense apontam aspetos menos favoráveis que colocam várias tensões na sua implementação. Os tópicos enunciados pelos participantes do estudo que fazem parte de entidades de supervisão/regulação encontram-se em linha com o trabalho de Amankwaa e McCartney (2018). Onde, ao nível da implementação do PoFA, a complexidade informática para a eliminação total dos dados e do perfil de DNA é um ponto preocupante, pois pode verificar-se a permanência de perfis que deveriam ter sido eliminados da base de dados. Um/a dos/as participantes, membro de uma entidade de supervisão/regulação revela que aplicar os procedimentos de eliminação numa tecnologia com tantos anos e que não previa a eliminação de dados pode demonstrar-se uma tarefa complicada e comprometer a implementação total do regime de retenção.

“A dificuldade foi implementar um regime de retenção como este que quando foi implementado usou uma tecnologia que foi desenvolvida há 30 anos e que não foi concebida para estes fins. E assim, o resultado foi, por causa do fracasso no investimento em tecnologia nesta fase, a criação de um regime de retenção que na verdade nunca será capaz de ser implementado na íntegra.” [D03-entidade de supervisão/regulação]

Na mesma linha, outro elemento de uma entidade de supervisão/regulação realça os constrangimentos ao nível das infraestruturas informáticas da polícia e a consequente dificuldade em eliminar toda a informação a respeito de um perfil de DNA.

“É terrivelmente difícil [o PoFA]. (...) E particularmente na polícia, as infraestruturas informáticas (IT) não são muito boas. Para além disso, há as questões relacionadas com o facto de as amostras de DNA serem processadas em conjunto, portanto, se se tentar excluir uma amostra, não se pode excluir todo o conjunto. Portanto, tem havido esta questão de os nossos colegas dissociarem os dados brutos de qualquer informação que possamos rastrear até à fonte. Mas certificarmo-nos de que se pode separar completamente estes dados brutos de qualquer informação é muito difícil.” [D07-entidade de supervisão/regulação]

As críticas ao novo regime de retenção remetem ainda para dificuldades, por parte das forças policiais, na compreensão de certas regras, nomeadamente, as que clarificam os trâmites a serem adotados caso se pretenda a retenção ilimitada de um perfil de DNA de uma pessoa inocente (Amankwaa & McCartney, 2018), situação que implicitamente revela o desconforto de parte das forças policiais em relação às opções do legislador (*idem*). No extrato abaixo, o/a entrevistado/a revela as tensões entre as forças policiais e a opção do legislador relativamente aos procedimentos para a permissão da retenção ilimitada de perfis de DNA de pessoas detidas, não condenadas. O/a participante, com formação em direito, posiciona-se ao lado da polícia ao referir que o risco de uma retenção injustificada deveria ser assegurado pelo legislador, ao invés de ser imputado à própria polícia.

“Em geral, existem regras claras quando se trata de requerimentos. (...) Onde quer que se escreva uma alínea, haverá alguns casos que serão terrivelmente lamentáveis, mas isso seria um risco para o legislador, e o que ele, inteligentemente, fez foi transferi-lo para a polícia. Então, quando tudo der errado, poderá dizer ‘eu teria apreciado que tivesse feito um requerimento’ e, talvez, eles (polícia) não o tenham feito. Acho que há aspetos do regime que são desnecessariamente complicados e, francamente, carecem de coragem política.” [D03-entidade de supervisão/regulação]

A complexidade tecnológica da eliminação de perfis de DNA e respetivos dados de pessoas não condenadas pode acarretar consequências sérias no âmbito da atuação policial e judicial. Um erro no apagamento de perfis de DNA ou de dados subjacentes pode culminar na retenção de informações na base de dados sem o devido enquadramento legal. Em termos práticos, pode ocorrer a correspondência de um perfil de DNA ilegalmente retido com um perfil legalmente retido na base de dados. Esta situação apresenta-se como uma violação da privacidade e da proteção de dados das pessoas envolvidas no processo. Neste seguimento, um/a outro/a participante, também membro de uma das entidades de supervisão/regulação, mostra-se preocupado/a com as opções a tomar caso se verifique uma correspondência ilegal no âmbito do novo regime de retenção de perfis de DNA. No excerto, é defendida uma recolha mais cuidada tanto de amostras, como de perfis de DNA,

acrescentando que o mais adequado seria o país possuir um base de dados mais pequena, porém, mais eficiente (Santos et al., 2013).

“Os nossos perfis serão destruídos. E o que acontece se um perfil não for destruído (...) e dá uma correspondência? Eu acho que gostaria de saber se temos os recursos para realmente cumprir o procedimento, quando se trata da destruição de um perfil, mas acho que devemos ser mais cuidadosos e mais restritos ao recolher perfis, amostras, devemos ser muito diligentes em apagá-los depois de um tempo, devemos ter uma base de dados menor mas com mais qualidade.” [D06-entidade de supervisão/regulação]

O/a mesmo/a entrevistado/a apresenta uma solução para a eliminação de dados que deveria resolver a questão da eliminação de perfis de DNA de pessoas detidas cujo processo terminou sem condenação em tribunal. Situação que, no novo regime, obriga à remoção do perfil de DNA da base de dados, onde a retenção do mesmo tem de ser realizada através de um pedido específico e caso-a-caso.

“Acho que quando os novos perfis são inseridos [na base de dados] poderiam ter uma data de expiração, seriam eliminados automaticamente a menos que alguém parasse o processo. (...) E, também, podemos pensar em métodos de *machine learning*. O sistema poderia aprender os padrões de destruição dos perfis e, em seguida, marcar automaticamente os valores discrepantes, perfis que podem ter sido esquecidos, (...) na base de dados. Acho que, neste caso, acredito realmente em soluções tecnológicas.” [D06-entidade de supervisão/regulação]

O aumento constante do número de perfis de DNA na base de dados forense e o crescimento de sentimentos de insegurança – medo do crime – camuflaram a diminuição das taxas de criminalidade no país (McCartney et al., 2010; Skinner, 2013, p. 978). A inclusão continuada de perfis de DNA de pessoas não condenadas na base de dados forense pode apresentar-se como um obstáculo ao cumprimento das liberdades civis e do direito à privacidade e proteção de dados (Downey et al., 2012). Um/a dos/as participantes do presente estudo, a trabalhar numa ONG, refere que a mudança das perceções públicas

acerca da base de dados forense esteve relacionada, entre outros motivos, com a decisão do Tribunal Europeu dos Direitos Humanos (caso de *S. and Marper*). As perspetivas pós decisão foram no sentido de repensar a proporcionalidade da opção de reter perfis de DNA de pessoas inocentes na base de dados. Apesar de se verificar um consenso público quanto à retenção de perfis de pessoas condenadas, em relação às pessoas detidas não condenadas existe alguma resistência nesta prática (Amankwaa, 2018). As questões relacionadas com privacidade e possíveis desvirtuamentos da informação foram os aspetos mais elencados para justificar a opção de não concordar com a retenção (*idem*).

No extrato apresentado, o/a entrevistado/a dá conta do contexto político em que o novo regime de retenção foi discutido. Por um lado, a existência de debate público a respeito da base de dados e a decisão do caso *S. and Marper*. Por outro lado, a opção escocesa em não permitir a retenção ilimitada de perfis de DNA de pessoas inocentes. Para o/a entrevistado/a, a maior consciencialização pública acerca da base de dados forense levou a que se verificasse um aumento dos pedidos de informação, por parte do público à sua ONG, de modo a solicitar a remoção das suas informações da base de dados. Acrescente-se que, na sua perspetiva, a ONG em que desempenha funções teve um papel importante na desmistificação de certos imaginários sobre a elevada resolução de crimes através da inclusão de DNA de inocentes na base de dados forense.

“Bem, penso que não foi apenas o caso de *Marper*, o debate público aqui no Reino Unido também foi muito significativo. (...) Os indivíduos que estavam na base de dados, ou cujos filhos estavam na base de dados, começaram a perceber o que estava a acontecer e ficaram mais preocupados. Começamos a receber muitos telefonemas e e-mails de pessoas a perguntar como poderiam sair da base de dados, e começaram a ir ao parlamento para pedir a remoção [do perfil]. Assim, o caso *Marper* é até agora muito significativo, mas ocorreu num contexto em que o exemplo escocês era muito importante. O governo também tinha assumido que, naquela altura, tinha resolvido muitos crimes usando esta função e que tinham o apoio do público para a sua expansão. Mas, na realidade, conseguimos demonstrar com os números do governo que eles não tinham resolvido mais crimes e que o público estava muito dececionado. Então, isto ajudou a criar o espaço político para (..) a decisão de implementar (o novo regime) porque, como provavelmente sabe, o

Reino Unido nem sempre implementa as decisões do Tribunal Europeu.” [D05-ONG de direitos humanos]

O modo como a maioria dos/as entrevistados/as abordaram a temática do novo regime de retenção de dados na base de dados forense é reveladora de raciais de pensamento diferentes dependendo das funções desempenhadas no âmbito das suas categorias profissionais. Apesar de diferentes nuances no entendimento do PoFA, o imaginário comum acerca da alteração do regime é consonante com a ideia de que esta é uma alteração que veio reforçar a proporcionalidade da recolha de dados Estatal. Os participantes afetos aos órgãos de investigação criminal focaram as suas respostas na eficácia da base de dados forense com o PoFA considerando que, em termos práticos, esta não seria prejudicada nos seus índices de eficiência. Os entrevistados pertencentes a entidades de supervisão/regulação mostraram maior preocupação em aprofundar os problemas éticos e técnicos que, no seu entender, advêm da implementação do novo regime de retenção. Sendo que, estes dilemas éticos podem comprometer o sucesso da nova legislação e a legalidade da retenção de um perfil de DNA, situação que se pode apresentar como um obstáculo ao cumprimento das liberdades civis dos cidadãos britânicos. Os entrevistados que desenvolvem atividades no âmbito de ONGs optaram por salientar as consequências públicas do debate em torno do novo regime de retenção de dados e do papel deste tipo de entidades para o esclarecimento de dúvidas por parte dos cidadãos.

Vantagens e desafios do sistema Prüm

A entrada do Reino Unido no sistema Prüm tem sido caracterizada por avanços e recuos políticos. Cronologicamente, em 2007, o discurso político estava em linha com aqueles que eram os objetivos da União Europeia em relação ao sistema Prüm. Em 2013, verificou-se o recuo do novo Governo em relação à implementação de Prüm por motivos de ordem económica. Em 2014, a União Europeia recebeu a decisão da não entrada do Reino Unido no sistema Prüm. Esta decisão veio contrariar o imaginário de cooperação transnacional que tem como ambição aumentar a segurança ao nível internacional, como também no panorama nacional. A decisão foi criticada por vários académicos, mesmo antes de se tornar oficial, em 2013, McCartney (2013) referia, num dos seus trabalhos, que a não

entrada no sistema Prüm isolava o Reino Unido em matéria de cooperação policial e de segurança na União Europeia (p. 559). Entre os anos de 2017 e 2018 foram retomadas as negociações em Prüm e o Reino Unido encontrava-se a realizar a avaliação nacional da implementação de Prüm que com o *Brexit* voltou a abrandar e está dependente das negociações com a União Europeia.

De modo geral, os geneticistas forenses entrevistados mostram-se favoráveis à participação do Reino Unido no sistema Prüm. Os motivos elencados por este grupo para justificar a entrada do país no sistema Prüm encontram-se a par com as vantagens enunciadas na literatura (McCartney, 2013). No qual, este sistema oferece aos países um empoderamento (Prainsack & Toom, 2010) na capacidade e celeridade na resolução de crimes que ocorrem em diferentes jurisdições, pois permite a procura de correspondências nas bases de dados forenses de todos os Estados-Membros. No extrato abaixo apresentado, o/a entrevistado/a demonstra a sua receptividade ao sistema Prüm dando conta de uma investigação criminal que poderia ter sido mais rápida e, possivelmente, evitado novas vítimas se os países envolvidos possuísem ferramentas de cooperação. Para concluir, refere que a direção a seguir é a da cooperação transnacional entre Estados-Membros.

“Estou feliz! Porque nós tivemos o caso de um camionista que matou muitas prostitutas e outras mulheres entre a fronteira do País A, do País B e do País C. E eles só não o apanharam porque não partilharam informações. (...) Só o apanharam porque uma mulher escapou. (...) Se eles tivessem o DNA mais cedo poderiam ter percebido que era um camionista porque todos os homicídios aconteceram ao longo de uma autoestrada. (...) Temos que ir nesta direção [da partilha de dados transnacionais].” [D08-geneticista forense]

Um/a outro/a entrevistado/a, também geneticista forense, refere que o sistema Prüm seria mais adequado enquanto ferramenta de cooperação policial e judicial do que o mandado de detenção europeu⁶⁰. Nas suas palavras, o mandado de detenção europeu possui um caráter arbitrário, ao passo que a gestão de bases de dados forenses entre diferentes países, através do sistema Prüm, é mais controlada. Numa segunda fase da

⁶⁰ Para mais informações a respeito do mandado de detenção europeu consultar: https://e-justice.europa.eu/content_european_arrest_warrant-90-pt.do

resposta, desenvolve aqueles que considera serem pontos problemáticos no sistema Prüm ao nível na União Europeia. Os tópicos enfatizados foram partilhados com a literatura que pretende dar conta dos desafios do sistema Prüm (Amankwaa, 2019; Sallavaci, 2017; Santos, 2017; Santos & Machado, 2017). Em particular, a existência de tradições judiciais distintas entre Estados-Membros e os diferentes *standards* científicos aplicados à ciência forense e às bases de dados, por exemplo, o número de marcadores de um perfil de DNA inserido na base de dados.

“Penso que seria provavelmente a favor da procura transnacional nas bases de dados de DNA. Na verdade, sou provavelmente mais favorável a isso do que ao mandado de captura internacional, que me parece ser bastante arbitrário. E isso é muito mais preocupante para mim do que ter dados de perfis de DNA enviados para outras jurisdições através da gestão das bases de dados. Ainda ninguém foi algemado e colocado num avião por causa disso. (...) Pela Europa, como um todo, tenho algumas dúvidas, porque penso que existem diferentes abordagens à justiça e diferentes padrões de ciência. Diferentes estados de desenvolvimento na ciência. (...) Além disso, é aí que precisamos de fazer perguntas: ‘Bem, nós temos uma correspondência, mas espera um minuto, quais foram os padrões de acreditação deste laboratório? É confiável?’” [D11-geneticista forense]

No decorrer da entrevista, o/a mesmo/a participante refere, mesmo sendo a favor do sistema Prüm, que uma base de dados europeia universal também seria uma opção. No entanto, um ponto enfraquecedor da existência de uma base de dados europeia é a existência de comportamentos corruptos no seio das forças policiais que, ainda que diminutos, poderiam vulnerabilizar os cidadãos que constassem na base de dados. O receio do desvirtuamento da utilização dos dados devido a atividades corruptas das polícias ou órgãos similares (Amankwaa, 2018; McCartney, 2014a) é uma das preocupações mais recorrentes em relação à utilização de bases de dados de material biológico. Contudo, quando este tipo de situação ocorre no âmbito criminal pode levar à incriminação de inocentes e a abusos de poder por parte das autoridades (*idem*).

“Eu gostaria de ser a favor de ter, digamos, uma base de dados universal, mas infelizmente parece que por vezes as investigações têm problemas (...), más práticas. Investigações com um comportamento realmente corrupto. Portanto, se tivermos todas as pessoas (...) numa base de dados Europeia, isto deixá-las-ia vulneráveis a este tipo de situação. No meu ponto de vista estes eventos são raros, mas acontecem, e quando acontecem destroem a vida das pessoas.” [D11-geneticista forense]

Os argumentos utilizados para justificar a não entrada do Reino Unido no sistema Prüm, em 2014, remeteram para o elevado dispêndio de recursos económicos e para um esforço desproporcional do país no segundo passo de Prüm, por comparação com os restantes Estados-Membros (McCartney, 2013, p. 555). O fluxo de trabalho acrescido, por parte do Reino Unido, derivava do facto de possuir a maior base de dados forense da União Europeia (Downey et al., 2012; Johnson & Williams, 2007) e da probabilidade de ocorrerem falsos positivos (Council of the European Union, 2017). Implicitamente, encontra-se uma narrativa política que entende que os países iriam ‘usufruir’ mais da base de dados forense do Reino Unido do que o inverso, numa perspetiva que coloca o ‘interesse nacional’ acima dos ideais da cooperação europeia.

No extrato que se segue, o/a entrevistado/a, geneticista forense, realça vários aspetos que contrariam o discurso político vigente aquando da não entrada no sistema Prüm, bem como dá conta da sua opinião em relação ao *Brexit*. Dito isto, revela-se bastante crítico/a do clima político associado ao *Brexit* e do discurso político que coloca o sistema Prüm enquanto ferramenta a ser utilizada para maximizar a deteção do crime no país, em detrimento de um discurso de maior enfoque na cooperação entre Estados-Membros. Esta entrevista foi aplicada após a votação do referendo, porém ainda não havia consenso em relação ao modelo de saída do Reino Unido da União Europeia. Quanto aos falsos positivos, apesar de reconhecer que poderiam consumir muito tempo, encara que a partilha de informação é mais importante.

“Eu sei que houve preocupações porque a nossa base de dados é muito maior que a dos outros países, iria ter muitos falsos positivos e o tempo que levaria a resolvê-los seria mau para toda a gente. Mas sou bastante a favor da partilha de

informações. Penso também que aqui as pessoas consideram que não há grandes riscos por causa do mar que nos separa, que não vamos ter muitos *[hits]*. Mas, não gosto de olhar para isto na base de ‘o que é que vamos tirar daqui?’. Acho que isso é ridículo. É como todo este absurdo que as pessoas estúpidas estão a tentar aprovar [o Brexit].” [D09-geneticista forense]

Na mesma ótica, o/a entrevistado/a seguinte, geneticista forense, refere que não está certo/a do modo como os cidadãos britânicos irão encarar o sistema Prüm. Por um lado, devido aos meios de comunicação social que são muitas vezes responsáveis por apresentar conteúdo pouco favorável ao programa da União Europeia. Por outro lado, devido à noção implícita de que são os estrangeiros que cometem crimes no Reino Unido e não a situação inversa denotando, novamente, a tentativa de colocar o sistema Prüm a trabalhar em prol dos benefícios para o Reino Unido. Este tipo de discurso é encarado com um tom crítico por parte deste/a entrevistado/a como se pode observar no excerto.

“Penso que o sistema Prüm é uma coisa bem-vinda, como as pessoas na Grã-Bretanha o vão ver isso eu não sei. Mais uma vez, voltando à imprensa, pode haver muitos discursos negativos em relação ao projeto da [União] Europeia. (...) O problema será olhar para todos os europeus a cometer crimes na Grã-Bretanha, isto não é terrível? Em vez de todos os britânicos a cometer crimes em Espanha.” [D10-geneticista forense]

Dois dos geneticistas forenses entrevistados para o estudo elencam um aspeto interessante em relação à avaliação que fazem do fluxo de trabalho do sistema Prüm no Reino Unido, importa referir que ambos são favoráveis à cooperação transnacional através deste sistema. Os/as participantes referem que devido ao afastamento geográfico e à não partilha de fronteiras terrestres com outros Estados-Membros, o impacto do sistema Prüm será menor do que em países que partilhem o espaço geográfico continental da União Europeia. O entendimento de que Prüm terá um impacto menor devido ao facto de ter as suas fronteiras banhadas por mar contraria, de algum modo, o discurso político que elencou o excesso de trabalho no segundo passo como um dos fatores dissuasores da entrada em Prüm (McCartney, 2013).

“[O sistema Prüm] é mais importante na Europa [continental]. (...) Penso também que aqui as pessoas consideram que não há grandes riscos por causa do mar que nos separa, que não vamos ter muitos [*hits*].” [D09-geneticista forense]

“Penso que [o sistema Prüm] é uma decisão positiva. Acho que é muito mais aplicável à Europa continental do que ao Reino Unido. (...) Tenho a certeza de que há pessoas da União Europeia a cometer crimes aqui e vice-versa, mas o impacto não será tão grande como na fronteira entre a Alemanha e a França.” [D10-geneticista forense]

O acesso mútuo a bases de dados forenses dos países da União Europeia assegurado pelo sistema Prüm veio, na perspetiva dos/as entrevistados/as que desempenham funções em órgãos de investigação criminal, permitir vários avanços na cooperação policial e deteção do crime. Primeiro, tornou a partilha de informações mais barata devido à reduzida dimensão dos ficheiros partilhados, pois os perfis de DNA encontram-se em formato textual. Segundo, consequência da redução dos custos, trouxe consigo a possibilidade de se partilharem todos os perfis, sejam eles de crimes mais ou menos graves. Terceiro, a automatização do primeiro passo de Prüm conferiu maior rapidez e simplicidade a todo o processo de partilha de informação pessoal a respeito de um perfil de DNA. O extrato que se segue denota o imaginário forense (Williams, 2010) a respeito das potencialidades de um sistema como o de Prüm para a partilha de informação com vista à deteção e detenção do crime transnacional. Dito isto, o sistema Prüm é caracterizado pelos entrevistados como rápido, simples e com elevado volume de informação a ser confirmada e partilhada em detrimento de outros mecanismos de cooperação existentes como a Interpol que consome mais tempo devido às infraestruturas em que opera (Van Camp & Dierickx, 2007).

“Podem enviar-se a custo reduzido alguns *kilobytes* de dados para vários países. (...) Podem enviar todos os vossos perfis de cena de crime. Dito isto, o volume é importante, a velocidade é importante e a simplicidade extra, porque foi projetado um sistema no qual as pessoas em vez de transcreverem manualmente um perfil de cena de crime para o sistema da Interpol e depois a Interpol transcrevê-lo

manualmente para outros países... Isto acontece automaticamente.” [D04-órgão de investigação criminal]

A par com as vantagens elencadas pelos/as entrevistados/as, um/a dos/as entrevistados/as de um órgão de investigação criminal, refere explicitamente os benefícios que o Reino Unido pode retirar do sistema Prüm. Na sua perspetiva, a adesão a esta ferramenta de cooperação policial e judiciária permite, potencialmente, a identificação de pessoas estrangeiras que cometeram crimes em território nacional e que ainda não são conhecidas das autoridades britânicas. A narrativa presente no extrato denota uma tentativa de instrumentalização do sistema Prüm com o objetivo de diminuir o número de crimes praticados por estrangeiros no Reino Unido em detrimento de uma lógica de cooperação transnacional que funciona nos dois sentidos.

“[E]ncontramos alguns crimes, crimes graves como violação, assaltos. Isto [o sistema Prüm] não afeta necessariamente o nível de crimes que são cometidos, mas, certamente, se 30% das pessoas presas em Londres forem estrangeiras, então devemos obter um benefício no sentido de detetar crimes através da pesquisa nas bases de dados. Quanto maior for a base de dados em que se procura, claramente, maior será a chance de detetar o crime e, particularmente, (...) onde existem ofensores perigosos que iriam cometer mais crimes.” [D01-órgão de investigação criminal]

Os participantes do estudo pertencentes a órgãos de investigação criminal revelam que o sistema Prüm permite descobrir os padrões de crime de determinadas pessoas ou organizações criminosas a operar no espaço da União Europeia. Associada à identificação destes padrões, verifica-se ainda a possibilidade de relacionar investigações policiais entre fronteiras (Hufnagel & McCartney, 2017). O sistema Prüm, nas narrativas dos/as entrevistados/as, aparece enquadrado enquanto ferramenta complementar que, através da automatização do primeiro passo, permite uma maior celeridade nas comunicações entre países (Machado & Granja, 2019a). O excerto seguinte evidência a noção de que o sistema Prüm é um sistema que permite a produção de inteligência para auxílio na investigação criminal (Bigo, 2006).

“O sistema Prüm é importante porque tem a capacidade de relacionar um criminoso no país A com um criminoso no país B. (...) É isto que nos dá a capacidade de estar à frente e mostra que ele [criminoso] está a cometer crimes em A, B, C e D, mas, na verdade, analisamos qual é a inteligência por trás deste indivíduo. (...) Alguém que esteve no sítio A também esteve no sítio B e, depois, como relacionar estas investigações?” [D04-órgão de investigação criminal]

No entanto, o/a mesmo/a entrevistado/a demonstra-se crítico/a da noção do DNA enquanto ‘máquina de verdade’ (Lynch et al., 2008) veiculada por diversos atores sociais, como os meios de comunicação social, referindo que as correspondências no sistema Prüm não são provas concretas, mas antes um modo de justificar determinadas ações. Segundo o/a participante, uma correspondência neste sistema não é o suficiente para mover ações judiciais sobre um indivíduo no Reino Unido (Innes et al., 2005). Pelo que este tipo de ação só ocorre após uma investigação mais aprofundada que prove e contextualize a correspondência obtida. No extrato apresentado encontra-se o fenómeno de Prüm enquanto produtor de *intelligence* entre forças policiais, sendo que uma ação judicial obriga a uma investigação contextual do caso.

“Não estamos a trazer pessoas de volta apenas com base numa correspondência em Prüm. A correspondência é a inteligência que justifica um caminho de ação em particular.” [D04-órgão de investigação criminal]

A adesão do Reino Unido às Decisões Prüm foi acompanhada de um debate a respeito dos potenciais desafios que acompanhariam a implementação do sistema Prüm. As perspetivas dos entrevistados dos órgãos de investigação criminal encontram-se a par daqueles que foram os pontos enunciados no debate político a respeito do tema. Como tal, um/a dos/as participantes concorda com o discurso político, em 2013, em torno do elevado dispêndio de recursos financeiros para a utilização do sistema Prüm como um dos desafios que o país equacionou (McCartney, 2013). Situação que via a sua amplitude aumentada principalmente devido à elevada dimensão da base de dados forense (Downey et al., 2012; Johnson & Williams, 2007).

“Primeiro, e muito importante, é o dinheiro: o custo. Penso que, como a base de dados do Reino Unido era muito maior quando comparada com as europeias, quando o custo para colocar todos os dados de DNA sem o programa CODIS foi analisado, estar na partilha em Prüm seria muito caro.” [D01-órgão de investigação criminal]

O mesmo Governo, em 2013, referiu que, ao possuir a maior base de dados forense de perfis de DNA, ficava numa posição periclitante em relação ao aumento do volume de trabalho consequência do potencial elevado número de pedidos de informação dos Estados-Membros (McCartney, 2013, p. 555). Deste modo, um/a dos/as participantes a desempenhar funções num órgão de investigação criminal, cujo extrato é abaixo apresentado, denota a mesma preocupação em relação à adesão às Decisões Prüm. A preocupação com o excesso de trabalho das forças policiais parece compreender a ideia de um fluxo de informações que segue o sentido do Reino Unido para os restantes Estados-Membros, com um maior ganho por parte dos segundos atores envolvidos nesta partilha de dados.

“As minhas preocupações estão mais relacionadas com a possível sobrecarga de trabalho dos serviços policiais com o número de *hits* (...), porque é preciso mais do que um simples ‘isto é um *hit*’, é preciso desenvolver um processo que olhe para os assuntos internacionais num contexto mais amplo.” [D04-órgão de investigação criminal]

O aumento da possibilidade de ocorrerem falsos positivos devido ao grande volume de perfis partilhados no sistema Prüm (Kierkegaard, 2008, p. 245; Prainsack & Toom, 2010, p. 1124; Santos & Machado, 2017, p. 307; Van der Beek, 2011) foi uma das preocupações políticas elencadas devido à grande amplitude da base de dados forense nacional – NDNAD (McCartney, 2013). Posto isto, os entrevistados dos órgãos de investigação criminal reconhecem a importância de confirmar se as correspondências no sistema Prüm são falsos positivos. No entanto, no primeiro extrato abaixo apresentado, refere-se que nenhum país está a partilhar informação pessoal nestas condições, bem como se relega para os geneticistas forenses a responsabilidade de assegurar que as correspondências respondem

aos critérios exigidos. A demarcação que o/a entrevistado/a de um órgão de investigação criminal demonstra em relação à responsabilidade dos geneticistas forenses em assegurar a qualidade das correspondências tem que ver com o facto de o sistema Prüm ser responsável pela alteração da autoridade epistémica da investigação criminal para o trabalho laboratorial dos geneticistas forenses (Machado & Granja, 2019a; Prainsack & Toom, 2010, pp. 1124–1126).

O/a segundo/a entrevistado/a, problematiza as opções disponíveis consoante os critérios adotados para a ocorrência de uma correspondência. No segundo extrato abaixo apresentado, encontra-se patente uma análise sobre os custos-benefícios de colocar os limites de uma correspondência demasiado elevados ou demasiado baixos (de acordo com o número de *loci* no perfil de DNA). No caso do Reino Unido, o/a entrevistado/a refere que o limite será algo elevado com o objetivo de evitar falsos positivos. Portanto, de modo a evitar falsos positivos deve manter-se o limite de correspondência elevado e procurar um *match* de acordo com a seriedade dos crimes. O facto de os entrevistados não estarem particularmente preocupados com esta questão pode estar relacionado com a forma como o sistema Prüm é encarado por este grupo profissional. Pois, o sistema é entendido enquanto ferramenta de produção de inteligência por parte das forças policiais (Bigo, 2006), pelo que as correspondências não são provas vinculativas.

“Existiu um certo medo de que os falsos positivos poderiam prejudicar o sistema e que as pessoas estariam a fornecer dados pessoais em função dessas correspondências falsas. (...) Não o vamos fazer. (...) Nenhum país o faz. Os cientistas são suficientemente bons, têm de se preocupar com a sua integridade científica.”
[D04-órgão de investigação criminal]

“É difícil, porque se se estabelecerem limites muito altos não se consegue deter o crime, se forem demasiado baixos vão ser gerados muitos *hits* que não têm qualquer valor. (...) Portanto, vamos estabelecer um limite algo elevado, que é o reconhecimento de que queremos correspondências com significado para prosseguir com o processo. A outra coisa que decidimos fazer no [teste] piloto foi focarmo-nos nos crimes mais graves (...). Penso que pode estabelecer-se um limite deste modo, bem como definir a qualidade da correspondência. Penso que são estes dois – a

gravidade do crime e o volume de DNA (...) seriam de facto o que teríamos em conta.” [D01-órgão de investigação criminal]

Uma das dimensões do guião de entrevista remeteu para a temática da garantia das liberdades civis e da supervisão não só das atividades da base de dados como também das atividades do sistema Prüm. Assim, o Reino Unido possui um conjunto de infraestruturas de supervisão que têm como objetivo abarcar os vários desafios da utilização de perfis de DNA para fins de investigação criminal. As entidades de supervisão são responsáveis pela manutenção da base de dados, pelo aconselhamento ético independente em todas as situações que envolvam a base de dados, pela supervisão da retenção e utilização de amostras e perfis de DNA por parte das forças policiais e, por fim, pela manutenção dos regimes de standardização científica no âmbito do trabalho realizado ao nível forense (Amankwaa & McCartney, 2018). Neste sentido, um/a dos/as entrevistados/as, elemento de um órgão de investigação criminal, considera que os direitos civis e o direito à privacidade se encontram assegurados através de um conjunto sólido de entidades responsáveis pela supervisão da base de dados forense e das atividades desenvolvidas no sistema Prüm. No extrato apresentado, realça também que a separação institucional entre os órgãos de supervisão e as organizações afetas de algum modo à investigação criminal permite uma supervisão isenta de influências.

“Penso que temos estruturas de governação bem desenvolvidas, e todas essas pessoas ou funções estão separadas da polícia e mesmo do governo. Então, elas respondem a um Ministério ou reportam ao Parlamento. Isto não é interno ao serviço da polícia ou do Ministério do Interior ou à *Crown justice*.” [D01-órgão de investigação criminal]

A postura política do Reino Unido em relação à adesão de Tratados e documentos vinculativos em matéria de cooperação judicial e policial tem sido revestida de ceticismo (McCartney, 2013). O Tratado de Lisboa e as Decisões Prüm são exemplos representativos da atitude de desconfiança do país em relação aos valores da União Europeia. No seio político, a União Europeia representa uma perda de soberania e de poderes em várias esferas que, para certos políticos, é uma situação ‘inaceitável’ (House of Commons Hansard

Debates 2013, col. 773). A perda de soberania nacional em prol do controlo exercido pela União Europeia encontra-se intimamente relacionada com a sujeição do Reino Unido ao Tribunal de Justiça da União Europeia e à possibilidade de penalização pela Comissão em caso de incumprimento das normas instituídas (McCartney, 2013). No extrato seguinte, um/a dos/as entrevistados/as refere a existência do debate parlamentar acerca dos potenciais desafios aos direitos civis com a adesão ao sistema Prüm. Apesar de não tecer comentários aprofundados acerca da sua perspetiva pessoal a respeito da temática aponta que o debate foi feito à luz de um ‘prisma Eurocético’. Esta entrevista foi aplicada meses antes da votação do referendo *Brexit*, pelo que o debate parlamentar poderá ter sido fortemente condicionado pela conjuntura política à data.

“Foi no debate parlamentar [sobre liberdades civis], sim. Portanto, apenas perfis de ofensores condenados são enviados. [O debate] foi, principalmente, à volta dos falsos positivos, *standards*, tudo encarado sob um prisma eurocético.” [D04-órgão de investigação criminal]

A reflexão acerca dos direitos e liberdades civis dos cidadãos (direito à privacidade, proteção de dados, etc.) com o sistema Prüm foi relativamente superficial e sem questionamento aprofundado. No entender dos entrevistados pertencentes a órgãos de investigação criminal os mecanismos de supervisão existentes ao nível nacional são adequados para o controlo dos padrões éticos necessários à partilha de informação pessoal quer ao nível nacional quer ao nível transnacional. A categoria profissional dos entrevistados – órgão de investigação policial – pode estar na origem da brevidade da discussão, pois as funções desempenhadas no âmbito das suas profissões estão em grande medida associadas à procura de provas que auxiliem na deteção de pessoas ou organizações responsáveis por crimes.

Os participantes do estudo, membros de entidades de supervisão/regulação, foram igualmente convidados a dar a sua perspetiva pessoal em relação ao sistema Prüm, os seus benefícios, riscos e desafios no contexto do Reino Unido. As vantagens apontadas estão em linha com as que foram elencadas pelos entrevistados de outras categorias profissionais e têm que ver com a escala de toda a operação, a rapidez e a eficiência do sistema Prüm. No excerto seguinte, o/a entrevistado/a expressa explicitamente estas vantagens, enfatizando

que esta ferramenta pode oferecer contribuições significativas para a prevenção e a detenção do crime ao nível nacional. Acrescenta que, não estar no sistema Prüm seria um obstáculo à cooperação internacional, na medida em que os restantes Estados-Membros poderiam não estar dispostos a soluções bilaterais que obriguem a um maior dispêndio de recursos.

“A capacidade para procurar numa escala maior em vez de se escolher um país em particular, e fazê-lo muito mais rápido e eficientemente. Penso que é capaz de ser o maior contributo para a prevenção e deteção do crime neste país (...). E, a minha perceção, é de que há um sentimento real na polícia de que não há uma outra opção igualmente satisfatória como alternativa aos acordos individuais com os países europeus, porque não estão interessados, compreensivelmente, em gastar mais tempo a negociar separadamente com o Reino Unido.” [D03-entidade de supervisão/regulação]

No mesmo sentido, um/a segundo/a entrevistado/a, a desempenhar funções numa entidade de supervisão/regulação, está em consonância com a perceção dos restantes participantes quanto à simplificação oferecida pelo sistema Prüm. No excerto é realçado que com a Interpol a cooperação policial transnacional é mais complexa devido à plasticidade dos critérios para a partilha de informação. Portanto, a partilha transnacional de dados pessoais mais eficiente em termos de recursos económicos e humanos encontra-se intimamente dependente da capacidade de standardização das tecnologias de vigilância. Pois, é o processo de standardização de procedimentos que permite tornar o mundo ‘equivalente entre culturas, tempo e espaço’ (Bowker & Star, 1999) precisamente pela construção de critérios comuns aos países para diminuir a flexibilidade do tipo de dados partilhados. Ao contrário da Interpol, o sistema Prüm, através da harmonização de procedimentos, permitiu agregar diferentes comunidades e diferentes práticas numa rede comum, ainda que estejam separadas pela distância e pela heterogeneidade de legislações nacionais (Bowker & Star, 1999; Lampland & Star, 2009, pp. 4-5; Timmermans & Epstein, 2010, p. 71).

“O que é que acrescenta? Tudo. A Interpol não o faz bem porque depende demasiado do que os países querem colocar [na base de dados] (...). Portanto, penso

que (o sistema Prüm) é uma mudança de paradigma e penso que o seu sucesso nos países que o têm usado, até agora, fala por si.” [D06-entidade de supervisão/regulação]

Na perspetiva dos entrevistados pertencentes a entidades de supervisão/regulação, o sistema Prüm veio acompanhado de vários desafios ao nível nacional, nomeadamente, 1) em relação ao tamanho da base de dados forense; 2) ao custo da implementação do sistema Prüm e 3) ao possível aumento de falsos positivos com o aumento da escala de comparação. Os participantes deste estudo mostram-se críticos da postura política de exaltação da identidade nacional em detrimento da retórica de cooperação que, inicialmente, caracterizou o debate acerca do sistema Prüm e influenciou a opção do Reino Unido de não entrar no sistema, em 2014 (House of Lords, 2013; McCartney, 2013). No extrato abaixo, o/a primeiro/a entrevistado/a, integrante de um órgão de supervisão, denota preocupação com os custos de implementação do sistema Prüm devido à elevada dimensão da base de dados e ao fluxo de trabalho necessário para prosseguir com o segundo passo. O/a segundo/a entrevistado/a, considera que, para além da exigência da criação de infraestruturas adequadas à partilha de dados no país, o *Brexit*⁶¹ pode apresentar-se como um dos maiores desafios à implementação do sistema Prüm. A saída do Reino Unido do espaço da União Europeia tem abarcado negociações em várias esferas sociais, uma delas é a que remete para acordos de cooperação ao nível da investigação criminal. O referendo *Brexit* foi apontado como um dos desafios para a implementação do sistema Prüm, pois à data da entrevista já era conhecido o resultado favorável à saída do Reino Unido da União Europeia.

“A base de dados de DNA é muito maior do que a dos outros [países], a implementação de Prüm pode ter impactos financeiros e de tempo consideráveis para a polícia deste país. Porque o número de correspondências que podem vir a ser obtidas e investigadas neste país, por parte de forças [policiais] estrangeiras, pode ser demasiado elevado.” [D03-entidade de supervisão/regulação]

⁶¹ Para mais informações a respeito das negociações e cronologia de trabalho consultar <https://www.consilium.europa.eu/pt/policies/eu-uk-after-referendum/>.

“O Brexit é o [desafio] número 1. (...) O maior. Para além disso, temos de garantir que existem infraestruturas suficientes para a verificação que é feita na segunda fase. Também é preciso colocar em funcionamento todas as infraestruturas necessárias para a partilha automática [passo 1].” [D07-entidade de supervisão/regulação]

A instrumentalização política do sistema Prüm nos debates parlamentares iniciais é novamente alvo de desconforto por parte de um/a dos/as entrevistados/as integrante de uma entidade de supervisão/regulação que se mostra mais favorável à entrada do Reino Unido no sistema Prüm, decisão essa que estava a ser implementada entre 2017 e 2018 (Council of the European Union, 2017, 2018b). No excerto, é referida a falta de reciprocidade de valores do Reino Unido para com a União Europeia. Num tom crítico denota que o respeito moral pelos seres humanos deveria abranger todas as pessoas e não apenas os cidadãos britânicos, por ser importante que todos os países sejam seguros. Posto isto, a conjuntura política inicial é reveladora de um imaginário que hierarquiza os ‘seres humanos’ de acordo com o seu local de pertença, onde quem ‘pertence’ ao Reino Unido goza de um maior valor de vida e de segurança do que as pessoas de outros países. Levada esta hierarquização ao limite, discerne-se que uma vítima de um crime no Reino Unido é mais importante do que uma vítima em qualquer outro país. No mesmo extrato, refere ainda que não existiu um debate que abarcasse adequadamente as liberdades civis em questão no sistema Prüm.

“O debate foi enquadrado pelo governo da seguinte forma: ‘Isto vai manter o Reino Unido seguro’, sem referir se poderíamos ajudar a manter [os outros países] seguros (...). O conceito moral de igualdade em relação a todos os seres humanos não entra facilmente na política moderna (...). E esta foi a forma como o debate foi retratado e trazido para Prüm: ‘Isto é o estado policial Europeu’. (...) Muito habilmente o governo moveu-se desta posição prévia para uma cautelosa aceitação de Prüm. (...) Não parece ter havido qualquer abordagem às liberdades civis.” [D02-entidade de supervisão/regulação]

A crítica à deturpação dos objetivos de Prüm em relação a uma análise autocentrada dos riscos e benefícios da cooperação transnacional foi transversal à maioria dos entrevistados pertencentes a entidades de supervisão/regulação. As perspetivas desta categoria profissional situam-se numa visão holística da cooperação policial e de valores de reciprocidade e solidariedade entre os Estados-Membros. Ao contrário do discurso político que iniciou o debate acerca da adesão ao sistema Prüm com a emergência de uma corrente cujo objetivo foi o de analisar se o saldo dos benefícios de Prüm para o Reino Unido era positivo em relação aos custos da sua implementação. A par com a instrumentalização política do sistema Prüm, no extrato, o/a entrevistado/a traz à discussão três pontos para compreender a postura do Reino Unido face a este sistema. Primeiro, a noção de que Prüm só seria útil se ajudasse os cidadãos britânicos a estarem mais seguros, ideal materializado na suspeição e criminalização do outro (Aas, 2011; Aas & Bosworth, 2013), onde ‘o outro não fala inglês’ (D02). Segundo, o medo de se moverem ações judiciais contra cidadãos britânicos fora fronteiras por crimes que no plano nacional não usufruam da mesma moldura penal. Terceiro, a falta de confiança em relação aos sistemas policiais e judiciais dos restantes países da União Europeia (Hufnagel & McCartney, 2015), aquilo a que o/a entrevistado/a nomeia de ‘ponto de vista ativista’.

“Os desafios às liberdades civis trazidos por Prüm não me parecem ser Prüm em si mesmo, mas (...) baseados no medo e suspeição do outro, onde o outro não fala inglês (...), e o medo de que alguém possa ser preso (...) por algo que não constitui uma ofensa criminal em Inglaterra (...). Ainda há, claro, o ponto de vista ativista: a suspeição de que todo o sistema de justiça criminal que não esteja sob a alçada da Rainha é profundamente dúbio, por isso, nenhum *Englishmen* deveria enfrentá-lo. (...) Em termos de diálogo há pouca discussão acerca do contexto europeu, mas uma identidade nacional particular emergiu neste debate. (...) Mas, realmente, só se focou em resolver crimes cometidos aqui, no Reino Unido.” [D02-entidade de supervisão/regulação]

O aumento dos falsos positivos como consequência do aumento do volume de informação partilhada (Krimsky & Simoncelli, 2011; McCartney, 2014a; Toom, 2018) foi um dos desafios éticos elencados por parte dos participantes que desenvolvem atividades no

âmbito de entidades de supervisão. No entanto, um/a dos/as entrevistados/as desta categoria profissional não considera esta questão demasiado problemática. O sistema de confirmação de correspondências entre perfis de DNA em conjugação com os métodos tradicionais de investigação (Miranda, 2015) poderão ser suficientes para evitar erros que levem pessoas às malhas da justiça com base em informações erradas.

“[Em Prüm] os falsos positivos aumentam. (...) No entanto, penso que isto não será um grande problema, uma vez que é necessária uma análise para a confirmação. E acredito que, em conjunto com provas circunstanciais do caso, não existirão assim tantas situações em que apareçam *hits* onde é provável que o perfil não tenha vindo do perpetrador do crime. Porque, se houver um crime que aconteceu em Portugal e a pessoa estava na Dinamarca naquela altura, então, é o fim da história.” [D06-entidade de supervisão/regulação]

Os entrevistados a desempenhar funções em ONGs apontam os erros na justiça, a falta de transparência na implementação do sistema Prüm e a (des)confiança entre Estados-Membros como os pontos mais debilitantes deste sistema. Os falsos positivos são uma preocupação comum a todos os entrevistados do estudo e podem ocorrer devido à falta de regras standardizadas na cadeia de custódia, à contaminação de amostras no ato de recolha ou análise da prova e devido à interpretação errada de resultados da prova genética no âmbito da investigação criminal (Krimsky & Simoncelli, 2011; McCartney, 2004, 2006b; Murphy, 2007, 2018; Toom, 2018). No excerto que se segue, um dos elementos de uma ONG refere a preocupação com o número de *loci* para a comparação de perfis de DNA, sendo um ponto comum ao exposto nos relatórios subsequentes à avaliação da implementação do sistema Prüm no Reino Unido (Council of the European Union, 2017, 2018b). Numa segunda fase, elenca a falta de procedimentos standardizados nas práticas de recolha de prova e na cadeia de custódia que antecedem a análise laboratorial. Sendo que, a harmonização técnico-científica sugerida pelo/a entrevistado/a atua como garante de boas práticas no decorrer da obtenção da prova genética com o objetivo de neutralizar as diferenças legais, culturais, científicas e políticas dos Estados-Membros (Lampland & Star, 2009, pp. 4–5; Prainsack & Toom, 2010, 2013).

“Têm havido preocupações a respeito de erros na justiça, particularmente devido ao critério que foi estabelecido para o número de *loci* (...), mas não há um sistema pan-europeu que assegure a qualidade da cena do crime ou da cadeia de custódia [da prova] da cena de crime até ao laboratório. (...) Penso que poderão existir alguns casos de contaminação ou de falsos positivos (...) e não estou convencido de que serão detetados. (...) Por isso, em alguns países é exigida a corroboração da prova antes do processo [em tribunal]. (...) Esta exigência é feita por todos os países europeus? Não sei, desconfio que não.” [D05-ONG de direitos humanos]

A estabilidade e credibilidade do sistema Prüm é garantida através da prestação de contas, da transparência e da confiança entre Estados-Membros (Santos & Machado, 2017). No entanto, a supervisão insuficiente dos fluxos de informação à escala transnacional, através do sistema Prüm, dificultam o compromisso de transparência, sendo que grande parte dos cidadãos não está a par dos desafios da partilha de dados entre países (McCartney, 2014a). Neste sentido, a construção de estatísticas mais robustas sobre as informações pessoais partilhadas transnacionalmente e em que condições a partilha é, ou não, efetuada foi uma das soluções apontadas para uma melhor supervisão (Santos & Machado, 2017; Wilson, 2016). Ao nível nacional/local também se coloca a questão da transparência na implementação de Prüm, esta questão é destacada por um dos/as entrevistados/as de uma ONG que se mostra preocupado/a com a falta de transparência durante o processo. No excerto apresentado, dá conta de uma curta interação com o Governo que terminou sem que as questões fossem esclarecidas. Numa tentativa de compreender o papel das entidades de supervisão, contactou algumas delas e foi informado/a de que estas não estavam diretamente envolvidas no processo de implementação do sistema Prüm. Na sua perspetiva, a mera presença em reuniões dirigidas a *stakeholders* e o não envolvimento direto das entidades responsáveis pela supervisão da base de dados forense nacional nos processos de implementação do sistema Prüm contribuem ativamente para a falta de transparência pública.

“Não estou a ver nenhuma transparência [risos]. Escrevemos ao Governo e foi-nos dito: ‘Mas vocês estiveram na reunião dos *stakeholders* antes da decisão,

deveriam estar felizes' [risos]. O que não foi o suficiente. Falei com [outros órgãos de supervisão] e, neste momento, não estão diretamente envolvidos, penso que deveriam estar. Portanto, não há uma transparência efetiva sobre o que está a acontecer com a implementação." [D05-ONG de direitos humanos]

No extrato abaixo apresentado, o/a entrevistado/a, a desempenhar funções numa ONG, mostra-se igualmente apreensivo/a com a possível falta de supervisão das forças policiais/judiciais responsáveis pela gestão local das bases de dados forenses nacionais. Sendo que a implementação do sistema Prüm é rigorosa tanto ao nível técnico (acreditação de laboratórios, etc.), como ao nível da proteção de dados garantida pela estrutura de dois passos (Prainsack & Toom, 2010). No entanto, considera que o rigor do sistema Prüm também se encontra dependente da fiabilidade das autoridades policiais/judiciais no plano nacional que deve ser assegurada por entidades de supervisão. Supervisão essa que pode não ser suficiente para as atividades desenvolvidas pelas forças policiais/judiciais e pela partilha de dados pessoais no sistema Prüm, situação que conduz à transnacionalização de erros judiciais. Portanto, ao nível macro depreende-se que o sistema em si equacionou adequadamente a necessidade de standardização técnica ao nível laboratorial e a importância da proteção dos dados pessoais das pessoas envolvidas na partilha de informações. Contudo, as contingências locais, no plano micro, influenciam a eficácia de todo o sistema.

"A rede de Prüm não está totalmente completa, mas não tem havido grande supervisão ao nível europeu sobre o que tem sido feito com o sistema. Quer dizer, o processo pelo qual os Estados-Membros têm que passar para participar é bastante rigoroso tanto em termos técnicos, como do ponto de vista da proteção de dados. As leis estão em vigor, a supervisão a funcionar, etc. Também se aplica às autoridades nacionais, à fiabilidade das autoridades policiais nacionais. Em que condições recolhem o DNA. (...) É uma questão de confiança nas autoridades policiais nacionais e se os sistemas que estão previstos para a supervisão ao nível nacional são suficientemente rigorosos. (...) Suponho que o problema é que as autoridades responsáveis provavelmente não estão sujeitas a tanta supervisão quanto as pessoas poderiam esperar." [D16-ONG de direitos humanos]

Envolvimento das entidades de supervisão no sistema Prüm

O envolvimento das entidades de supervisão das atividades da NDNAD no grupo de trabalho formado para discutir a implementação do sistema Prüm no Reino Unido é apreendido de diferentes modos de acordo com as categorias profissionais dos entrevistados. Por um lado, as narrativas dos entrevistados pertencentes a órgãos de investigação criminal, como demonstra o extrato abaixo, pautam-se pelo imaginário pragmático de que as entidades de supervisão têm como função ‘mostrar ativamente que o que está a ser feito é justo e proporcional’ (D04). Numa perspetiva menos explícita está presente a noção de que a partilha de dados pessoais no Reino Unido reúne todas as condições de justiça e proporcionalidade, onde o papel das entidades de supervisão se cinge à demonstração pública destas características e não à participação ativa na redução de potenciais desafios.

“Partilhamos dados que são considerados sensíveis e pessoais. Sentimos, e o Parlamento concordou, que seria importante podermos mostrar que isto está a ser feito de forma justa, eficiente e efetiva. Da mesma forma, existe um *national DNA database Strategy* previsto na legislação, o governo achou que era importante mostrarmos que estávamos a fazer as coisas de maneira apropriada. Portanto, é para isso que serve o órgão de supervisão: para mostrar que estamos, efetivamente, a ser justos e adequados.” [D04-órgão de investigação criminal]

Por sua vez, verifica-se um consenso geral entre os participantes a desempenhar funções em entidades de supervisão/regulação quanto ao diminuto envolvimento destas entidades no processo de implementação do sistema Prüm. No primeiro excerto, é referido que no decorrer do processo de implementação do sistema Prüm, a entidade de supervisão para a qual trabalha foi apenas informada das decisões tomadas, não tendo um papel tão visível como o que seria de esperar. No segundo extrato, constata-se novamente o pouco envolvimento das entidades de supervisão na implementação do sistema Prüm. Neste sentido, o/a entrevistado/a realça que o papel da supervisão se encontra num estado embrionário, pelo que existem vários tópicos não esclarecidos em relação às funções a serem desempenhadas no sistema Prüm.

“O [órgão de supervisão] deveria ter sido mais envolvido. Não nos foi realmente perguntado, fomos informados. E acho que isso é uma pena.” [D06-entidade de supervisão/ regulação]

“Penso que deveria ser transparente. Concretamente, como é que os elementos de Prüm e como é que a sua gestão funcionaria, não sei qual é o papel que o [órgão de supervisão] teria nisto. Parece fazer sentido ter esta estrutura e supervisionar também a partilha em Prüm, o que lhe daria transparência.” [D07-entidade de supervisão/regulação]

Os entrevistados afetos a ONGs são igualmente críticos da falta de clarificação dos mecanismos que permitirão o escrutínio das atividades de partilha de informação pessoal transnacional. No entanto, atribui-se parte das incertezas, que ainda não foram esclarecidas em relação ao sistema Prüm, à conjuntura política em que o Reino Unido se encontrava quando foi aplicada esta entrevista, nomeadamente, na negociação da sua saída da União Europeia devido ao *Brexit* (Wilson, 2016).

“O escrutínio extra da implementação de Prüm que o governo prometeu no parlamento não tem um mecanismo claro. Por isso, em relação a Prüm, acho que ainda não é óbvio quem é que está a supervisionar ou se será publicamente debatido. Mas, devido ao referendo da UE, isto tem, obviamente, algum nível de incerteza adicional e, pode ser, que depois, algumas coisas fiquem mais claras.” [D05-ONG de direitos humanos]

Implicações do contexto político do Brexit no sistema Prüm

As preocupações e incertezas oriundas das negociações políticas que se encontram em andamento devido ao *Brexit* foram expressas por diversas ocasiões durante a realização das entrevistas. Esta situação revela explicitamente a dimensão política e social do sistema Prüm que não é apenas uma mera ferramenta tecnológica com o objetivo de auxiliar a detenção e deteção do crime. Como já foi referido existem várias vozes críticas à saída do Reino Unido da União Europeia e à não adesão ao sistema Prüm (House of Lords, 2013; McCartney, 2013). Os entrevistados, de forma geral, também se revelam muito críticos da

classe política do Reino Unido que foi responsável por estas decisões. Neste sentido, um dos tópicos que gerou preocupação veio nas palavras de um/a dos/as geneticistas forenses entrevistado/a, cuja entrevista foi aplicada após a votação do *Brexit*. Considerando que a acreditação dos laboratórios é uma das obrigações a ser cumprida pelos países do sistema Prüm (Jornal Oficial da União Europeia, 2008), a saída da União Europeia e de todos os trâmites legais e burocráticos associados a par com a resistência das forças policiais pode atrasar a acreditação.

“Eu acho para além do Brexit o maior [desafio] para mim é a acreditação. (...) Já estamos atrasados no tempo. (...) E há muita resistência por parte das forças policiais, porque têm que pagar por isto. E os orçamentos estão a ser cortados. (...) Por isso, politicamente, haverá muito mais resistência das forças policiais. (...) Acho que isso pode ter impacto.” [D10-geneticista forense]

O *Brexit* serviu também de plataforma para a reflexão sobre os valores de união da União Europeia. Na perspetiva de um/a dos/as entrevistados/as, a desempenhar funções num órgão de supervisão/regulação, a postura do Reino Unido tem sido a de aproveitar da União Europeia as ferramentas que lhe são mais convenientes após a análise de custo-benefício ao nível nacional. Apesar de concordar com a adesão ao sistema Prüm, este/a entrevistado/a, à semelhança da maioria dos participantes, foi muito crítico/a da morosidade com que a decisão foi tomada. Constatando-se que institucionalmente o discurso tem sido revestido por uma tensão entre os interesses nacionais do Reino Unido e os objetivos comuns da União Europeia (House of Commons Hansard Debates 2013; House of Lords, 2013; McCartney, 2013). O imaginário acerca da relevância política de sistemas como o de Prüm não é coincidente entre os entrevistados e o discurso político inicial que foi responsável pela opção de não entrar na partilha de informações ao nível transnacional. De modo latente, no extrato, identifica-se ainda uma tendência do Reino Unido em querer sair da União Europeia, mas, em simultâneo, de continuar a usufruir das ferramentas e diretrizes de vigilância e detenção do crime. No extrato é referido o ‘medo do *Brexit*’ pois, a entrevista ocorreu meses antes da votação do referendo.

“Acho que o Reino Unido está a optar muito rápido pela entrada [em Prüm] por causa do medo do Brexit. E acho que é absolutamente horrível que o Reino Unido demore tanto para tomar uma decisão e a veja como algo que deve ser precedido por uma análise de custo-benefício. Porque se fazemos parte da UE, fazer este tipo de coisas sem fazer uma análise própria de custo-benefício é o que deve ser feito. É suposto fazermos parte desse sistema. Então, estou feliz por estarmos a decidir entrar. (...) Às vezes, acho que os *stakeholders* no Reino Unido, incluindo o Primeiro Ministro e outras pessoas, não entendem o que é a União Europeia. E não entendem a relevância política de algo como Prüm.” [D06-entidade de supervisão/regulação]

Um/a dos/as entrevistados/as, a desempenhar funções numa ONG de Direitos Humanos, enfatiza que o modelo europeu de controlo do crime e do terrorismo verteu, em muitos aspetos, da estratégia escolhida pelo Reino Unido. Em particular, a utilização de bases de dados forenses de perfis de DNA para detenção do crime foi uma das medidas adotadas pela União Europeia, em 2008, através das Decisões Prüm (Union, 2008), ao passo que o Reino Unido já possuía uma base de dados forense nacional desde 1995. Neste sentido, a NDNAD tem sido apontada como o modelo ao qual os restantes Estados-Membros têm recorrido para a criação das suas bases de dados forenses nacionais (Johnson & Williams, 2007, p. 106). No que concerne à relação entre o Reino Unido e a União Europeia, o/a entrevistado/a refere que apesar da saída do espaço da UE, o país tentará fazer parte dos sistemas de informação existentes no âmbito da atuação policial/judicial.

“No que diz respeito ao controlo da criminalidade, ou em relação ao combate ao terrorismo em particular, a estratégia contraterrorismo da UE é basicamente uma cópia da estratégia do Reino Unido, embora aplicada num contexto muito diferente. (...) Assim, percebe-se como o Reino Unido teve uma enorme influência nas políticas e práticas da UE no que diz respeito ao crime e ao terrorismo. (...) No que diz respeito aos interesses do Reino Unido ao nível da UE, é tudo o *Brexit*, não é? Basicamente gostariam de ficar em tantos sistemas de informação quanto possível, mas ninguém sabe se serão capazes.” [D16-ONG de direitos humanos]

Sintetizando, as percepções dos entrevistados em relação às vantagens do sistema Prüm têm certos pontos em comum com todas as categorias profissionais analisadas. Neste sentido, os pontos de consenso entre os participantes dizem respeito à maior rapidez e eficiência na resolução do crime e no melhoramento da cooperação transnacional. Em particular, os geneticistas forenses demonstraram-se muito críticos do contexto político atual, com o *Brexit*, bem como da instrumentalização do sistema Prüm para reduzir o crime nacional cometido por estrangeiros. Os entrevistados dos órgãos de investigação criminal focaram-se, tendencialmente, na capacidade de produção de inteligência através do sistema Prüm, sendo que as suas narrativas se voltaram maioritariamente para a instrumentalização da base de dados forense. Na categoria que remete para as entidades de supervisão/regulação, os entrevistados revelaram uma visão mais holística do sistema Prüm e foram críticos da não cooperação devido à falta de reciprocidade de valores, crítica também subjacente às narrativas dos geneticistas forenses. Os participantes das ONGs de direitos humanos, realçaram as salvaguardas que o sistema Prüm oferece à proteção de dados através do mecanismo de dois passos.

Os desafios da implementação do sistema Prüm também gozaram de algum consenso, principalmente quanto à necessidade de evitar falsos positivos devido à grande amplitude na partilha de dados. De modo mais pormenorizado, os geneticistas forenses exploraram as diferentes tradições judiciais e a existência de *standards* científicos diferenciados consoante os Estados-Membros como os desafios mais prementes no sistema Prüm. Os participantes dos órgãos de investigação criminal revelaram uma racional mais associada ao custo-benefício deste tipo de infraestruturas. Posto isto, referiram que os outros países retirariam mais benefícios da base de dados do Reino Unido do que o inverso, associando-se também o elevado dispêndio de recursos devido ao tamanho da NDNAD como desafios inerentes ao sistema Prüm. Na categoria entidade de supervisão/regulação as preocupações expressas pelos entrevistados foram, ainda que num tom diferente, semelhantes às da categoria profissional anterior. Para estes participantes os desafios de Prüm passam pelo potencial aumento do fluxo de trabalho no segundo passo que, por sua vez, se encontra associado à dimensão da base de dados e aos custos associados ao reforço desta atividade. Os elementos de ONGs de direitos humanos mostraram-se preocupados com a possível transnacionalização de erros judiciais (contaminação, etc.) potenciados pela escassez de harmonização de procedimentos na cadeia de custódia das provas entre

Estados-Membros. Ainda nesta categoria, os entrevistados criticaram a falta de transparência no processo de implementação do sistema Prüm no contexto nacional, bem como a (des)confiança entre os países da União Europeia.

O envolvimento das entidades responsáveis pela supervisão das atividades da NDNAD na implementação de Prüm revelou uma clivagem entre as perspetivas dos entrevistados dos órgãos de investigação criminal e dos participantes a desempenhar funções em entidades de supervisão/regulação e ONGs de direitos humanos. Se, por um lado, o primeiro grupo não considerou existirem problemas de maior relativamente à supervisão realizada a Prüm. Por outro lado, no segundo grupo, enfatizou-se o papel passivo que as entidades de supervisão adquiriram nas reuniões acerca do sistema Prüm, bem como a falta de clarificação sobre os modos como a supervisão poderá escrutinar as atividades deste sistema. Num último ponto, os elementos de ONGs elencaram a falta de supervisão ao nível nacional, das forças policiais e das bases de dados forenses dos Estados-Membros como debilitantes da confiança entre países.

Em relação às preocupações com as consequências do *Brexit*, os geneticistas forenses mostraram-se receosos com os potenciais atrasos na acreditação dos laboratórios forenses. Os entrevistados enquadrados na categoria profissional de entidade de supervisão/regulação e ONGs de Direitos humanos partilharam a mesma crítica em relação ao contexto político vivido atualmente no Reino Unido. No seu entender, o país tentará continuar em todos os sistemas de informação e de vigilância que lhe forem permitidos, sempre numa racional de custo-benefício para o contexto nacional.

Interoperabilidade entre bases de dados forenses e biobancos

Uma das perguntas do guião de entrevista aplicado visou obter as perspetivas dos participantes em relação à potencial interoperabilidade entre bases de dados forenses de perfis de DNA e biobancos para fins de investigação/diagnóstico médico. Deste modo, as narrativas serão analisadas a partir das categorias analíticas de ‘negação técnico-legal’, ‘interoperabilidade pela excecionalidade’, ‘negação pela finalidade’ e, por fim, ‘interoperabilidade pela expansão’ (consultar página 120 para o aprofundamento de cada categoria). Genericamente, os entrevistados das várias categorias profissionais revelam-se pouco favoráveis à interoperabilidade das bases de dados do campo forense e do campo médico. No primeiro extrato apresentado, um/a dos/as geneticistas forenses considera que

a interoperabilidade nestes termos não é um procedimento ético pois aproxima dois campos com finalidades totalmente diferentes, sendo que os erros possuem também consequências distintas para os indivíduos (Gaskell et al., 2013; Machado & Silva, 2015a, p. 820; Santos et al., 2013). Um erro ao nível forense pode colocar um inocente na prisão, ao passo que um erro de diagnóstico não tem resultados tão gravosos. Ao referir que os profissionais a operar no campo forense estão a par das incongruências que ocorrem no seio dos biobancos médicos é defendido, implicitamente, que as bases de dados forenses oferecem maior proteção na inserção de dados pessoais de foro genético.

“Acho que isso [interoperabilidade] seria antiético. Não gostaria de o fazer. Acho que, no campo forense, estamos todos cientes dos erros das bases de dados de diagnóstico, estes erros não são importantes em medicina. Mas se se vai colocar alguém na prisão (...) não se pode cometer um erro.” [D09-geneticista forense]

O princípio da limitação da finalidade da recolha de dados pessoais foi um dos tópicos trazido à discussão acerca da interoperabilidade entre campo médico e forense. O não respeito por um dos princípios gerais da proteção de dados – limitação da finalidade – pode conduzir a situações potencialmente danosas para os indivíduos cujos dados constam em biobancos através da *function creep* que deriva deste tipo de conduta (Dahl & Sætнан, 2009; Liu, 2013, p. 66). No extrato apresentado, apesar de não clarificada a perspetiva do/a entrevistado/a a respeito da interoperabilidade entre bases de dados é assumido que esta consistiria no acesso forense a bases de dados médicas e não o inverso. Neste caso, o obstáculo colocar-se-ia ao nível do acesso legal a dados médicos no âmbito de uma investigação criminal.

“Acho que o problema é que quando as pessoas dão amostras para investigação médica, não estão a consentir realmente que a amostra seja testada para uma investigação criminal. (...) Acho que precisaria de permissão de um juiz.” [D11-geneticista forense]

Tendo em consideração a categorização proposta anteriormente, as narrativas dos geneticistas forenses a respeito deste ponto situam-se nas categorias analíticas de ‘negação

pela finalidade’ e de ‘negação técnico-legal’. No primeiro grupo, encontram-se as perspectivas que são robustecidas com reflexões éticas sobre as diferentes consequências que permeiam a utilização das bases de dados forenses e dos biobancos. No segundo grupo, enquadram-se os entrevistados que não tecendo uma posição clara a respeito avançam com aspetos legais que inviabilizam esta prática.

Na mesma linha, o/a entrevistado/a de um órgão de investigação criminal refere que esta prática não é permitida no Reino Unido. Apesar de também não ter demonstrado a sua perspectiva acerca da interoperabilidade entre bases de dados forenses e médicas, refere quais os potenciais obstáculos à mesma em termos práticos. Deste modo, clarifica que os diferentes *standards* científicos para a inserção de informação genética em ambos os tipos de bases de dados podem condicionar inevitavelmente a interoperabilidade. Dito isto, numa base de dados forenses só pode constar informação a respeito da parte não codificante do DNA (Balzacq et al., 2006, p. 14), ao passo que nos biobancos os dados genéticos armazenados e analisados são, na sua maioria, da parte codificante do DNA.

“A resposta para isso, no Reino Unido, é absolutamente ‘não’ e continuará a ser absolutamente ‘não’. (...) Nem sei se um genoma completo é realmente compatível com um perfil de DNA de uma cena de crime. Não esqueçamos que o perfil de DNA de uma cena do crime é retirado do DNA não-codificante. O ponto principal deste tipo de bases de dados de DNA é que estão a decodificar o DNA.”
[D04-órgão de investigação criminal]

Posto isto, as narrativas dos elementos dos órgãos de investigação criminal dizem respeito à categoria de ‘negação técnico-legal’ por avançarem com argumentos de carácter técnico e científico para justificar a não realização da interoperabilidade. Este tipo de posicionamento vem de algum modo contrariar uma racional policial que se caracteriza pela primazia na produção de inteligência através de todas as fontes disponíveis (Innes et al., 2005). No entanto, o baixo número de entrevistas realizadas a elementos dos órgãos de investigação criminal pode estar na origem da presente discrepância entre a narrativa dos entrevistados e o modo de atuação que lhe é atribuído na literatura.

No excerto apresentado, o/a entrevistado/a, a desempenhar funções numa entidade de supervisão/regulação, concorda com a postura pública desfavorável à interoperabilidade

entre bases de dados forenses e biobancos. O aumento da pressão para o acesso policial a todas as bases de dados, identificado pelo/a entrevistado/a, tem que ver com três pontos associados ao desenvolvimento de infraestruturas técnico-científicas deste tipo. Primeiro, com o aumento da capacidade de armazenamento de informações. Segundo, com o aumento exponencial da velocidade do fluxo de dados partilhados. E, terceiro, com a simplificação dos processos de cruzamento de dados devido à tentativa de standardização dos vários sistemas (Goos et al., 2015, p. 56; Mostert et al., 2017; Nissenbaum, 2010, p. 36). O/a entrevistado/a identifica um último argumento que poderá ser elencado pelas polícias para a justificação da interoperabilidade entre o campo médico e forense que remete para a ideia de que o cidadão cumpridor da lei que não tenha nada a esconder não deve temer esta prática. A neutralização da discussão ética acerca da proteção de dados e da privacidade, bem como do possível desvirtuamento dos objetivos de solidariedade e altruísmo que sustentam os biobancos (Machado & Silva, 2015b) é realizada através da premissa de ‘nothing to hide, nothing to fear’ (Crossman, 2008, p. 116).

“Neste momento, seria inaceitável. E parece ser uma visão razoavelmente ampla, mas haverá inevitavelmente uma pressão crescente, uma tentação crescente, por parte das autoridades, de querer aceder a todo o tipo de bases de dados. E, claramente, seriam estes a dizer convictamente: ‘Por que não? Se não fez nada de errado, não tem nada com que se preocupar (...)’.” [D03-entidade de supervisão/regulação]

Os participantes afetos a entidades de supervisão/regulação situam o seu posicionamento sobre a interoperabilidade na categoria de ‘negação pela finalidade’. Pelo que, mostram a sua preocupação quanto à constante pressão exercida pelas forças policiais para o acesso a todas as bases de dados disponíveis.

Por fim, um/a dos/as entrevistados/as pertencente a uma ONG de direitos humanos, aborda a questão da interoperabilidade sob um prisma diferente. Neste sentido, discerne acerca da interoperabilidade dos sistemas de informação para a migração e segurança da União Europeia. Sendo que, atualmente, a União Europeia se encontra a trabalhar num sistema que pretende tornar interoperáveis bases de dados pré-existentes (Eisele, 2018), nomeadamente, o *Schengen Information System* (SIS), o EURODAC, o *Visa Information*

System (VIS), o Entry-Exit System (EES), o European Travel Information and Authorisation System (ETIAS), o European Criminal Records Information System (ECRIS), a Stolen and Lost Travel Documents database (SLTD-Interpol) e, por fim, o Europol Information System (EIS). Esta proposta encontra-se em fase de aprovação para que se conciliem os aspetos relativos ao seu funcionamento. A eu-LISA será a agência responsável pela gestão deste sistema de interoperabilidade entre as bases de dados já existentes e prevê-se que o sistema em causa esteja operacional em 2023. A este respeito o/a entrevistado/a denota, criticamente, que com a criação de um sistema desta amplitude ‘todas as pessoas se tornarão suspeitas’ (D16).

Na sua perspetiva, as medidas de proteção e segurança estatais começam com a premissa de que apenas são verificados os indivíduos que são externos ao espaço da União Europeia. Mais tarde, assiste-se à evolução para uma segunda fase em que começa a ser permitido que se verifiquem os cidadãos da UE em bases de dados policiais, sempre que pretendam atravessar as fronteiras. Para o/a entrevistado/a, o modo como os critérios de verificação se tendem a expandir conduz à suspeição generalizada de todas as pessoas, sejam ou não cidadãos da União Europeia, pelo facto de cruzarem as fronteiras.

“Não foi acordado, mas este sistema foi estudado pela Comissão [Europeia] ao longo dos anos para incluir todas as passagens de fronteiras dos cidadãos da UE. Já mudaram as regras sobre a verificação de cidadãos da UE em bases de dados da polícia quando atravessam as fronteiras. Então, sim, primeiro são os estrangeiros ou os outros, e a seguir são os próprios cidadãos. Então, no final, todas as pessoas se tornarão suspeitas.” [D16-ONG de direitos humanos]

O/a mesmo/a entrevistado/a considera que, mesmo que o sistema de interoperabilidade entre em atividade, é fundamental perceber que do ponto de vista legal a única informação disponível para acesso policial é a inserida pós criação da infraestrutura. Assim, tornar as informações pessoais, previamente inseridas nos diversos sistemas de informação disponíveis, vai contra um dos princípios da proteção de dados, nomeadamente, o princípio da limitação da finalidade. As relações de poder assimétricas impressas no meio político-social entre o Estado e as ONG são identificadas como uma das dificuldades para a defesa dos direitos civis em práticas governamentais deste tipo. Acrescendo o facto de que,

segundo o/a entrevistado/a, os média encontram-se de modo mais ou menos explícito do lado do Estado e são responsáveis pela reprodução de estigmas e estereótipos em relação a determinadas populações de migrantes e refugiados. Tendo em consideração esta conjuntura política, defender os direitos de certas parcelas da sociedade pode apresentar-se como uma função de extrema dificuldade devido às assimetrias de poder implícitas no controlo dos sistemas de informação.

“Do ponto de vista legal, não há problema se tudo a partir desse ponto [da legalização do sistema] for disponibilizado à polícia. Mas, tudo o que houver antes disso e que não foi recolhido para esse propósito [não pode ser disponibilizado], ou está a violar-se um dos princípios básicos da proteção de dados. (...) Suponho que seja um desvirtuamento. (...) Desafiar este tipo de narrativa é difícil. Número um, porque estamos sempre por trás de organizações civis que tentam desafiar as atividades do governo porque é muito mais poderoso do que nós, ele [governo] tem os média do seu lado. (...) E é muito difícil, por causa da hostilidade geral em grandes secções dos média em relação aos migrantes e refugiados (...), defender os seus direitos, com medidas como esta.” [D16-ONG de direitos humanos]

No que diz respeito à interoperabilidade entre as bases de dados forenses e os biobancos médicos, os geneticistas forenses consideram que este tipo de prática não respeita os critérios de ética. Por um lado, através de uma avaliação dos riscos do acesso forense a biobancos, pela defesa de que a ocorrência de erros iria aumentar devido às características das bases de dados médicas, potenciando a identificação de pessoas inocentes num contexto criminal. Por outro lado, pela constatação de que a prática não está em concordância com princípio da proteção de dados da limitação da finalidade da recolha e utilização dos dados armazenados. Os/as entrevistados/as enquadrado na categoria órgão de investigação criminal não demonstram a sua posição em relação à interoperabilidade, mas indicam que os diferentes *standards* na codificação dos dados que são inseridos em ambas as plataformas seriam um obstáculo à sua realização. Por fim, um/a dos/as entrevistados/as pertencentes a um dos órgãos de supervisão/regulação mostra-se pouco favorável à prática da interoperabilidade entre bases de dados forenses e biobancos.

Contudo, alerta para a expansão tendencial que se tem observado no acesso a dados pessoais concedido às polícias.

O/a entrevistado/a de uma das ONGs de Direitos Humanos remete a sua resposta para uma infraestrutura, atualmente a ser debatida na UE, com o objetivo de tornar interoperáveis os sistemas de informação pré-existentes para a migração e segurança no espaço da União Europeia. Refere, por um lado, que sistemas desta amplitude contribuem para a coletivização da suspeição de todos os cidadãos e não cidadãos a circular na União Europeia. Por outro lado, reflete sobre o poder estatal e as dificuldades que uma organização civil enfrenta para defender os direitos das pessoas numa clara desvantagem em termos de poder e de representação nos média.

4.3. Perspetiva comparativa entre Portugal e o Reino Unido: o papel dos imaginários sociotécnicos

Os discursos sobre o risco têm colocado pressão nos países no sentido de melhorar a proteção e segurança dos seus cidadãos. Sendo que as noções de risco e do que é o risco vêm muitas vezes acompanhadas de ideários de vigilância expansiva sobre os indivíduos. Sob este panorama a apropriação da tecnologia e a criação de projetos que visam precisamente a dissipação do risco não calculável por parte dos Estados possui diferentes práticas, políticas e aceitação dos cidadãos. Neste caso em particular, conceito de imaginários sociotécnicos permite discernir os imaginários acerca da ordem social e do que é prioritário em relação à diminuição dos fatores de risco. Deste modo, a última secção do capítulo pretende tornar visíveis os imaginários sociotécnicos que decorrem da análise das narrativas dos geneticistas forenses e *stakeholders* de Portugal e do Reino Unido de modo a compreender os seus pontos em comum e os que diferem entre contextos nacionais. Posto isto, a mobilização do conceito de imaginários sociotécnicos (Jasanoff & Kim, 2009) afigura-se relevante para o estudo de um mesmo fenómeno, o sistema Prüm, que ocorre em países diferentes. O conceito é igualmente útil no âmbito deste estudo uma vez que possui a sensibilidade necessária para alcançar e identificar as múltiplas narrativas que permeiam este fenómeno tecnológico e científico (Pfotenhauer & Jasanoff, 2017, p. 783).

O conceito de imaginários sociotécnicos possui uma dimensão flexível e mutável que reconhece o carácter democrático que acompanha a formação de políticas. Por este motivo, a criação de políticas é permeável a mais do que um imaginário sociotécnico a respeito da

produção de conhecimento científico e da aplicação de uma determinada tecnologia (Jasanoff & Kim, 2009; Kim, 2018, pp. 177–178). No entanto, o Estado continua a ser o ator central na disputa daqueles que serão os imaginários sociotécnicos vigentes na sociedade. Esta assimetria de poderes entre o Estado e os restantes atores sociais deve-se ao facto de este controlar grande parte dos meios de produção de significados, nomeadamente, através da realização de campanhas políticas e dos discursos plasmados nos diversos documentos oficiais (Jasanoff & Kim, 2009). Dito isto, neste estudo, propõe-se uma análise mais aprofundada que englobe não só o nível macro nacional (discurso político), como também um nível micro representado pelas narrativas dos geneticistas forenses e dos *stakeholders* de Portugal e do Reino Unido. A expansão da utilização do conceito pauta-se pelo facto de que, *grosso modo*, as perceções sobre as vantagens e desafios do sistema Prüm, por exemplo, não serem coincidentes entre entrevistados com formações e profissões diferentes. Sendo que, também os desafios elencados pelos entrevistados em relação à utilização de bases de dados de DNA serem tendencialmente diferentes de acordo com a sua formação académica e profissional.

As tabelas 7. e 8. que surgem ao longo da presente secção têm como objetivo guiar o leitor ao longo da comparação dos imaginários sociotécnicos dos dois estudos de caso. Na tabela 7. encontram-se identificadas as narrativas dominantes dos geneticistas e dos *stakeholders* de Portugal e do Reino Unido no âmbito das bases de dados forenses de perfis de DNA, das vantagens e dos desafios de Prüm, das questões de privacidade e proteção de dados das bases de dados forenses e, por último, da interoperabilidade entre bases de dados forenses e biobancos. As informações constantes nesta tabela vertem unicamente das narrativas identificadas nas entrevistas realizadas. A tabela 8. pretende dar conta das características específicas de Portugal e do Reino Unido relativamente aos aspetos técnicos e legais das bases de dados forenses, bem como dos moldes em que ocorre a cooperação transnacional através do sistema Prüm. Os dados presentes na tabela foram obtidos através de documentos oficiais de ambos os países e das entrevistas realizadas.

Tabela 7-Comparação entre geneticistas forenses e stakeholders de Portugal e do Reino Unido em relação às bases de dados forenses de DNA, à cooperação transnacional e à interoperabilidade entre bases de dados forenses e biobancos

	Portugal	Reino Unido (Inglaterra e País de Gales – NDNAD)
	Bases de dados forenses de perfis de DNA	
Geneticistas forenses	- Falta de potencial utilitário - Neutralização dos riscos éticos/escassa reflexão - Proteção de dados com recurso a tecnologia: encriptação + restrição de acessos + análise da região não-codificante do DNA	- Sobre-representação de minorias - Sobrevalorização da prova genética (potencial) - ‘Pragmatismo biométrico’ (Williams & Johnson, 2004b)
Supervisão/ regulação	- Processo expansivo - Falta de interesse político - Tradição jurídica conservadora/ legislação restritiva - Adequação das medidas legais de proteção de dados - Supervisão adequada - Limitação dos dados trocados no sistema Prüm	- Atualização necessária do enquadramento ético (físico/moral)
Investigação criminal	- Falta de potencial utilitário - Neutralização dos riscos éticos/escassa reflexão - Proteção de dados com recurso a tecnologia: restrição de acessos	- Adequação das medidas legais de proteção de dados - Neutralização dos riscos éticos/escassa reflexão
Professor(a)/ investigador(a)	- Equilíbrio entre direitos civis e segurança coletiva	---
ONGs	---	- Crítica à expansão constante das bases de dados - Crítica à introdução de novas tecnologias por motivos comerciais
	Vantagens do sistema Prüm	
Geneticistas forenses	- Acompanhar a inovação - Estandardização técnica = + confiança e + responsabilidade	- Estandardização técnica = + confiança e + responsabilidade
Supervisão/ regulação	- Acompanhar a inovação - Gestão do risco	- Avanços na cooperação - Automatização e celeridade - Estandardização técnica = + confiança e + responsabilidade
Investigação criminal	- Acompanhar a inovação - Produção de inteligência	- Avanços na cooperação - Automatização e celeridade - Detecção de crime cometido por estrangeiros - Produção de inteligência
Professor(a)/ investigador(a)	- Acompanhar a inovação	---
ONGs	---	---
	Desafios do sistema Prüm	
Geneticistas forenses	- Tensões locais e globais - Falta de estandardização legal (<i>standard</i> de privacidade) - Passo 2: lei muito restritiva + custódia	- Tensões locais e globais - Falta de estandardização legal (<i>standard</i> de privacidade) - Falta de estandardização técnica (nas

	judicial	bases de dados nacionais) - Falsos positivos - Desvirtuamento da utilização dos dados
Supervisão/ regulação	- Passividade política na implementação - Falta de standardização legal (<i>standard</i> de privacidade) - Equilíbrio entre direitos civis e segurança coletiva - Fluxo de informação necessita de supervisão	- Elevado dispêndio de recursos financeiros - Falsos positivos: tamanho da base de dados forense - <i>Brexit</i> - Desconfiança entre Estados-Membros - Baixo envolvimento das entidades de supervisão na implementação
Investigação criminal	- Falsos positivos - Falta de standardização da cadeia de custódia - Cedência de dados vs disponibilidade da informação	- Elevado dispêndio de recursos financeiros - Aumento do volume de trabalho devido ao fluxo de informações: tamanho da base de dados forense - Falsos positivos: tamanho da base de dados forense
Professor(a)/ investigador(a)	- Equilíbrio entre direitos civis e segurança coletiva	---
ONGs	---	- Transnacionalização de erros judiciais - Falta de transparência - Desconfiança entre Estados-Membros - Falsos positivos - Falta de standardização da cadeia de custódia - Crítica à não clarificação dos mecanismos de escrutínio da informação trocada
Interoperabilidade entre bases de dados forenses e biobancos		
Geneticistas forenses	- Interoperabilidade pela excecionalidade	- Negação pela finalidade - Negação técnico-legal
Supervisão/ regulação	- Negação pela finalidade	- Negação pela finalidade
Investigação criminal	- Interoperabilidade pela expansão - Negação pela finalidade	- Negação técnico-legal
Professor(a)/ investigador(a)	- Negação pela finalidade - Interoperabilidade pela excecionalidade	---
ONGs	---	---

4.3.1 Imaginários sociotécnicos dos geneticistas forenses e stakeholders no contexto português

Os imaginários sociotécnicos a respeito dos projetos tecnocientíficos que levaram à criação das bases de dados forenses permitem explorar de que modo a aplicação da ciência na esfera legal (Pickersgill, 2011, p. 28) (re)configura as perceções dos geneticistas e dos *stakeholders* em relação aos mecanismos de vigilância. Em Portugal, os imaginários sociotécnicos a respeito das bases de dados forenses de perfis de DNA possuem pontos em comum entre grupos profissionais (tabela 7.). Para compreender os imaginários

sociotécnicos são avançadas duas categorias analíticas, respetivamente, ‘privacidade tecnológica’ e ‘privacidade ético-legal’. Deste modo, os geneticistas forenses e os elementos que desempenham funções em órgãos de investigação criminal focam os seus imaginários nas expectativas futuras da base de dados forense enquanto instrumento de identificação que ainda não alcançou o seu potencial utilitário. Estes imaginários dão primazia aos benefícios da inovação tecnológica e neutralizam os desafios éticos deste progresso através da ‘privacidade tecnológica’. A ‘privacidade tecnológica’ caracteriza-se pelo *black boxing* da privacidade e da proteção de dados por meio da tecnologia. Alguns exemplos desta ‘privacidade tecnológica’ dizem respeito à limitação de acessos, à encriptação de dados e à análise das regiões não-codificantes do DNA nas bases de dados forenses. Os elementos das entidades de supervisão/regulação e os professores(as)/investigadores(as) revelam um imaginário sociotécnico que acompanha o enquadramento dos benefícios da base de dados forenses. Porém, estes imaginários enfatizam a capacidade de gestão dos desafios éticos associados à utilização da tecnologia no contexto legal português. Em particular, através da ‘privacidade ético-legal’ que engloba as narrativas a respeito do equilíbrio entre os direitos civis e a segurança coletiva e a supervisão adequada das atividades da base de dados forense.

A criação do sistema Prüm enquanto projeto tecnocientífico transnacional da agenda securitária da União Europeia pretendeu que esta infraestrutura facilitasse o fluxo de informação entre Estados-Membros no âmbito da esfera policial e judicial. Em Portugal, os imaginários sociotécnicos dos geneticistas forenses e dos *stakeholders* são favoráveis à existência do sistema Prüm. Este estudo denomina estes imaginários enquanto ‘imaginários sociotécnicos de reciprocidade’, sendo que acompanhar a inovação tecnológica e a gestão do crime dos países considerados mais desenvolvidos possui um papel central para a legitimação desta ferramenta. Para além dos imaginários coletivos sobre os benefícios do sistema Prüm, estes grupos mobilizam de diferentes modos a sua formação profissional para identificar aqueles que são os contributos específicos desta plataforma. Deste modo, nos ‘imaginários sociotécnicos de reciprocidade’ englobam-se os benefícios associados à standardização técnica (geneticistas forenses), à gestão do risco (entidades de supervisão/regulação) e à produção de inteligência (órgãos de investigação criminal). Porém, em projetos tecnológicos desta amplitude, a sua universalidade pode entrar em conflito com as dinâmicas locais (Pfotenhauer & Jasanoff, 2017, p. 783).

Em Portugal, os mesmos atores identificam os fatores de desconexão que podem colocar em causa os ‘imaginários sociotécnicos de reciprocidade’ que revelam a respeito do sistema Prüm. Os pontos de tensão entre o local e o global são elencados à luz das especificidades das atividades que desenvolvem em torno deste sistema no país. Em particular, os geneticistas forenses elencam a este respeito a falta de standardização legal (*standard* de privacidade) e o caráter restrito da lei da base de dados nacional. Por outras palavras, estes profissionais assumem que ao nível técnico-científico a standardização existente permite a manutenção da universalidade do sistema, os desafios encontram-se ao nível das especificidades legais do país. Os elementos de entidades de supervisão/regulação partilham a mesma narrativa quanto ao enquadramento legal português. Num plano transnacional, identificam ainda que o imaginário da reciprocidade pode estar em causa devido à necessidade de uma maior supervisão do fluxo de dados que permita tornar mais adequado o equilíbrio entre os direitos civis e de segurança coletiva. Sendo o último ponto igualmente partilhado pelos professores(as)/ investigadores(as). Por fim, os elementos afetos aos órgãos de investigação criminal referem que a universalidade deste sistema tecnocientífico é colocada em causa pela ocorrência de falsos positivos, pela falta de standardização da cadeia de custódia e pela tensão entre os dados cedidos e a disponibilidade de informação. Posto isto, apesar de os grupos profissionais revelarem ‘imaginários sociotécnicos de reciprocidade’ a respeito do sistema Prüm apontam que a não standardização (que difere de acordo com o grupo profissional) de vários pontos da troca de dados pode condicionar o sucesso da implementação deste projeto tecnocientífico securitário.

Estudar as perspetivas sobre a possível interoperabilidade entre bases de dados forenses e os biobancos no âmbito da investigação criminal permite compreender de que modo os imaginários sociotécnicos a este respeito moldam os limites entre as conexões e a incorporação da ciência na lei. Sendo que, a estruturação dos discursos antecipatórios (Barben et al., 2008; Guston, 2014) e as práticas associadas a este tipo de modelo tecnocientífico pautam-se pela demarcação dos seus futuros imaginados (Pickersgill, 2011, p. 28). Esta demarcação é realizada pelo diálogo entre as fronteiras da ciência, da lei e da ética (idem, p. 36), na medida em que traduzem um conjunto específico de imaginários sobre o que é a ordem social e a interferência estatal na supressão de direitos civis, como a privacidade e a proteção de dados. Estes imaginários são ainda condicionados pelas

representações coletivas sobre a gestão do risco, por meio da conexão entre o campo forense e o campo médico, que levam a diferentes enquadramentos a respeito dos modos de governação de um aparelho tecnocientífico desta natureza (Jasanoff et al., 2007). Neste sentido, os imaginários sociotécnicos dos grupos profissionais a respeito da interoperabilidade nestes moldes são restritivos por se considerar que existem limites ético-legais que não devem ser ultrapassados numa investigação criminal. Sendo que ‘a interoperabilidade pela excecionalidade’ pretende dar resposta às tensões entre a restituição da justiça à(s) vítima(s) e o respeito pelos valores de altruísmo e solidariedade de um biobanco. Portanto, os imaginários sociotécnicos acerca da interoperabilidade demonstram que, no contexto português, os futuros coletivos imaginados desta prática vão no sentido de se manter a delimitação entre a ciência forense e o campo médico.

4.3.2 Imaginários sociotécnicos dos geneticistas forenses e stakeholders no contexto britânico

No Reino Unido, os imaginários sociotécnicos que recaem sobre a base de dados forense de DNA possuem um carácter maioritariamente crítico quanto à sua manutenção, sendo que estes ramificam-se em diferentes pontos consoante o seu grupo profissional de pertença (tabela 7.). A exceção a esta tendência crítica encontra-se nos elementos afetos a órgãos de investigação criminal cujos imaginários sociotécnicos se encontram em linha com a ‘privacidade ético-legal’ numa racionalidade que se caracteriza pela neutralização de riscos e pela escassa reflexão ética. Relativamente ao grupo dos geneticistas forenses, os seus imaginários sociotécnicos revelam uma reflexão das questões éticas que surgem no decorrer da governação, em contexto nacional, deste sistema tecnocientífico. Pelo que o equilíbrio dos direitos civis associados à ‘privacidade ético-legal’ é colocado em causa devido à sobre-representação de minorias étnicas na base de dados forense e à potencial sobrevalorização da prova genética por partes das forças policiais. Dito isto, estes imaginários sociotécnicos compreendem narrativas que deixam transparecer os riscos associados à conexão entre a ciência, a tecnologia e a lei. Em particular, estes riscos podem levar à (re)configuração do papel de determinados grupos enquanto ‘suspeitos’ com base em critérios discriminatórios e sem fundamentação legal. Por sua vez, os elementos das entidades de supervisão/regulação possuem imaginários sociotécnicos que se focam na expectativa da atualização do enquadramento ético de sistema tecnocientíficos, como as

base de dados forenses, que obrigam o plano dos danos a equacionar, para além dos danos físicos, os danos morais e psicológicos que podem decorrer do uso desvirtuado deste tipo de tecnologia. Posto isto, a ‘privacidade ético-legal’ é novamente colocada em causa no âmbito da interconexão entre a ciência e tecnologia e a lei. Por fim, os elementos de ONGs de direitos humanos elencam um aspeto que não pode ser dissociado do desenvolvimento tecnológico forense e da integração das suas ferramentas no auxílio à aplicação da lei, nomeadamente, o papel dos atores comerciais. Deste modo, revelam um imaginário sociotécnico que coloca o ator privado no seio do diálogo entre a delimitação das fronteiras entre a tecnologia, a ciência, a lei e as entidades privadas.

O sistema Prüm enquanto exemplo da aplicação da ciência e da tecnologia nos objetivos securitários da União Europeia é permeável a vários imaginários sociotécnicos. Por um lado, têm-se os imaginários acerca dos futuros desejáveis para a contribuição da ciência na comunidade política (Jasanoff & Kim, 2009, p. 121). Por outro lado, têm-se os imaginários acerca dos dilemas, desafios e danos que podem ser causados na esfera social pelo desenvolvimento tecnológico e a sua integração na lei (idem). Sendo que, a coexistência desta dualidade é responsável pela depuração da consciência coletiva de uma sociedade (ou comunidade política) quanto à necessidade de prever e gerir os potenciais danos de uma tecnologia. Dito isto, os geneticistas forenses e *stakeholders* do Reino Unido conservam esta dualidade nos seus imaginários sociotécnicos a respeito do sistema Prüm. No que toca à contribuição deste sistema para a sociedade, situam-se, genericamente, no ‘imaginário sociotécnico de reciprocidade’ que é favorável à sua implementação no contexto britânico. Porém, os motivos elencados são condicionados pelas suas áreas de conhecimento e a sua formação profissional. Em específico, os geneticistas forenses enfatizam que a standardização técnica, ao nível laboratorial, resulta na produção de dados mais confiáveis, pelo facto de todos os países estarem obrigados a cumprir com certos requisitos relativamente à recolha e análise de perfis de DNA. Os elementos das entidades de supervisão/regulação focam-se nos avanços que o sistema Prüm permite em termos de automatização e celeridade dos processos de troca de dados entre Estados-Membros. Por fim, para os elementos a desempenhar funções nos órgãos de investigação criminal, esta ferramenta veio permitir a produção de inteligência e a deteção de crimes cometidos por estrangeiros. Sendo que os pontos elencados pelo último grupo encontram-se em linha com uma racional policial que procura o acesso ao máximo de informações disponíveis.

Relativamente aos imaginários sociotécnicos acerca dos desafios, danos e dilemas da integração deste projeto tecnocientífico na esfera da lei, os grupos profissionais apontam a ocorrência de falsos positivos como uma preocupação comum. No entanto, são, novamente, discerníveis as variações em função da sua categoria profissional quanto aos restantes pontos elencados. Dito isto, os geneticistas forenses apontam a falta de standardização técnico-legal e o desvirtuamento dos dados como fatores problemáticos à universalidade do sistema Prüm. Por sua vez, nas entidades de supervisão/regulação, estes desenvolvimentos tecnológicos encontram tensões ao nível da desconfiança entre Estados-Membros, do elevado dispêndio de recursos económicos e do baixo envolvimento das entidades de supervisão, no contexto do Reino Unido, quanto à implementação do sistema Prüm. Os membros de ONGs de direitos humanos partilham parte do imaginário coletivo com o grupo anterior pela ênfase na falta de confiança entre países e na crítica à necessidade de se esclarecerem os mecanismos de escrutínio da informação trocada. Identificando ainda vários questionamentos éticos que podem afetar a ordem social das sociedades europeias. Em particular, a possibilidade da transnacionalização de erros judiciais, a falta de transparência e a falta de standardização da cadeia de custódia que pode conduzir à perpetuação de erros procedimentais a um nível transnacional. Por fim, os órgãos de investigação criminal referem o expectável aumento do volume de trabalho motivado pelo tamanho da base de dados forense como um ponto de tensão entre a implementação global e local do sistema Prüm. Dito isto, no 'imaginário sociotécnico de reciprocidade', característico dos grupos analisados, encontram-se patentes as dinâmicas conflituantes entre o que é desejável para ajudar a manter as sociedades seguras e os dilemas que surgem de um projeto de dimensão transnacional que interage com diferentes contextos nacionais.

As perspetivas a respeito da interoperabilidade entre bases de dados forenses e biobancos para fins de investigação criminal foram igualmente reveladores de imaginários sociotécnicos que dão conta das demarcações entre a ciência forense e a ciência com aplicação médica. A reflexão a respeito desta prática recorre às limitações que lhe são impostas de modo a prever o que é ou não desejável na sua evolução tecnológica e científica com aplicação direta na lei. Neste sentido, todas as categorias profissionais partilham coletivamente o 'imaginário sociotécnico restritivo' quanto à aplicabilidade da interoperabilidade nestes termos. No entanto, são de realçar certas nuances que se

correlacionam com as tarefas desempenhadas ao nível profissional. Os geneticistas forenses possuem um posicionamento holístico que nega a interoperabilidade quer pelo seu aspeto técnico, quer pelo desvirtuamento da finalidade dos biobancos. Nas entidades de supervisão/regulação assiste-se à enfatização dos dilemas éticos do acesso forense a biobancos, principalmente, pelo facto de a prática ferir os princípios de altruísmo e voluntariedade essenciais ao funcionamento dos biobancos. Neste caso, a reflexão realizada recai sobre o que é desejável tanto ao nível da segurança coletiva, como da importância da manutenção da saúde pública. Por último, os órgãos de investigação criminal entendem a interoperabilidade no plano do tempo presente onde ainda existem condicionamentos técnicos e legais para a sua realização. Posto isto, a prática da interoperabilidade, no Reino Unido, revela imaginários sociotécnicos que favorecem a demarcação entre o campo forense e o campo médico de modo a assegurar outros aspetos da ordem social, como a saúde pública.

4.3.3 Comparação ao nível nacional: Portugal e Reino Unido

Tabela 8-Comparação entre Portugal e o Reino Unido em relação às bases de dados forenses de DNA e à cooperação transnacional

	Portugal	Reino Unido (Inglaterra e País de Gales – NDNAD)
Base de dados forense de DNA		
Enquadramento legal	Lei n.º 5/2008 (atual Lei n.º 90/2017)	- <i>Protection of Freedoms Act 2012</i>
Criação	2008 (12 anos)	1995 (25 anos)
Critérios de inclusão/exclusão	Restritivos	Expansivos
Custódia	Judicial	Policial
Recolha de amostra	- Por indicação judicial no decorrer de um processo/investigação	- No ato de detenção pela polícia
Argumentos a favor (documentos oficiais)	- Ajuda a combater a criminalidade - Justiça mais eficaz através da identificação de pessoas - Contribui para o bem-comum e a confiança na justiça - Estar a par do percurso dos países mais desenvolvidos nesta área - Prender culpados e exonerar inocentes - Dissipação de riscos	- Aumento da eficácia na deteção e detenção do crime - Ajuda no ‘combate ao crime’ - Aumento da velocidade da investigação criminal - Quem não deve, não teme
Argumentos contra (perceção pública)	- Corrupção na investigação criminal - Problemas de confidencialidade	- Privacidade e propriedade dos dados - Potenciais usos desadequados da

	- Falta de segurança da informação - Utilização do material genético para outros fins	informação retida - Criminalização de pessoas inocentes⁶² - Sobre-representação de grupos étnicos - Desconfiança em relação aos procedimentos de retenção e utilização dos perfis
Dimensão	- Pequena dimensão 5 339 perfis de referência⁶³ (0.05% da população)	- Grande dimensão (a maior da UE) 4 733 755 perfis de referência²⁵ (8.8% da população)
Supervisão	Um órgão: - Conselho de Fiscalização da Base de Dados de Perfis de ADN (3 elementos) (a CNPD também é consultada)	Quatro órgãos: - <i>National DNA Database Strategy Board</i> - <i>National DNA Database Ethics Group</i> - <i>Biometrics Commissioner</i> - <i>Forensic Science Regulator</i>
Inserção de perfis de DNA (âmbito criminal)	- Cenas de crime - Indivíduos condenados a pena efetiva de prisão igual ou superior a 3 anos, por crime doloso - Voluntários (com consentimento) - Profissionais que recolhem e analisam material biológico (para efeitos de exclusão)	- Cenas de crime - Indivíduos condenados - Indivíduos detidos⁶⁴ - Voluntários²⁵ - Profissionais que recolhem e analisam material biológico: foi criada uma base de dados para o efeito, a CED
Retenção de perfis de DNA	Restrição: - Perfis eliminados consoante os anos de pena - Não é possível a retenção indefinida - Voluntários só com consentimento revogável	Semi-restritiva (PoFA): - É possível reter permanentemente perfis de condenados - Retenção limitada de perfis de pessoas inocentes⁶⁵ - Retenção limitada de perfis de voluntários²⁶
Acesso às informações	- Profissionais do INMLCF responsáveis pela inserção dos dados	- Cerca de 30 profissionais com acesso completo à base - Forças policiais só com indicação da existência de um <i>hit</i>

Cooperação transnacional – Decisões Prüm

Ano de entrada	2008 (Presença em reuniões desde 2006)	2019 (relacionado com o <i>Brexit</i>) - Realização de um projeto piloto
Argumentos a favor	- Estar a par do percurso dos países mais desenvolvidos nesta área	- Benefícios na identificação de pessoas (estrangeiras) que cometem crimes no país
Argumentos contra	---	- Cedência de soberania à UE - Número desproporcional de pedidos de informação por parte dos outros Estados - Elevado dispêndio de recursos económicos - Falsos positivos
Perfis disponíveis	Condenados	Condenados

⁶² Durante um longo período de tempo foi possível a retenção de perfis de inocentes de modo ilimitado

⁶³ Em junho 2016, dados do relatório "A comparative audit of legislative frameworks within the European Union for the collection, retention and use of forensic DNA profiles" do EUROFORGEN.

⁶⁴ Desde o PoFA com mais restrições na retenção

⁶⁵ Desde o PoFA

Alterações à lei nacional	- Expansão da Lei n.º 5/2008 para aumentar o número de perfis de DNA na base de dados	- Em matéria de proteção de dados para garantir os padrões da UE
Racional da decisão	Cooperação transnacional	Interesse nacional em detrimento da cooperação

No sistema Prüm, os imaginários sociotécnicos são consolidados, num primeiro momento, por instituições supranacionais, como a União Europeia, através de decisões e narrativas políticas que realçam os benefícios públicos da adoção deste sistema (Levenda et al., 2018). Num segundo momento, pelos Estados-Membros da comunidade europeia que partilham os mesmos imaginários quanto à gestão do risco. Os imaginários sociotécnicos, no caso do sistema Prüm, evoluíram a partir de um conjunto de decisões institucionais responsáveis por moldar o modo como a cooperação policial e judicial é encarada no seio na União Europeia. Neste sentido, os objetivos da agenda securitária da UE foram uma ‘cultura política sociotécnica única’ (Kim, 2018, pp. 177-178). Portanto, as narrativas acerca do sucesso ou potencial sucesso de uma tecnologia e as políticas e regulações aprovadas a seu respeito são fundamentais para a sua continuidade. Estes dois fatores permitem influenciar a forma de conceção da tecnologia, o gasto de dinheiro público para o seu desenvolvimento, bem como justifica a (não) inclusão dos cidadãos em relação aos benefícios de determinado progresso tecnológico (Jasanoff & Kim, 2009, p. 120). A análise do sistema Prüm, em Portugal e no Reino Unido, à luz dos seus desafios éticos, científicos e políticos permite compreender de que modo as noções de ‘Estado’ e ‘interesse nacional’ são “reinventadas (ou reproduzidas) na projeção, produção, implementação e compreensão dos imaginários sociotécnicos” (*idem*, p. 124).

O projeto piloto levado a cabo pelo Reino Unido para auxiliar a decisão de fazer ou não parte do sistema Prüm é representativo do modo como o ‘interesse nacional’ é reproduzido na construção de um imaginário sociotécnico. Dito isto, os decisores políticos britânicos revelaram um ‘imaginário sociotécnico de utilidade’ quanto à sua entrada no sistema Prüm, na medida em que, apesar de inseridos na União Europeia, encararam que esta adesão deveria ser feita à luz de uma análise dos custos e benefícios para o país que originou por diversos momentos avanços e recuos na entrada. Sob este pano de fundo foram elencados vários argumentos desfavoráveis ao sistema Prüm. Na tabela 8. podem observar-se os seguintes pontos: cedência da soberania nacional à União Europeia, elevado dispêndio de recursos económicos na implementação, existência de falsos positivos e

potencial existência de um número desproporcional de pedidos de informação por parte dos outros Estados-Membros. No entanto, os entrevistados geneticistas forenses e *stakeholders* divergem deste imaginário de utilidade e, genericamente, situam-se no ‘imaginário sociotécnico de reciprocidade’, como já foi observado. O discurso político português encarou o sistema Prüm enquanto uma ferramenta tecnológica para o auxílio transnacional na resolução de crimes (nacionais ou não). No fundo o sistema Prüm seria mais uma tecnologia para melhorar a segurança do espaço europeu do qual faz parte. No caso português, ainda que com diferentes intensidades, tanto o discurso político como as narrativas dos geneticistas forenses e *stakeholders* revelam um ‘imaginário sociotécnico de reciprocidade’. Exemplo da vontade política em contribuir para o sucesso deste projeto tecnocientífico é a alteração à Lei n.º 5/2008 que teve como objetivo permitir o aumento do número de perfis de DNA não só para melhorar a base de dados forense ao nível nacional, como também para ser mais eficaz ao nível transnacional.

Os diferentes imaginários sociotécnicos destes países a respeito do sistema Prüm são condicionados pelo imaginário securitário coletivo da União Europeia. No entanto, o modo como se procedeu à criação e construção das infraestruturas das bases de dados forenses também é um fator explicativo do modo como o ‘interesse nacional’ foi mobilizado pelo Reino Unido. Dito isto, a criação das bases forense teve uma evolução diferente nestes dois países. Portugal possui uma base de dados forense de reduzida dimensão, ao passo que o Reino Unido é o país europeu com a maior base de dados (tabela 8.). Esta assimetria numérica é justificada pelo tempo de funcionamento das bases de dados e pelos critérios de inserção/retenção/eliminação de perfis de DNA. Como se pode observar na tabela 8., em Portugal verifica-se uma maior restrição nos critérios de inserção/ retenção/ eliminação de perfis de DNA. A decisão de manter estes limites rígidos tem que ver com a tentativa de manter a tradição humanista do sistema penal nacional, ainda que a tendência seja a da expansão desses critérios. No Reino Unido, os critérios de recolha/retenção/eliminação de perfis da base de dados são mais latos e, portanto, atualmente, possui um sistema semi-restritivo. Sendo uma base de dados com mais anos já passou por vários sistemas de retenção de perfis movendo-se de um sistema restritivo, para um expansivo e, atualmente, para um sistema semi-restritivo.

Relativamente aos critérios adotados, um dos mais representativos é o facto de no Reino Unido ser possível reter o perfil de DNA de pessoas inocentes (não condenadas) na

base de dados e em Portugal esta prática não ser legalmente possível. O segundo com maior expressão tem que ver com a permissão da retenção ilimitada de perfis de DNA de condenados, situação que em Portugal também não é passível de ocorrer por limitações legalmente impostas. Deste modo, através das opções legais adotadas para os critérios enunciados, discerne-se que, no contexto português, a privacidade é entendida à luz de ‘imaginários sociotécnicos restritivos’. Sendo que no Reino Unido, observa-se um conjunto de medidas latas que resultam na construção de ‘imaginários sociotécnicos expansivos’ a respeito da privacidade dos cidadãos cujas informações constam na base de dados forense ao nível nacional. Porém, quando envolvidos na troca de dados transnacional os imaginários parecem inverter-se. Isto é, Portugal tem-se mostrado comprometido com os objetivos de cooperação e da reciprocidade da mesma, ao passo que o Reino Unido tem tido uma postura mais protetora da sua base de dados forense relativamente à partilha das informações que nela constam.

O modo como a supervisão destas infraestruturas é realizada nos dois contextos nacionais revela que, apesar de possuir critérios de inserção/eliminação e retenção mais abrangentes, o Reino Unido, possui mais entidades de supervisão do que Portugal (tabela 8.). As entidades de supervisão diferem igualmente no perfil profissional e no número de elementos que as integram. Posto isto, no Reino Unido há uma aposta na integração de várias áreas de formação (direito, ética, ciências exatas), sendo que, em Portugal, a única entidade de supervisão é constituída por três membros, maioritariamente, da área do direito. Esta discrepância na constituição das entidades de supervisão mostra que, no Reino Unido, a base de dados é encarada à luz de um imaginário que abarca vários questionamentos ao nível ético, político e científico. Realçando-se que esta fragmentação torna a participação dos cidadãos mais acessível.

Dar sentido a políticas nacionais que apoiam o desenvolvimento de projetos tecnocientíficos, como o sistema Prüm, obriga os países a mobilizar tanto os seus recursos materiais e organizacionais, como os seus recursos do imaginário que permitem a relação entre este tipo de políticas e o bem-comum dos cidadãos (manter a sociedade em segurança) (Jasanoff et al., 2007). Dito isto, a projeção das infraestruturas do Sistema Prüm é o resultado de um conjunto de escolhas científicas, éticas e políticas. Científicas porque é necessário que funcionem corretamente para o que foram pensadas, por exemplo, a comparação de perfis de DNA é uma técnica consolidada. Éticas porque equacionam os

potenciais riscos ou erros da tecnologia: falsos positivos, privacidade, abuso de poder. E políticas porque foram pensadas para o contexto europeu, que mais tarde tornou o sistema Prüm obrigatório para toda a União Europeia. Deste modo, a análise comparativa do sistema Prüm em Portugal e no Reino Unido mostra que os diferentes modos de implementação deste sistema não podem ser equacionados apenas como meras variações da sua utilização. A partir do conceito de imaginários sociotécnicos foi possível identificar as tensões entre a universalidade do sistema Prüm e os imaginários locais que conduziram a modelos de implementação diferenciados entre estes países.

CONCLUSÕES

Nesta fase final do estudo é chegado o momento de sistematizar os resultados alcançados e refletir sobre o modo como estes respondem aos objetivos traçados na fase inicial da presente tese. Desta reflexão surgem as conclusões finais e uma problematização do modo como o trabalho empreendido contribui para a produção de conhecimento na Sociologia, nomeadamente, ao nível dos estudos da ciência e da tecnologia, dos estudos da vigilância e dos estudos sociais da genética forense.

À luz das especificidades associadas à análise de um fenómeno social complexo como o sistema Prüm, o presente estudo apresenta-se como um contributo, ao nível nacional e internacional, para a compreensão aprofundada das narrativas dos atores envolvidos na sua operacionalização. Deste modo, esta tese explorou quais os desafios éticos e sociais da proteção de informações genéticas no âmbito da sua partilha como ferramenta de combate à criminalidade na União Europeia. Em particular, almejou-se compreender os sentidos atribuídos à noção de proteção de dados e privacidade no sistema Prüm pelas narrativas de profissionais de várias esferas de ação, nomeadamente, os Pontos de Contacto Nacionais, os cientistas forenses, os membros de comissões de ética e de diversos atores do sistema de justiça. De modo complementar, a consulta de documentação oficial sobre a temática da proteção de dados na União Europeia permitiu o mapeamento das especificidades da sua regulação no contexto particular da investigação criminal, bem como o reconhecimento dos pontos de tensão entre o equilíbrio dos direitos civis de privacidade e proteção de dados e da vigilância como prática de gestão de risco nas sociedades europeias.

Atendendo à complexidade do objeto em estudo e à valorização das perspetivas e significados socialmente construídos pelos atores sociais entrevistados no âmbito desta investigação, a tese adotou uma metodologia de carácter qualitativo e interpretativo. Posto isto, a tese norteou-se em alguns dos pressupostos da *grounded theory* por permitir uma estratégia de articulação constante e paralela entre a análise, a empiria e a teoria. Esta opção metodológica permitiu também a construção de hipóteses de trabalho e de conceitos em conformidade com a realidade empírica em estudo. Situação particularmente premente aquando do capítulo da análise dos estudos de caso de Portugal e do Reino Unido, países

com particularidades próprias e que, por isso mesmo, apresentam diferentes dimensões teórico-analíticas. De realçar que a representatividade sociológica de cada caso foi valorizada neste estudo e, por esse motivo, os resultados não são generalizáveis a populações ou universos, devendo antes ser enquadrados enquanto enunciações teóricas. Complementarmente, os estudos já existentes e com pontos de ligação com a tese foram úteis para a procura de conceitos sensibilizadores de apoio à análise empírica. No entanto, a análise deu primazia à construção teórica e conceptual baseada nos dados com valor heurístico.

A significação atribuída às narrativas dos entrevistados verteu, como já mencionado, da conjugação de três campos de estudo das ciências sociais, nomeadamente, dos estudos da ciência e da tecnologia, dos estudos da vigilância e dos estudos sociais da genética forense. Deste modo, foi necessária a mobilização de um corpo diversificado de literatura para dar conta da complexidade e da interconexão entre as várias dimensões e desafios elencados a respeito das implicações da partilha transnacional de dados pessoais na proteção da privacidade dos indivíduos. Estudar em profundidade o sistema Prüm implicou avaliar: 1) A sua dimensão tecnológica, na medida em que a partilha de dados é realizada através de sistemas interoperáveis e ligados em rede, onde a standardização e o avanço tecnológico são essenciais. 2) A sua dimensão genética/forense, pois os desenvolvimentos ocorridos no conhecimento do genoma humano e na própria aplicação da ciência forense na lei foram indispensáveis para a constituição das infraestruturas deste sistema. E 3) a sua dimensão da vigilância como fator de legitimação do empreendimento tecnocientífico de vigilância por *target* com base na agenda securitária da União Europeia e no discurso do risco.

A análise empírica das perspetivas veiculadas pelos Pontos de Contacto Nacionais do sistema Prüm permitiu explorar, ao nível macro, os dilemas éticos, sociais e tecnocientíficos que decorrem da partilha transnacional de dados genéticos, inseridos em bases de dados forenses, entre países da União Europeia, bem como as suas expectativas quanto à standardização e evolução da cooperação policial e judiciária operada pelo sistema Prüm. As suas narrativas situaram o sistema Prüm enquanto instrumento de empoderamento e em linha com o imaginário europeu de modelo ideal-tipo de governação da criminalidade e da cooperação policial e judiciária entre países. Posto isto, esta solução tecnológica de combate à criminalidade foi uma das respostas encontradas para os desafios securitários

que acompanharam o aumento da mobilidade dos cidadãos no espaço europeu. De modo complementar, a sua eficácia foi legitimada por argumentos que remeteram para a standardização de práticas de comunicação e partilha de dados, principalmente numa fase inicial do sistema, materializando-se numa maior celeridade na cooperação transnacional. A análise das narrativas destes profissionais revelou vários pontos em comum entre os argumentos de legitimação da troca de dados no sistema Prüm e o discurso político plasmado em documentação oficial da União Europeia. Deste modo, constatou-se que o discurso político da União Europeia relativamente às novas modalidades de cooperação policial e judiciária tem sido assimilado, internalizado e reproduzido, na sua generalidade, pelos Pontos de Contacto Nacionais.

Como se observou, os desafios securitários da União Europeia, em particular, ao nível da criminalidade organizada e do terrorismo trouxeram consigo discursos que enfatizaram a importância da manutenção da segurança nacional e a necessidade de gestão do risco. As biotecnologias de vigilância, onde se insere o sistema Prüm, fazem parte de uma panóplia de respostas encontradas para controlar o fluxo de pessoas no seio da União Europeia. Reconhecida a importância deste sistema para a segurança das sociedades europeias, neste estudo, ambicionou-se também a desconstrução das narrativas entusiásticas dos profissionais a respeito das vantagens da implementação de sistemas tecnológicos de controlo. Pois, a standardização de parte do processo da partilha de dados transnacional pode camuflar os vários desafios e tensões sentidos pelos países durante a sua implementação. Esses desafios têm origem na diversidade de contextos nacionais, que possuem diferentes tradições jurídicas, diferentes modos de apropriação das tecnologias biométricas forenses, bem como na existência de diferentes expectativas quanto ao impacto da vigilância nas suas sociedades. Nestas, também os significados dados aos conceitos de privacidade e proteção de dados se encontram dependentes de políticas nem sempre consonantes entre países.

Devido às responsabilidades atribuídas aos Pontos de Contacto Nacionais e ao modo de funcionamento, em dois passos, do sistema Prüm, a análise empírica foi realizada separadamente. Num primeiro momento, foram exploradas as narrativas dos Pontos de Contacto Nacionais, com um perfil tipicamente laboratorial, do primeiro passo do sistema Prüm. Num segundo momento, identificaram-se as perspetivas dos profissionais responsáveis pelos processos de decisão do segundo passo do sistema Prüm, os quais

apresentam um perfil tipicamente policial. Esta decisão deveu-se ao reconhecimento de que o perfil profissional e a natureza das funções desempenhadas no âmbito da cooperação transnacional constituem um dos fatores explicativos do modo como estes profissionais apreendem o sistema quanto aos seus riscos e desafios.

Atendendo às narrativas dos Pontos de Contacto Nacionais para o primeiro passo, constatou-se que, na sua generalidade, os desafios identificados se prendem com as questões técnicas que advêm da implementação do sistema. Este enfoque na tecnicidade dos procedimentos de cooperação conduziu a narrativas pautadas pela minimização de riscos as quais, por conseguinte, revelam uma escassa reflexão sobre a tensão e complexidade das relações de confiança, controlo e segurança entre países. Assim, a neutralização dos potenciais riscos às liberdades civis dos cidadãos aliada a um elevado entusiasmo quanto à automatização de procedimentos na primeira fase da cooperação coloca estes profissionais próximos de um posicionamento de ‘minimalismo genómico’. Isto porque a neutralização dos riscos e desafios do sistema Prüm operada por meio da standardização dos procedimentos técnicos é um aspeto característico da maioria dos entrevistados com um perfil laboratorial. Os significados atribuídos às noções de privacidade e de proteção de dados seguiram a mesma linha retórica. Estes profissionais consideram que os protocolos técnicos e standardizados são os instrumentos necessários à segurança dos dados recolhidos e partilhados. Novamente, foi relegado para segundo plano o debate ético mais aprofundado sobre o caráter e o tipo de informação presente no DNA forense e nos ficheiros sociodemográficos a ele associados. Portanto, a reflexão a respeito da privacidade e proteção de dados no âmbito do sistema Prüm caracterizou-se, na sua maioria, por um conjunto de narrativas instrumentalizadas que se refugiaram tanto em ‘protocolos’ legais, como em fontes de ‘objetividade administrativa’. Uma vez que estes profissionais apresentam em comum um perfil laboratorial, conclui-se que o seu posicionamento dá conta de uma cultura epistémica específica, característica da sua forma de olhar, compreender e manusear o mundo que os rodeia.

Relativamente ao segundo grupo de profissionais, os Pontos de Contacto Nacionais do segundo passo, as suas perspetivas acerca dos riscos e desafios do sistema Prüm enquadraram-se, *grosso modo*, num posicionamento de ‘pragmatismo biométrico’. Importa referir que as categorias apresentadas em ambas as análises das perspetivas dos Pontos de Contacto Nacionais vertem diretamente do trabalho de Williams e Johnson (2004b) sobre as

representações sociais em torno das tecnologias forenses de DNA. Porém, no caso particular dos profissionais do segundo passo propôs-se uma expansão desta categoria de modo a incluir na sua definição as preocupações com a legitimidade da utilização dos dados genéticos partilhados entre os Estados-Membros em consonância com as fontes de obtenção do DNA e da informação partilhada. Apesar da existência de uma reflexão ética mais aprofundada dos riscos deste sistema, constatou-se que as narrativas a respeito dos desafios à privacidade e proteção de dados incidiram, em muitos casos, na reprodução de discursos institucionalizados que careceram de elaboração acerca do modo como são asseguradas as leis de proteção de dados na cooperação transnacional. Neste sentido, para estes profissionais a proteção de dados passa pela criação de soluções ao nível tecnológico e pela adequação da legislação nacional às necessidades da partilha numa ótica de priorização dos aspetos tecnocientíficos da partilha de dados. Quanto às funções que estes profissionais desempenham ao nível do segundo passo, foram tecidas críticas específicas à falta de standardização desta fase do sistema que, no seu entender, condicionam a celeridade e aumentam a complexidade da partilha de dados entre países. Deste modo, foram identificados quatro fatores de destandardização dos procedimentos da cooperação policial e judicial no sistema Prüm, respetivamente: 1) A falta de compactação e de um formato standardizado para o envio de informação. 2) A heterogeneidade dos canais de comunicação entre países. 3) As diferentes custódias das bases de dados forenses. 4) E a heterogeneidade dos critérios de *follow-up*. À semelhança do primeiro grupo, as narrativas veiculadas por estes profissionais são condicionadas quer pelas funções que desempenham no sistema Prüm quer pelo seu perfil profissional – perfil policial. Deste modo, as críticas à destandardização do segundo passo e a reprodução dos discursos institucionais quanto aos riscos e desafios da cooperação nestes termos podem encontrar justificação na racional de atuação característica das forças policiais. Genericamente, depreendeu-se das perspetivas dos participantes, que uma maior standardização dos procedimentos do segundo passo do sistema Prüm potencia um ganho em termos de produção de inteligência e de acesso a informação permitindo maior celeridade na investigação criminal.

O estudo das narrativas dos Pontos de Contacto Nacionais permitiu apreender a dimensão macro da análise da cooperação policial e judicial transnacional e das perspetivas em torno da privacidade e proteção de dados no seio da União Europeia, tendo como objeto de estudo o sistema Prüm. Para compreender com maior profundidade este objeto

de estudo, foram integrados dois estudos de caso, respetivamente, Portugal e o Reino Unido, que devido às suas características nacionais foram elucidativos dos diferentes modos de apropriação e (d)estandardização do sistema Prüm. Em traços latos, os fatores tidos em consideração para a escolha destes dois países relacionaram-se com os seguintes critérios: a sua inovação ao nível das tecnologias de DNA e posterior utilização no sistema de justiça criminal; tipo de sistema de justiça (inquisitorial e adversarial); tamanho, antiguidade e legislação da base de dados forense de perfis de DNA; e postura política quanto à implementação do sistema Prüm ao nível nacional.

O enfoque nestes países possibilitou uma compreensão da complexidade da partilha de dados transnacional e do papel das especificidades nacionais ao nível da implementação de sistemas com esta amplitude de atuação. Da análise das narrativas dos diversos profissionais direta ou indiretamente afetos à implementação do sistema Prüm foi possível apreender o modo como estes países estão (des)alinhados com aquelas que são as expectativas e as práticas de cooperação transnacional na investigação criminal. Em particular, a integração de dois estudos de caso à luz do quadro concetual dos estudos da ciência e da tecnologia consolidou o mapeamento do debate em torno dos benefícios e das controvérsias levantadas pelo uso de biotecnologias nos sistemas de justiça. Ainda, os imaginários sociotécnicos dos atores do campo da ética, do direito e da ciência forense, em ambos os países, sobre os modos de implementação de projetos tecnocientíficos mostraram-se fortemente condicionados pelas conceções sobre o seu valor utilitário e as suas implicações para a privacidade e proteção de dados dos cidadãos.

De modo a captar a pluridimensionalidade narrativa que permeia sistemas tecnocientíficos como o sistema Prüm esta tese apresenta uma análise que abrangeu um nível macro/nacional, representado pelo discurso político, e um nível micro operado pelas narrativas dos geneticistas forenses e dos *stakeholders* dos países em estudo. A expansão desta análise permitiu explorar, numa dimensão micro, as (des)coincidências narrativas, quanto aos desafios e vantagens do sistema Prüm, entre os entrevistados com diferentes perfis profissionais. Num primeiro momento, os imaginários sociotécnicos são influenciados pela autoridade simbólica das instituições da União Europeia responsáveis pela criação de regulações e por narrativas políticas cujo ênfase é feito no aumento da segurança por via dos sistemas tecnológicos de vigilância. Num segundo momento, estes são condicionados e reapropriados com base nas especificidades legais e técnicas dos contextos nacionais, por

exemplo, ao nível da disponibilidade de recursos económicos, humanos e tecnocientíficos para a partilha de dados. Os dados empíricos recolhidos em Portugal e no Reino Unido quanto às expectativas relativas à implementação do sistema Prüm foram analisados com base nas categorias de ‘imaginário sociotécnico de utilidade’ e ‘imaginário sociotécnico de reciprocidade’. A apresentação desta categorização constitui um dos contributos teórico-analíticos originais da tese, os quais vertem das opções metodológicas adotadas ao nível da *grounded theory*.

No que diz respeito à análise dos dados empíricos no Reino Unido constatou-se que, as decisões políticas, relativamente à implementação do sistema Prüm, foram fortemente condicionadas pela configuração do interesse nacional como principal fator de ponderação para a adesão ao mesmo. Nesta linha de pensamento, os decisores políticos britânicos foram enquadrados na categoria de ‘imaginário sociotécnico de utilidade’ por terem revelado um posicionamento que entendeu a adesão ao sistema Prüm à luz de uma análise dos custos e benefícios para o próprio país. Em particular, os imaginários inicialmente desfavoráveis à implementação do sistema Prüm sustentaram-se pelos seguintes argumentos: 1) Cedência da soberania nacional à União Europeia; 2) Elevado dispêndio de recursos económicos; 3) Ocorrência de falsos positivos; e 4) Potencial desproporcionalidade de pedidos de informação por parte dos outros Estados-Membros. Porém, a um nível micro, a análise das narrativas dos geneticistas forenses e dos *stakeholders* tornou visíveis as discrepâncias quanto ao discurso político utilitarista sobre o sistema Prüm. Os imaginários sociotécnicos destes profissionais, ainda que condicionados pelos seus perfis e funções profissionais, situam-se no ‘imaginário sociotécnico de reciprocidade’. As perspetivas veiculadas pela maioria dos participantes realçam a importância de um projeto europeu de combate à criminalidade organizada e ao terrorismo. Num contexto, em que os Estados-Membros deveriam contribuir ativamente para este projeto, na medida em que, a segurança de uma sociedade está dependente da segurança das restantes sociedades.

A descoincidência entre os imaginários sociotécnicos da classe política e dos geneticistas forenses e *stakeholders* observada no Reino Unido em relação às expectativas e modos de implementação do sistema Prüm não se verificou em Portugal. Neste contexto nacional, o discurso político retratou o sistema Prüm enquanto ferramenta tecnocientífica fundamental à cooperação transnacional e à resolução de crimes tanto no país, como nos

restantes Estados-Membros da União Europeia. Por este motivo, o discurso político português em consonância com as narrativas dos geneticistas forenses e *stakeholders* revelaram um ‘imaginário sociotécnico de reciprocidade’. Conclui-se, assim, que os diferentes modos de apropriação do sistema Prüm se encontram relacionados com os imaginários sociotécnicos a respeito da utilização da ciência forense na lei, da cooperação transnacional e das tensões entre o caráter global do sistema Prüm em relação às contingências locais de cada país. Porém, ao interpretar os dados empíricos recolhidos no Reino Unido é necessário reforçar que o momento político sentido no país durante o trabalho de campo terá tido influência nas narrativas dos diversos profissionais. Em particular, as entrevistas foram realizadas num período próximo à votação e às conversações a respeito do *Brexit* que ditou a saída do Reino Unido da União Europeia.

Esta tese apresenta um contributo original para o estudo da complexidade e das tensões presentes na implementação de sistemas de controlo e gestão da criminalidade na União Europeia, tendo como objeto de estudo específico o sistema Prüm. Face à riqueza do material empírico e à diversidade dos perfis profissionais dos participantes, este estudo vem complementar empiricamente a literatura já existente a respeito: 1) Das vantagens e benefícios do sistema Prüm; 2) Dos riscos e desafios da sua implementação nos diversos contextos nacionais; e 3) Dos significados atribuídos à proteção de dados e privacidade no âmbito da investigação criminal e da cooperação policial e judiciária transnacional. Seguindo os princípios da *grounded theory*, este estudo debruçou-se sobre as narrativas, significados e sentidos atribuídos, por parte dos profissionais entrevistados, a respeito das dimensões sociais, éticas, culturais e regulatórias da utilização das tecnologias forenses de DNA nos sistemas de justiça e a partilha de dados pessoais operada através do sistema Prüm. No entanto, a inexistência de estatísticas oficiais, em praticamente todos os países, que contenham dados representativos que permitam aferir a eficácia real do sistema Prüm, apresentou-se como uma limitação, não só ao presente estudo como também ao próprio aperfeiçoamento do sistema. A aposta na produção deste tipo de informações oficiais é de suma importância para uma melhor delineação das políticas a adotar no âmbito da cooperação transnacional.

O estudo inovador da comparação de dois estudos de caso à luz dos imaginários sociotécnicos sobre o sistema Prüm revelou-se igualmente importante sob o ponto de vista sociológico, pois possibilitou a exploração das narrativas de outros atores envolvidos no

sistema Prüm, para além dos Pontos de Contacto Nacionais. A compreensão e mapeamento dos significados atribuídos à proteção de dados e à privacidade em contextos nacionais específicos no âmbito da cooperação transnacional deixa pistas para uma melhor e mais ampla reflexão a respeito da influência dos imaginários sociotécnicos locais no sucesso da implementação de sistemas tecnológicos de vigilância.

Próximas investigações acerca do sistema Prüm serão igualmente relevantes para permitir o mapeamento e acompanhamento histórico da evolução das narrativas dos Pontos de Contacto Nacionais, dos geneticistas forenses e de *stakeholders* a respeito do seu desenvolvimento e evolução. Sendo que, as interações entre a ciência, a esfera legal e a tecnologia são também suscetíveis às mudanças de paradigma das próprias sociedades em termos das suas agendas securitárias. Por fim, a realização de estudos comparativos aprofundados, à semelhança do que foi realizado em Portugal e no Reino Unido, pode gerar dados significativamente relevantes para novas propostas técnicas, científicas e legais a respeito do sistema Prüm, bem como de outro tipo de tecnologia que opere segundo os mesmos pressupostos.

REFERÊNCIAS BIBLIOGRÁFICAS

- Aas, K. (2006). "The body does not lie": Identity, risk and trust in technoculture. *Crime, Media, Culture*, 2(2), 143–158. <https://doi.org/10.1177/1741659006065401>
- Aas, K. (2009). Commentary - Surveillance: Citizens and the state. *Surveillance & Society*, 6(3), 317–321.
- Aas, K. (2011). "Crimmigrant" bodies and bona fide travelers: Surveillance, citizenship and global governance. *Theoretical Criminology*, 15(3), 331–346. <https://doi.org/10.1177/1362480610396643>
- Aas, K. (2013). *Globalization and crime. Vol. I-III*. London: Sage.
- Aas, K., & Bosworth, M. (2013). *The borders of punishment: Migration, citizenship, and social exclusion*. (K. Aas & M. Bosworth, Eds.). Oxford: Oxford University Press.
- Ahrne, G. (1994). *Social Organizations*. London: Sage.
- Ahrne, G., & Brunsson, N. (2006). Organizing the world. In M. Djelic & K. Sahlin-Andersson (Eds.), *Transnational governance: Institutional dynamics of regulation* (pp. 74–94). Cambridge: Cambridge University Press.
- Ahrne, G., Brunsson, N., & Garsten, C. (2005). Standardizing through organization. In N. Brunsson & B. Jacobsson (Eds.), *A World of Standards* (pp. 50–68). Oxford: Oxford University Press.
- Allen-Castellitto, A. (1999). Coercing Privacy. *William and Mary Law Review*, 40, 723–757.
- Altheide, D. (2006). *Terrorism and the politics of fear*. Lanham, MD: Altamira Press.
- Amankwaa, A. (2018). Forensic DNA retention: Public perspective studies in the United Kingdom and around the world. *Science & Justice*. <https://doi.org/10.1016/j.scijus.2018.05.002>
- Amankwaa, A. (2019). Trends in forensic DNA database: Transnational exchange of DNA data. *Forensic Sciences Research*, 0(0), 1–7. <https://doi.org/10.1080/20961790.2019.1565651>
- Amankwaa, A., & McCartney, C. (2018). The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012. *Forensic Science International*, 284, 117–128. <https://doi.org/10.1016/j.forsciint.2017.12.041>
- Amankwaa, A., & McCartney, C. (2019). The effectiveness of the UK national DNA database. *Forensic Science International: Synergy*, 1, 45–55. <https://doi.org/10.1016/J.FSISYN.2019.03.004>
- Amelung, N., Granja, R., & Machado, H. (2020). *Modes of bio-bordering: The hidden (dis)integration of Europe*. Singapore: Palgrave Macmillan.
- Amoore, L. (2006). Biometric borders: governing mobilities in the war on terror. *Political Geography*, 25, 336–351.
- Amoore, L. (2007). Vigilant visualities: the watchful politics on the war on terror. *Security Dialogue*, 38, 215–232.
- Anil, K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 20–40.
- Annas, G. (2009). Protecting privacy and the public: Limits on police use of bioidentifiers in Europe. *New England Journal of Medicine*, 361(2), 196–201. Retrieved from <http://dnapolicyinitiative.org/>
- Appadurai, A. (1996). *Modernity at large: Cultural dimensions of globalization*. Minneapolis: University of Minnesota Press.
- Austin, L. (2003). Privacy and the question of technology. *Law and Philosophy*, 22, 119–166.

- Baines, D. (2006). "Whose needs are being served?" Quantitative metrics and the reshaping of social services. *Studies in Political Economy*, 77, 195–209.
- Baldwin, R., Scott, C., & Hood, C. (Eds.). (1998). *A Reader on Regulation*. Oxford: Oxford University Press.
- Ball, K., Di Domenico, M., & Nunan, D. (2016). Big data surveillance and the body-subject. *Body & Society*, 22(2), 58–81. <https://doi.org/10.1177/1357034X15624973>
- Balzacq, T. (2005). *From a Prüm of 7 to a Prüm of 8 +: What are the implications?* (No. IP/C/LIBE/FWC/2005-22). Policy Department C Citizens Rights and Constitutional Affairs. Brussels. Retrieved from http://www.libertysecurity.org/IMG/doc_From7to8__English.doc
- Balzacq, T., Bigo, D., Carrera, S., & Guild, E. (2006). *Security and the two-level game: The treaty of Prüm, the EU and the management of threats* (No. 234). Retrieved from http://www.libertysecurity.org/IMG/pdf/WD234_e-version.pdf
- Balzacq, T., & Hadfield, A. (2012). Differentiation and trust: Prüm and the institutional design of EU internal security. *Cooperation and Conflict*, 47(4), 539–561. <https://doi.org/10.1177/0010836712462781>
- Barad, K. (2003). Posthumanist performativity: Toward an understanding of how matter comes to matter. *Signs: Journal of Women in Culture and Society*, 28(3), 801–831. <https://doi.org/10.1086/345321>
- Barben, D., Fisher, E., Selin, C., & Guston, D. (2008). Anticipatory governance of nanotechnology: Foresight engagement and integration. In E. J. Hackett, O. Amsterdamska, M. Lynch, & J. Wajcman (Eds.), *The handbook of science and technology studies* (3rd ed., pp. 979–1000). Cambridge, MA and London: The MIT Press.
- Bateman, S. (1998). Biometrics initiatives signal need for digital identification. *Computer Shopper*. Retrieved from <https://www.highbeam.com/doc/1G1-20867818.html>
- Beck, U. (2005). *Power in the global age*. Cambridge: Polity Press.
- Bellanova, R. (2008). The "Prüm Process": The way forward for EU police cooperation and data exchange? In E. Guild & F. Geyer (Eds.), *Security versus Justice? Police and judicial cooperation in the EU* (pp. 203–221). Aldershot: Ashgate.
- Benecke, M. (2002). Coding or non-coding, that is the question. *EMBO Reports*, 3(6), 498–502. <https://doi.org/10.1093/embo-reports/kvf121>
- Bexellius, C., Hoyer, K., & Lynoe, N. (2007). Will forensic use of medical biobanks decrease public trust in healthcare services? Some empirical observations. *Scand J Public Health*, 35, 442–444.
- Bigo, D. (2006). Globalized (in)security: The field and the ban-opticon. In D. Bigo & A. Tsoukala (Eds.), *Terror, insecurity and liberty. Illiberal practices of liberal regimes after 9/11* (pp. 10–48). Abingdon: Routledge. Retrieved from <http://www.people.fas.harvard.edu/~ces/conferences/muslims/Bigo.pdf>
- Bigo, D. (2008). EU Police Cooperation: National Sovereignty framed by European security? In E. Guild & F. Geyer (Eds.), *Security versus Justice? Police and judicial cooperation in the EU* (pp. 91–108). Farnham, UK: Ashgate.
- Bigo, D., Bruggeman, W., Burgess, P., & Mitsilegas, V. (2007). *The Principle of Information Availability*. Paris: CHALLENGE.
- Bijker, W., Hughes, T., & Pinch, T. (1987). *The Social construction of technological systems: new directions in the sociology and history of technology*. (W. Bijker, T. Hughes, & T. Pinch, Eds.) (Anniversar). London: MIT Press.
- Boa, K. (2007). Privacy outside the castle: Surveillance technologies and reasonable

- expectations of privacy in Canadian judicial reasoning. *Surveillance & Society*, 4(4), 329–345. Retrieved from <http://www.surveillance-and-society.org>
- Bogard, W. (2007). Welcome to the society of control: The simulation of surveillance revisited. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 55–78). Toronto: University of Toronto Press.
- Boli, J. (2006). The Rationalization of Virtue and Virtuosity in World Society. In M. Djelic & K. Sahlin-Andersson (Eds.), *Transnational governance. Institutional dynamics of regulation*. Cambridge: Cambridge University Press.
- Borup, M., Brown, N., Konrad, K., & Van Lente, H. (2006). The sociology of expectations in science and technology. *Technology Analysis & Strategic Management*, 18(3/4), 285–298. <https://doi.org/10.1080/09537320600777002>
- Böstrom, M., & Garsten, C. (Eds.). (2008). *Organizing transnational accountability. Mobilization, tools, challenges*. Cheltenham, UK and Northampton, MA, USA: Edward Elgar.
- Böstrom, M., & Klintman, M. (2008). *Eco-standards, product labelling, and green consumerism*. Basingstoke: Palgrave Macmillan.
- Botzem, S., & Dobusch, L. (2012). Standardization cycles: A process perspective on the formation and diffusion of transnational standards. *Organization Studies*, 33(5–6), 737–762. <https://doi.org/10.1177/0170840612443626>
- Botzem, S., & Quack, S. (2006). Contested Rules and Shifting Boundaries: International Standard Setting in Accounting. In M. Djelic & K. Sahlin-Andersson (Eds.), *Transnational governance. Institutional dynamics of regulation*. Cambridge: Cambridge University Press.
- Bourdieu, P. (1977). *Outline of a Theory of Practice*. Cambridge: Cambridge University Press.
- Bourdieu, P. (1984). *Distinction: A Social Critique of The Judgment of Taste*. Cambridge: Harvard University Press.
- Bowker, G., & Star, S. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA and London: The MIT Press. <https://doi.org/10.1109/MAHC.2000.841148>
- Brandão, A. (2010). *E se tu fosses um rapaz? Homo-erotismo feminino e construção social da identidade*. Porto: Edições Afrontamento.
- Brown, M. (2009). *Science in democracy: Expertise, institutions, and representation*. Cambridge, MA and London: MIT Press.
- Brown, N., Kraft, A., & Martin, P. (2006). The Promissory Past of Blood Stem Cells. *BioSocieties*, 1(3), 329–348. <https://doi.org/10.1017/S1745855206003061>
- Brunsson, N., & Jacobsson, B. (Eds.). (2005). *A world of standards*. Oxford: Oxford University Press.
- Brunsson, N., & Olsen, J. (1998). *Organizing Organizations*. Oslo: Fagbokforlaget.
- Burke, A. (2001). *In fear of security*. Annandale, NSW: Pluto Press.
- Bygrave, L. (2002). *Data protection law. Approaching its rationale, logic, and its limits*. The Hague: Kluwer Law International.
- Cabezudo, M. (2013). Assessment of the DNA data protection system in the European framework (The lack of data level protection harmonization at and between the international, European and national levels). In M. Cabezudo (Ed.), *Police DNA databases: Are they truly effective tool in the fight against serious national and cross-border crime?* (pp. 43–62). Madrid: Dykinson.
- Callon, M. (1991). Techno-economic networks and irreversibility. In J. Law (Ed.), *Sociology of*

- monsters: Essays on power, technology and domination* (pp. 132–161). London: Routledge.
- Campbell, C., & Van Brakel, R. (2015). Privacy as a line of flight in societies of mass surveillance. *Ethical Space: International Journal of Communication Ethics*, 12(3–4), 39–46.
- Case of S. and Marper v. The United Kingdom. (2008). Strasbourg. Retrieved from <https://rm.coe.int/168067d216>
- Cavoukian, A. (2001). Public safety is paramount - But balanced against privacy. Ontario: Office of the Information and Privacy Commissioner. Retrieved from <http://www.ontla.on.ca/library/repository/mon/2000/10298479.pdf>
- Chadwick, R., & Berg, K. (2001). Solidarity and equity: New ethical frameworks for genetic databases. *Nature Reviews Genetics*, 2(April), 318–321. <https://doi.org/10.1038/35066094>
- Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: SAGE Publications.
- Charmaz, K. (2009). *A construção da teoria fundamentada: Guia prático para análise qualitativa*. Porto Alegre: Artmed.
- Cho, M., & Sankar, P. (2004). Forensic genetics and ethical, legal and social implications beyond the clinic. *Nature Genetics*, 36(11 Suppl), S8–12. <https://doi.org/10.1038/ng1594>
- Chow-White, P., & Duster, T. (2011). Do health and forensic DNA databases increase racial disparities? *PLoS Medicine*, 8(10), e1001100. <https://doi.org/10.1371/journal.pmed.1001100>
- Clarke, A. (2005). *Situational analysis: Grounded theory after the postmodern turn*. San Francisco: Sage Publications.
- Clarke, R. (2001). Biometrics and privacy. Retrieved from <http://www.rogerclarke.com/DV/Biometrics.html>
- Cochoy, F. (2004). The industrial roots of contemporary political consumerism: The case of the French standardization movement. In M. Micheletti & A. Follesdal (Eds.), *Politics, Products, and Markets. Exploring Political Consumerism Past and Present* (pp. 145–160). New Brunswick, London: Transaction Publishers.
- Cohen, J. (2000). Examined Lives: Informational privacy and the subject as object. *Stanford Law Review*, 52, 1373–1437.
- Cohen, S. (2002). *Folk devils and moral panics*. London: Routledge.
- Cole, S. (2013). Forensic culture as epistemic culture: The sociology of forensic science. *Studies in History and Philosophy of Biological and Biomedical Sciences*, 44(1), 36–46. <https://doi.org/10.1016/j.shpsc.2012.09.003>
- Cole, S., & Lynch, M. (2006). The social and legal construction of suspects. *Annual Review of Law and Social Science*, 2, 39–60. <https://doi.org/10.1146/annurev.lawsocsci.2.081805.110001>
- Collins, R. (1988). *Theoretical Sociology*. San Diego, CA: Harcourt Brace Jovanovich, Publishers.
- Conselho Nacional de Ética para as Ciências da Vida (Ed.). (2012). A Base de Dados de Perfis de DNA em Portugal: Conferências CNECV. In *Coleção Bioética 15* (p. 221). Coimbra. Retrieved from [http://www.cneqv.pt/admin/files/data/docs/1415190079_Livro bioetica_15_Base de dados de perfis de DNA.pdf](http://www.cneqv.pt/admin/files/data/docs/1415190079_Livro_bioetica_15_Base%20de%20dados%20de%20perfis%20de%20DNA.pdf)

- Contini, F., & Mohr, R. (2007). Reconciling independence and accountability in judicial systems. *Utrecht Law Review*, 26-43.
- Costa, S. (2003). *A justiça em laboratório: A identificação por perfis genéticos de ADN. Entre a harmonização transnacional e a apropriação local*. Coimbra: Almedina.
- Costa, S. (2014). Os constrangimentos práticos da investigação criminal em Portugal e suas repercussões na aplicabilidade da base de dados de ADN. In H. Machado & H. Moniz (Eds.), *Bases de dados genéticos forenses: Tecnologias de controlo e ordem social* (pp. 229–267). Coimbra: Coimbra Editores.
- Costa, S. (2017). Visibilities, invisibilities and twilight zones at the crime scene in Portugal. *New Genetics and Society*, 36(4), 375–399. <https://doi.org/10.1080/14636778.2017.1394835>
- Costa, S., & Nunes, J. (2001). As atribuições da ciência «impura»: A harmonização da biologia forense e a diversidade dos sistemas jurídicos. In J. A. Nunes & M. E. Gonçalves (Eds.), *Enteados de Galileu? A semiperiferia no sistema mundial da ciência* (pp. 107–141). Porto: Afrontamento.
- Council of the European Union. (2017). *Working Party on Information Exchange and Data Protection (DAPIX) - Prüm/DNA data exchange evaluation of United Kingdom (UK)*. Brussels. Retrieved from <http://www.statewatch.org/news/2018/jun/eu-council-prum-dp-questions-uk-5309-17.pdf>
- Council of the European Union. (2018a). *Working Party on Information Exchange and Data Protection (DAPIX): Implementation of the provisions on information exchange of the “Prüm Decisions.”* Brussels. Retrieved from http://register.consilium.europa.eu/content/out?lang=EN&typ=SET&i=ADV&ROWSPP=25&RESULTSET=1&NRROWS=500&DOC_LANCD=EN&ORDERBY=DOC_DATE+DESC&DOC_ID=5077%2F18&DOC_TITLE=&CONTENTS=&DOC_SUBJECT=&MEET_DATE=&single_comparator=&single_date=&from_date=&to_date=
- Council of the European Union. (2018b). *Working Party on Information Exchange and Data Protection (DAPIX) - Clarification on DNA concerns raised at previous DAPIX meetings*. Brussels. Retrieved from <http://www.statewatch.org/news/2018/apr/eu-council-dna-concerns-7772-Rev-1-18.pdf>
- Council of the European Union. (2019a). *Council Implementing Decision (EU) 2019/968 of June 2019 on the launch of automated data exchange with regard to DNA data in the United Kingdom*, Official Journal of the European Union. <https://doi.org/10.4324/9780429494512-9>
- Council of the European Union. (2019b). *Working Party on Information Exchange and Data Protection (DAPIX) 5077/18: Implementation of the provisions on information exchange of the “Prüm Decisions.”* Brussels.
- Craig, P., & Búrca, G. de. (2008). *EU Law. Text, cases, and materials*. Oxford: Oxford University Press.
- Crossman, G. (2008). Nothing to hide, nothing to fear? *International Review of Law, Computers & Technology*, 22(1), 115–118. Retrieved from [file:///C:/Users/CES/Documents/Bibliografia do projecto BDDNA/Crossman - 2010 - International Review of Law , Computers & Technology Nothing to hide , nothing to fear.pdf](file:///C:/Users/CES/Documents/Bibliografia%20do%20projecto%20BDDNA/Crossman%20-%202010%20-%20International%20Review%20of%20Law%20,%20Computers%20&%20Technology%20Nothing%20to%20hide%20,%20nothing%20to%20fear.pdf)
- Cunha, M. (2008). Disciplina, controlo, segurança: No rasto contemporâneo de Foucault. In C. Fróis (Ed.), *A sociedade vigilante: Ensaio sobre privacidade, identificação e vigilância* (pp. 67–81). Lisboa: Imprensa de Ciências Sociais.

- Cutler, A. (2002). Private International Regimes and Interfirm Cooperation. In R. Hall & T. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 23 – 42). Cambridge: Cambridge University Press.
- Cutler, A., Haufler, V., & Porter, T. (Eds.). (1999). *Private Authority and International Affairs*. Albany: State University of New York Press.
- Czarniawska, B., & Sevón, G. (Eds.). (1996). Travels of Ideas. In *Translating Organizational Change* (pp. 13–48). Berlin: de Gruyter.
- Czerniawski, A. (2007). From average to ideal: the evolution of the height and weight table in the United States, 1836–1943. *Social Science History*, 31, 273–96.
- Dahl, J., & Sætnan, A. (2009). “It all happened so slowly” – On controlling function creep in forensic DNA databases. *International Journal of Law, Crime and Justice*, 37(3), 83–103. <https://doi.org/10.1016/j.ijlcj.2009.04.002>
- de Hert, P., & Gutwirth, S. (2006). Interoperability of police databases within the EU: An accountable political choice? *International Review of Law, Computers & Technology*, 20(1–2), 21–35. <https://doi.org/10.1080/13600860600818227>
- Dedrickson, K. (2017). Universal DNA databases: a way to improve privacy? *Journal of Law and the Biosciences*, 4(3), 637–647. <https://doi.org/10.1093/jlb/lxx041>
- Derksen, L. (2000). Towards a sociology of measurement: The meaning of measurement error in the case of DNA profiling. *Social Studies of Science*, 30(6), 803–845. <https://doi.org/10.1177/030631200030006001>
- Derksen, L. (2010). Micro/macro translations: The production of new social structures in the case of DNA profiling. *Sociological Inquiry*, 80(2), 214–240. <https://doi.org/10.1111/j.1475-682X.2010.00328.x>
- Dias, F. (2007). *Direito Penal. Parte Geral. Tomo I. Questões fundamentais: A Doutrina Geral do Crime*. Coimbra: Coimbra Editora.
- Dierickx, K. (2008). A Belgian perspective - Forum on the Nuffield report “The forensic use of bioinformation: Ethical Issues.” *BioSocieties*, 3(1), 97–99. <https://doi.org/10.1017/S1745855208006005>
- Dijck, J. van. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208.
- Djelic, M., & Sahlin-Andersson, K. (Eds.). (2006). *Transnational governance. Institutional dynamics of regulation*. Cambridge: Cambridge University Press.
- Downey, J., Stephens, M., & Flaherty, J. (2012). The ‘sluice-gate’ public sphere and the national DNA database in the UK. *Media, Culture & Society*, 34(4), 439–456. <https://doi.org/10.1177/0163443711436357>
- Durkheim, É. (1999). *Da divisão do trabalho social*. São Paulo: Martins Fontes.
- Duster, T. (2004). Selective arrests, an ever-expanding DNA forensic database, and the specter of an early-twenty-first-century equivalent of phrenology. In D. Lazer (Ed.), *The technology of justice: DNA and the criminal justice system* (pp. 315–334). Cambridge: MIT Press.
- Duster, T. (2006). The molecular reinscription of race: Unanticipated issues in biotechnology and forensic science. *Patterns of Prejudice*, 40(4–5), 427–441. <https://doi.org/10.1080/00313220601020148>
- Dyer, R. (1997). *White*. New York and London: Routledge.
- Eisele, K. (2018). *Interoperability between EU information systems for security, border and migration management: establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*

- (COM(2017) 794).
- Epstein, S. (2007). *Inclusion: The Politics of Difference in Medical Research*. Chicago: University Chicago Press.
- Epstein, S. (2009). Beyond the standard human? In *Standards and their Stories: How quantifying, classifying, and formalizing practices shape everyday life* (pp. 35–53). Ithaca, NY: Cornell Univ. Press.
- European Data Protection Supervisor. (2006). *Annual report: Consolidating the EDPS. European Data Protection Supervisor* (Vol. 34). Luxembourg.
- Feldman, R. (2003). Considerations on the emerging implementation of biometric technology. *Hastings Communications & Entertainment Law Journal*, 25, 653–682. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/hascom25&section=21
- Finn, R., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Poullet (Eds.), *European data protection: Coming of age* (pp. 3–32). Dordrecht: Springer Netherlands. <https://doi.org/10.1007/978-94-007-5170-5>
- Fiodorova, A. (2014). DNA for crime investigation: European co-operation model. *Recent Advances in DNA and Gene Sequences*, 8(2), 126–133.
- Forsberg, J., Hansson, M., & Eriksson, S. (2009). Changing perspectives in biobank research: from individual rights to concerns about public health regarding the return of results. *Eur J Hum Genet*, 17, 1544–9.
- Forensic Science Regulator. (2014). *Protocol: DNA contamination detection -The management and use of staff elimination DNA databases (FSR-P-302)*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/355995/DNAcontaminationDetection.pdf
- Foucault, M. (1977). *Discipline and punishment: the birth of prison*. New York: Vintage.
- Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in Governmentality* (pp. 87–104). Chicago: University of Chicago Press.
- Foucault, M. (1994 [1976]). *História da sexualidade. A vontade de saber vol.1*. Lisboa: Relógio d'Água.
- Fox, R., Sickel, R., & Steiger, T. (2007). *Tabloid justice. Criminal justice in an age of media frenzy*. Boulder, CO: Lynne Rienner Publishers.
- Frois, C. (Ed.). (2008). *A sociedade vigilante. Ensaio sobre identificação, vigilância e privacidade*. Lisboa: Mundos Sociais.
- Fujimura, J. (2003). Future Imaginaries: Genome Scientists as Socio-Cultural Entrepreneurs. In A. H. Goodman, D. Heath, & M. S. Lindee (Eds.), *Genetic Nature/Culture: Anthropology and Science Beyond the Two Culture Divide* (pp. 176–199). Berkeley, CA: University of California Press.
- Gamero, J., Romero, J., Peralta, J., Corte-Real, F., Guillén, M., & Anjos, M.. (2008). A study of Spanish attitudes regarding the custody and use of forensic DNA databases. *Forensic Science International*, 2(2), 138–149. <https://doi.org/10.1016/j.fsigen.2007.10.201>
- Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview Press.
- Gandy, O. (2007). Data mining, surveillance, and discrimination in the post-9/11 environment. In K Haggerty & R. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 363–384). Toronto: University of Toronto Press.
- Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st Century*. Sebastopol:

- O'Reilly.
- Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford: Oxford University Press.
- Garland, D. (2008). On the concept of moral panic. *Crime, Media, Culture*, 4(1), 9–30. <https://doi.org/10.1177/1741659007087270>
- Gaskell, G., Stares, S., Allansdottir, A., Allum, N., Castro, P., Esmer, Y., . . . Wagner, W. (2010). *Europeans and Biotechnology in 2010: Winds of Change?* Retrieved from http://ec.europa.eu/research/science-society/document_library/pdf_06/europeans-biotechnology-in-2010_en.pdf
- Gavison, R. (1980). Privacy and the Limits of the Law. *Yale Law Journal*, 89, 421–471.
- Gieryn, T. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review*, 48(6), 781–795.
- Gilbert, N. (2007). *Dilemmas of privacy and surveillance: Challenges of technological change*. London.
- Gilliom, J. (2007). Struggling with surveillance: Resistance, consciousness, and identity. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 111–129). Toronto: University of Toronto Press.
- Gonçalves, M. (2018). Quem controla os nossos dados? *Público*, pp. 1–5.
- Gonçalves, M., & Jesus, I. (2012). Security and personal data protection in the European Union: Challenging trends from a Human Rights' perspective. *Human Security Perspectives*, 9(1), 117–144.
- Gonçalves, M., & Jesus, I. (2013). Security policies and the weakening of personal data protection in the European Union. *Computer Law & Security Review*, 29(October 1995), 255–263. <https://doi.org/10.1016/j.clsr.2013.03.008>
- Goode, E., & Ben-Yehuda, N. (1994). *Moral panics: The social construction of deviance*. Oxford: Blackwell.
- Goold, B. (2009). Surveillance and the political value of privacy. *Amsterdam Law Forum*, 1(4).
- Goos, K., Friedewald, M., William, C., Webster, R., & Leleux, C. (2015). The co-evolution of surveillance technologies and surveillance practices. In David Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 51–100). London: Routledge.
- Gottweis, H. (1998). *Governing molecules: The discursive politics of genetic engineering in Europe and in the United States*. Cambridge, MA: MIT Press.
- Granja, R., & Machado, H. (2019). Ethical Controversies of Familial Searching: The Views of Stakeholders in the United Kingdom and in Poland. *Science, Technology, & Human Values*, 44(6), 1068–1092. <https://doi.org/10.1177/0162243919828219>
- Guillén, M., Lareu, M., Pestoni, C., Salas, A., & Carracedo, Á. (2000). Ethical-legal problems of DNA databases in criminal investigation. *Journal of Medical Ethics*, 26, 266–271.
- Guston, D. (2014). Understanding “anticipatory governance.” *Social Studies of Science*, 44(2), 218–242. <https://doi.org/10.1177/0306312713508669>
- Haas, P. (1989). Do regimes matter? Epistemic communities and Mediterranean pollution control. *International Organization*, 43(3), 377–403. <https://doi.org/10.1017/S0020818300032975>
- Haas, P. (1992). Introduction: Epistemic Communities and International Policy Coordination. *International Organization*, 46(1), 1–35.
- Hacking, I. (1999). *The Social Construction of What?* Cambridge, MA: Harvard University Press.

- Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *The British Journal of Sociology*, 51(4), 605–622. <https://doi.org/10.1080/00071310020015280>
- Haggerty, K., & Ericson, R. (2007). The new politics of surveillance and visibility. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 3–25). Toronto: University of Toronto Press.
- Hall, R., & Biersteker, T. (Eds.). (2002). *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press.
- Hallström, K. (2004). *Organizing international standardization – ISO and the IASC in question of authority*. Cheltenham, UK, and Northampton, MA, USA: Edward Elgar.
- Hallström, K., & Boström, M. (2010). *Transnational multi-stakeholder standardization: Organizing fragile non-state authority*. Cheltenham, UK and Northampton, MA: Edward Elgar Publishing.
- Hancher, L., & Moran, M. (1989). Organizing regulatory space. In L. Hancher & M. Moran (Eds.), *Capitalism, culture, and economic regulation* (pp. 211–300). Oxford, UK: Clarendon Press.
- Haraway, D. (1991). *Simians, cyborgs, and women: The reinvention of nature*. London: Free Associations Books.
- Harbo, T. (2010). The function of the proportionality principle in EU law. *European Law Journal*, 16(2), 158–185. <https://doi.org/10.1111/j.1468-0386.2009.00502.x>
- Hauge, M., Stevenson, M., Rossmo, K., & Le Comber, S. (2016). Tagging Banksy: using geographic profiling to investigate a modern art mystery. *Journal of Spatial Science*, 61(6), 185–190.
- Hedgecoe, A., & Martin, P. (2003). The drugs don't work: Expectations and the shaping of pharmacogenetics. *Social Studies of Science*, 33(3), 327–364. <https://doi.org/10.1177/03063127030333002>
- Heinemann, T., Lemke, T., & Prainsack, B. (2012). Risky profiles: Societal dimensions of forensic uses of DNA profiling technologies. *New Genetics and Society*, 31(3), 249–258. <https://doi.org/10.1080/14636778.2012.687132>
- Hert, P. de. (2005). *Biometrics: Legal issues and implications*. Sevilla.
- Higgott, R., Underhill, G., & Bieler, A. (Eds.). (2000). *Non-state actors and. Authority in the global system*. London: Routledge.
- Hijmans, H. (2006). The Third Pillar in practice: coping with inadequacies-information sharing between Member States. Discussion paper for the meeting of the Netherlands Association for European Law (Nederlandse Vereniging voor Europees Recht, NVER).
- Hindmarsh, R. (2010). Biosurveillance and biocivic concerns, from “truth” to “trust”: The Australian forensic DNA terrain. In R. Hindmarsh & B. Prainsack (Eds.), *Genetic suspects: Global governance of forensic DNA profiling and databasing* (pp. 262–287). Cambridge: Cambridge University Press.
- Hindmarsh, R., & Prainsack, B. (2010). *Genetic suspects: Global governance of forensic DNA profiling and databasing*. (R. Hindmarsh & B. Prainsack, Eds.). Cambridge: Cambridge University Press.
- Hoeyer, K., Tupasela, A., & Rasmussen, M. (2016). Ethics policies and ethics work in cross-national genetic research and data sharing: Flows, nonflows, and overflows. *Science, Technology, & Human Values*, 42(3), 1–24. <https://doi.org/10.1177/0162243916674321>
- Home Office. (2017). *National DNA Database Strategy Board Annual Report 2015/16*. London. Retrieved from

- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/594185/58714_Un-Num_Nat_DNA_DB_Accessible.pdf
- House of Commons Hansard Debates. (2013). 15 July 2013, London. Retrieved from <https://publications.parliament.uk/pa/cm201314/cmhansrd/cm130715/debtext/130715-0001.htm>
- House of Lords. (2007). *Prüm: An effective weapon against terrorism and crime? Home Office*. London.
- House of Lords. (2013). *EU police and criminal justice measures: The UK's 2014 opt-out decision*. London.
- Hoven. (2001). Privacy and the varieties of moral Wrongdoing. In Spinello & Tavani (Eds.), *Readings in Cyberethics* (pp. 430–443). Sudbury: Bartlett & Jones.
- Hufnagel, S. (2012). Harmonising police cooperation laws in Australia and the European Union: The tension between local/national and national/supranational interests. *Australian Journal of Forensic Sciences*, 44(1), 45–62. <https://doi.org/10.3109/14756366.2014.1003216>
- Hufnagel, S., & McCartney, C. (2015). Police cooperation against transnational criminals. In N. Boister & R. J. Currie (Eds.), *Routledge handbook of transnational criminal law* (pp. 107–120). Oxon and New York: Routledge.
- Hufnagel, S., & McCartney, C. (Eds.). (2017). *Trust in international police and justice cooperation*. Oxford: Hart Publishing.
- Human Genetics Commission. (2001). *Whose hands on your genes? A discussion document on the storage protection and use of personal genetic information*. London.
- Human Genetics Commission. (2009). *Nothing to hide, nothing to fear? Balancing individual rights and the public interest in the governance and use of the National DNA Database*.
- Hustinx, P. (2010). EU data protection law - Current state and future perspectives. *Ethical Dimensions of Data Protection and Privacy*. Tallin, Estonia.
- Igo, S. (2007). *The Averaged American: Surveys, Citizens, and the Making of a Mass Public*. Cambridge, MA: Harvard University Press.
- Innes, M., Fielding, N., & Cope, N. (2005). "The appliance of science?": The theory and practice of crime intelligence analysis. *British Journal of Criminology*, 45(1), 39–57. <https://doi.org/10.1093/bjc/azh053>
- INTERPOL. (2009). *Handbook on DNA data and practice - Recommendations from the INTERPOL DNA monitoring expert group*. Lyon.
- IRISS. (2012). *Surveillance, fighting crime and violence*. Retrieved from http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf
- Jasanoff, S. (1990). *The fifth branch: Science advisers as policymakers*. Cambridge: Harvard University Press.
- Jasanoff, S. (1995). *Science at the bar. Law, science, and technology in America*. Cambridge, MA and London, UK: Harvard University Press.
- Jasanoff, S. (Ed.). (2004). *States of knowledge. The co-production of science and social order*. London and New York: Routledge. <https://doi.org/10.4324/9780203413845>
- Jasanoff, S. (2005). *Designs on nature: Science and democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.
- Jasanoff, S. (2006). Just evidence: The limits of science in the legal process. *Journal of Law, Medicine & Ethics*, 34(2), 328–341. <https://doi.org/10.1111/j.1748-720X.2006.00038.x>
- Jasanoff, S. (2011). *Reframing rights. Bioconstitutionalism in the genetic age*. (S. Jasanoff,

- Ed.). Chicago: MIT Press.
- Jasanoff, S., Kim, S., & Perling, S. (2007). *Sociotechnical Imaginaries and Science and Technology Policy: A cross-national comparison*.
- Jasanoff, S., & Kim, S. (2009). Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva*, 47(2), 119–146. <https://doi.org/10.1007/s11024-009-9124-4>
- Jasanoff, S., Markle, J., Petersen, J., & Pinch, T. (1995). *Handbook of science and technology studies*. Thousand Oaks: Sage Publications. Retrieved from <https://us.sagepub.com/en-us/nam/handbook-of-science-and-technology-studies/book225385#reviews>
- Johnson, P., & Williams, R. (2004). DNA and crime investigation: Scotland and the 'UK National DNA Database.' *Scottish Journal of Criminal Justice Studies*, 10, 71–84. Retrieved from <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1408072/pdf/nihms-6806.pdf>
- Johnson, P., & Williams, R. (2007). Internationalizing new technologies of crime control: Forensic DNA databasing and datasharing in the European Union. *Policing & Society*, 17(2), 103–118. <https://doi.org/10.1080/10439460701302669>
- Jones, R., & Raab, C. (2015). Effects of surveillance on civil liberties and fundamental rights in Europe – Good practice in privacy design: some examples. In D Wright & R. Kreissl (Eds.), *Surveillance in Europe*. London: Routledge.
- Jordan, K., & Lynch, M. (1998). The dissemination, standardization and routinization of a molecular biological technique. *Social Studies of Science*, 28(5–6), 773–800. <https://doi.org/10.1177/030631298028005005>
- Jordana, J., & Levi-Faur, D. (Eds.). (2004). *The Politics of Regulation*. Cheltenham, UK: Edward Elgar.
- Jornal Oficial da União Europeia. (2008). Decisão 2008/616/JAI do conselho de 23 de Junho de 2008 referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras.
- Katzenstein, P., Keohane, R., & Krasner, S. (1999). International Organizations and the Study of World Politics. In P. Katzenstein, R. Keohane, & S. Krasner (Eds.), *Explorations and Contestations in the Study of World Politics* (pp. 5–46). Cambridge: The MIT Press.
- Kekk, M., & Sikkink, K. (1998). *Activist beyond borders: Advocacy networks in international politics*. London: Cornell University Press.
- Kerwer, D. (2005). Rules that many use: Standards and global regulation. *Governance*, 18, 611–632.
- Kierkegaard, S. (2008). The Prüm decision - An uncontrolled fishing expedition in "Big Brother" Europe. *Computer Law and Security Report*, 24(3), 243–252. <https://doi.org/10.1016/j.clsr.2008.03.002>
- Kietz, D., & Maurer, A. (2006). From Schengen to Prüm. Deeper integration through enhanced cooperation or signs of fragmentation in the EU? *SWP - Stiftung Wissenschaft Und Politik*, (May), 1–5.
- Kim, E. (2018). Sociotechnical Imaginaries and the Globalization of Converging Technology Policy: Technological Developmentalism in South Korea. *Science as Culture*, 27(2), 175–197. <https://doi.org/10.1080/09505431.2017.1354844>
- Kirton, J., & Trebilcock, M. (2004). *Hard Choices, Soft Law: Voluntary Standards in Global Trade, Environment and Social Governance*. Aldershot: Ashgate.
- Knorr-Cetina, K. (1999). *Epistemic cultures. How the sciences make knowledge*. Cambridge,

- MA; London, UK: Harvard University Press.
- Kobrin, S. (2002). Economic Governance in an Electronically Networked Global Economy. In R. Hall & T. Biersteker (Eds.), *The Emergence of Private Authority in Global Governance* (pp. 43 – 75). Cambridge: Cambridge University Press.
- Kreissl, R., Norris, C., Krlic, M., Groves, L., & Amicelle, A. (2015). Surveillance - preventing and detecting crime and terrorism. In D Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 150–210). London: Routledge.
- Krimsky, S., & Simoncelli, T. (2011). *Genetic justice: DNA data banks, criminal investigations, and civil liberties*. New York: Columbia University Press.
- Krislov, S. (1997). *How Nations Choose Product Standards and Standards Change Nations*. Pittsburgh, PA: University Pittsburgh Press.
- Lampland, M., & Star, S. (Eds.). (2009). *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life*. Ithaca: Cornell University Press.
- Latour, B. (1987a). Centres of calculation. In B. Latour (Ed.), *Science in Action: How to Follow Scientists and Engineers Through Society* (pp. 215–257). Cambridge, MA: Harvard University Press.
- Latour, B. (1987b). *Science in action. How to follow scientists and engineers through society*. Cambridge, MA: Harvard University Press.
- Latour, B. (1988). *The Pasteurization of France*. Cambridge, MA: Harvard University Press.
- Law, J. (2008). On sociology and STS. *Sociological Review*, 56(4), 623–649. <https://doi.org/10.1111/j.1467-954X.2008.00808.x>
- Law, J. (2009). Actor network theory and material semiotics. In B. Turner (Ed.), *The New Blackwell companion to social theory*. Chichester: John Wiley & Sons, Ltd.
- Lawless, C. (2011). Policing markets: The contested shaping of neo-liberal forensic science. *British Journal of Criminology*, 51(4), 671–689. <https://doi.org/10.1093/bjc/azr025>
- Lawrence, L. (1999). *Code and other laws of cyberspace* (2nd ed.). New York: Basic Books.
- Lazer, D. (2004). Introduction: DNA and the criminal justice system. In David Lazer (Ed.), *DNA and the criminal justice system: The technology of justice* (pp. 3–12). Cambridge, MA: MIT Press.
- Lengwiler, M. (2009). Double standards: the history of standardizing humans in modern life insurance. In M. Lampland & S. Star (Eds.), *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life* (pp. 95–113). Ithaca, NY: Cornell Univ. Press.
- Lentzos, F. (2006). Rationality, risk and response: A research agenda for biosecurity. *BioSocieties*, 1(4), 453–464. Retrieved from http://journals.cambridge.org/abstract_S1745855206004066
- Levenda, A. , Richter, J., Miller, T., & Fisher, E. (2018). Regional sociotechnical imaginaries and the governance of energy innovations. *Futures*. <https://doi.org/10.1016/j.futures.2018.03.001>
- Lewin, K. (1951). *Field Theory in Social Science: Selected Theoretical Papers*. (D. Cartwright, Ed.). New York: Harper & Row.
- Liu, N. (2013). *Bio-privacy: Privacy regulations and the challenge of biometrics*. Abingdon: Routledge.
- Lynch, M. (2002). Protocols, practices, and the reproduction of technique in molecular biology. *The British Journal of Sociology*, 53(2), 203–220. <https://doi.org/10.1080/00071310220133304>

- Lynch, M. (2012). *Science and technology studies: Critical concepts in the social sciences*. London and New York: Routledge.
- Lynch, M. (2013). Science, truth, and forensic cultures: The exceptional legal status of DNA evidence. *Studies in History and Philosophy of Biological and Biomedical Sciences*, 44(1), 60–70. <https://doi.org/10.1016/j.shpsc.2012.09.008>
- Lynch, M., Cole, S., McNally, R., & Jordan, K. (2008). *Truth machine: The contentious history of DNA fingerprinting*. Chicago: University of Chicago Press.
- Lynch, M., & McNally, R. (2009). Forensic DNA databases: The co-production of law and surveillance technology. In P. Atkinson, P. Glasner, & M. Lock (Eds.), *Handbook of genetics and society: Mapping the new genomics era* (pp. 283–301). London: Routledge.
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.
- Lyon, D. (2003). *Surveillance after September 11*. Cambridge: Polity Press.
- Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology*, 19(2), 135–149. <https://doi.org/10.1177/0268580904042897>
- Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.
- Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, 1(2), 1–13. <https://doi.org/10.1177/2053951714541861>
- Lyon, D. (2015). The Snowden Stakes: Challenges for understanding surveillance today. *Surveillance & Society*, 13(2), 139–152. <https://doi.org/10.24908/ss.v13i2.5363>
- Machado, H. (2005). Dilemas e paradoxos da cientifização da justiça em Portugal - O caso dos perfis genéticos de ADN. *Manifesto*, 7, 64–75. Retrieved from <http://hdl.handle.net/1822/4495>
- Machado, H. (2011). Construtores da bio(in)segurança na base de dados de perfis de ADN. *Etnográfica*, 15(1), 153–166.
- Machado, H. (2012). Prisoners' views of CSI's portrayal of forensic identification technologies: A grounded assessment. *New Genetics and Society*, 31(3), 271–284. <https://doi.org/10.1080/14636778.2012.687086>
- Machado, H. (2016). Das bases de dados genéticos na investigação criminal: O debate nas ciências sociais e estudos empíricos em Portugal. In M. Cunha (Ed.), *Do crime e do castigo: Temas e debates contemporâneos* (pp. 163–179). Lisboa: Mundos Sociais.
- Machado, H., Alves, B., & Silva, S. (2015). Proteção de dados pessoais em biobancos médicos e forenses: “solidariedade” e reconfigurações da participação pública. In C. Fonseca & H. Machado (Eds.), *Ciência, identificação e tecnologias de governo* (pp. 56–74). Porto Alegre: Editora da UFRGS/CEGOV.
- Machado, H., & Costa, S. (2012). Biolegalidade, imaginário forense e investigação criminal. *Revista Crítica de Ciências Sociais*, 97(Junho), 61–84. Retrieved from <http://rccs.revues.org/4927>
- Machado, H., & Costa, S. (2013). Biolegality, the forensic imaginary and criminal investigation. *Revista Crítica de Ciências Sociais*, 5(5), 84–105.
- Machado, H., & Granja, R. (2018). Ethics in Transnational Forensic DNA Data Exchange in the EU: Constructing Boundaries and Managing Controversies. *Science as Culture*, 27(2), 242–264. <https://doi.org/10.1080/09505431.2018.1425385>
- Machado, H., & Granja, R. (2019a). Police epistemic culture and boundary work with judicial authorities and forensic scientists: the case of transnational DNA data exchange in the EU. *New Genetics and Society*, 38(3), 289–307.

- <https://doi.org/10.1080/14636778.2019.1609350>
- Machado, H., & Granja, R. (2019b). Risks and benefits of transnational exchange of forensic DNA data in the EU: The views of professionals operating the Prüm system. *Journal of Forensic and Legal Medicine*, 68, 101872. <https://doi.org/10.1016/J.JFLM.2019.101872>
- Machado, H., Martins, M., & Matos, S. (2013). Base de dados genéticos forense em Portugal e identidades tecnocientíficas. Análise a partir de grupos focais com estudantes universitários. *Oficina Do CES*, 403, 1–21.
- Machado, H., Moniz, H., Santos, F., & Silva, S. (2011). *Bases de dados genéticos com fins forenses: Análise comparativa de legislação europeia*. Coimbra. Retrieved from http://dnadatabase.ces.uc.pt/list_documents.php
- Machado, H., & Prainsack, B. (2012). *Tracing technologies: Prisoners' views in the era of CSI*. Farnham, UK: Ashgate.
- Machado, H., & Prainsack, B. (2014). *Tecnologias que incriminam: Olhares de reclusos na Era do CSI*. Coimbra: Almedina.
- Machado, H., & Santos, F. (2016). Culturas de objetividade, epistemologias cívicas e o suspeito transnacional. Uma proposta para mapeamentos teóricos em estudos sociais da genética forense. In C. Fonseca, F. Rohden, P. Machado, & H. Paim (Eds.), *Antropologia da ciência e da tecnologia: Dobras reflexivas* (pp. 179–203). Porto Alegre: Editora Sulina.
- Machado, H., Santos, F., & Silva, S. (2011). Prisoners' expectations of the national forensic DNA database: Surveillance and reconfiguration of individual rights. *Forensic Science International*, 210(1–3), 139–143. <https://doi.org/10.1016/j.forsciint.2011.02.020>
- Machado, H., & Silva, S. (2008a). A Portuguese perspective – Forum on the Nuffield report “The forensic use of bioinformation: Ethical issues.” *BioSocieties*, 3(1), 99–101. <https://doi.org/10.1017/S1745855208006017>
- Machado, H., & Silva, S. (2008b). Confiança, voluntariedade e supressão dos riscos: Expectativas, incertezas e governação das aplicações forenses. In C. Frois (Ed.), *A sociedade vigilante: Ensaio sobre privacidade, identificação e anonimato* (pp. 151–174). Lisboa: Imprensa de Ciências Sociais.
- Machado, H., & Silva, S. (2010). Portuguese forensic DNA database: Political enthusiasm, public trust and probable issues in future practice. In R. Hindmarsh & B. Prainsack (Eds.), *Genetic suspects: Global governance of DNA profiling and databasing* (pp. 218–239). Cambridge: Cambridge University Press.
- Machado, H., & Silva, S. (2014a). Identidades tecnocientíficas na esfera forense e médica: Perspectivas de cidadãos sobre inserção de perfil genético em base de dados e acerca de doação de embriões para investigação. In H. Machado & H. Moniz (Eds.), *Bases de dados genéticos forenses: Tecnologias de controlo e ordem social* (pp. 23–45). Coimbra: Coimbra Editora.
- Machado, H., & Silva, S. (2014b). “Would you accept having your DNA profile inserted in the National Forensic DNA database? Why?” Results of a questionnaire applied in Portugal. *Forensic Science International: Genetics*, 8(1), 132–136. <https://doi.org/10.1016/j.fsigen.2013.08.014>
- Machado, H., & Silva, S. (2015a). Public participation in genetic databases: Crossing the boundaries between biobanks and forensic DNA databases through the principle of solidarity. *Journal of Medical Ethics*, 41(10), 820–824. <https://doi.org/10.1136/medethics-2014-102126>
- Machado, H., & Silva, S. (2015b). Public perspectives on risks and benefits of forensic DNA

- databases: An approach to the influence of professional group, education, and age. *Bulletin of Science, Technology & Society*, 35(1–2), 16–24.
- Machado, H., & Silva, S. (2016). Voluntary participation in forensic DNA databases: Altruism, resistance, and stigma. *Science, Technology, & Human Values*, 41(2), 322–343. <https://doi.org/10.1177/0162243915604723>
- Machado, H., Silva, S., & Amorim, A. (2010). Políticas de identidade: Perfil de DNA e a identidade genético-criminal. *Análise Social*, XLV(196), 537–553.
- Machado, H., Silva, S., & Cunha, M. (2012). Multiple views of DNA surveillance: The surveilled, the surveillants and the academics. In G. Walle, E. Herrewegen, & N. Zurawski (Eds.), *Crime, security and surveillance. Effects for the surveillant and the surveilled* (pp. 179–194). The Hague: Boom Eleven Publishers.
- Machado, H., Silva, S., & Santos, F. (2008). *Justiça tecnológica: promessas e desafios*. Ermesinde: Ecopsy.
- Maciel, D., & Machado, H. (2014). Biovigilância e governabilidade nas sociedades da informação. In H. Machado & H. Moniz (Eds.), *Bases de dados genéticos forenses: Tecnologias de controlo e ordem social* (pp. 141–166). Coimbra: Coimbra Editora.
- Mackenzie, D. (1996). *Knowing machines: Essays on technical change*. Cambridge: MIT Press.
- Majone, G. (Ed.). (1996). *Regulating Europe*. London: Routledge.
- Maras, M. (2012). The social consequences of a mass surveillance measure: What happens when we become the ‘others’? *International Journal of Law, Crime and Justice*, 40(2), 65–81. <https://doi.org/10.1016/j.ijlcj.2011.08.002>
- Marx, G. (1988). *Undercover: Police surveillance in America*. University of California Press.
- Marx, G. (2006). Soft surveillance: The growth of mandatory volunteerism in collecting personal information - “Hey buddy can you spare a DNA?” *Lex Electronica*, 10(3), 10.
- Marx, G. (2007). Varieties of Personal Information as Influences on Attitudes towards Surveillance. In Kevin Haggerty & R. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 79–110). Toronto: University of Toronto Press.
- Marx, G. (2008). Vigilância soft - o crescimento da voluntariedade obrigatória na recolha de dados pessoais: «ó amigo, empresta-me uma amostra de ADN?». In C. Frois (Ed.), *A sociedade vigilante: Ensaio sobre privacidade, identificação e vigilância* (pp. 87–109). Lisboa: Imprensa de Ciências Sociais.
- Marx, G., & Muschert, G. (2007). Personal information, borders, and the new surveillance studies. *Annual Review of Law and Social Science*, 3(1), 375–395. <https://doi.org/10.1146/annurev.lawsocsci.3.081806.112824>
- Mason, M. (2005). *The new accountability. Environmental responsibility across borders*. London: Earthscan.
- Matos, S. (2013). *Base de dados de perfis de DNA com propósitos forenses em Portugal: questões de âmbito ético, prático e político Perspetivas de estudantes das ciências da vida e exactas*. Universidade do Minho.
- Matos, S. (2019). Privacy and data protection in the surveillance society: The case of the Prüm system. *Journal of Forensic and Legal Medicine*, 66, 155–161. <https://doi.org/10.1016/j.jflm.2019.07.001>
- Mayntz, R. (2010). Legitimacy and compliance in transnational governance. Cologne: Max Planck Institute for the Study of Societies.
- Mayring, P. (2004). Qualitative content analysis. In U. Flick, E. von Kardorff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 266–269). London: Sage.

- McCartney, C. (2004). Forensic DNA sampling and the England and Wales National DNA Database: A sceptical approach. *Critical Criminology*, 12(2), 157–178. <https://doi.org/10.1023/B:CRIT.0000040255.29101.7a>
- McCartney, C. (2006a). *Forensic identification and criminal justice: Forensic science, justice and risk*. Cullompton: Willan Publishing.
- McCartney, C. (2006b). The DNA expansion programme and criminal investigation. *British Journal of Criminology*, 46(2), 175–192. <https://doi.org/10.1093/bjc/azi094>
- McCartney, C. (2010). Trans-national exchange offorensic (Bio)information. In G. Bruinsma & D. Weisburd (Eds.), *Emerging Issues in International Forensic Bioinformation Exchange* (pp. 1–27). University of Leeds, London: Springer.
- McCartney, C. (2012). Of weighty reasons and indiscriminate blankets: The retention of DNA for forensic purposes. *The Howard Journal of Criminal Justice*, 51(3), 245–260. <https://doi.org/10.1111/j.1468-2311.2012.00717.x>
- McCartney, C. (2013). Opting in and opting out: Doing the hokey cokey with EU policing and judicial cooperation. *The Journal of Criminal Law*, 77, 543–561. <https://doi.org/10.1350/jcla.2013.77.6.879>
- McCartney, C. (2014a). Forensic data exchange: Ensuring integrity. *Australian Journal of Forensic Sciences*, 47(1), 36–48. <https://doi.org/10.1080/00450618.2014.906654>
- McCartney, C. (2014b). Transnational exchange of forensic evidence. In Gerben Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 5302–5313). New York: Springer. <https://doi.org/10.1007/978-1-4614-5690-2>
- McCartney, C. (2017). Trust and the international exchange of forensic information. In S. Hufnagel & C. McCartney (Eds.), *Trust in International Police and Justice Cooperation* (pp. 169–189). Oxford and Portland, Oregon: Bloomsbury.
- McCartney, C., Williams, R., & Wilson, T. (2010). *The future of forensic bioinformation - Executive summary*. Leeds.
- McCartney, C., Wilson, T., & Williams, R. (2011). Transnational exchange of forensic DNA: Viability, legitimacy, and acceptability. *European Journal on Criminal Policy and Research*, 17(4), 305–322. <https://doi.org/10.1007/s10610-011-9154-y>
- Metcalf, J., & Crawford, K. (2016). Where are human subjects in Big Data research? The emerging ethics divide. *Big Data & Society*, (June), 1–14. <https://doi.org/10.1177/2053951716650211>
- Meyer, J. (1996). Otherhood: The Promulgation and Transmission of Ideas in the Modern Organizational Environment. In B. Czarniawska & G. Sevón (Eds.), *Translating Organizational Change* (pp. 241 – 252). Berlin: de Gruyter.
- Meyer, J., & Jepperson, R. (2000). The “actors” of modern society: The cultural construction of social agency. *Sociological Theory*, 18(1), 100–120.
- Miranda, D. (2015). Criminal investigation through the eye of the detective: Technological innovation and tradition. *Surveillance & Society*, 13(3), 422–436.
- Mnookin, J. (2008). Of black boxes, instruments, and experts: Testing the validity of forensic science. *Episteme*, 5(3), 343–358. <https://doi.org/10.3366/E1742360008000440>
- Monahan, T. (2010). *Surveillllance in the time of insecurity*. New Brunswick, NJ: Rutgers University Press.
- Moniz, H. (2009). A base de dados de perfis de ADN para fins de identificação civil e criminal e a cooperação transfronteiras em matéria de transferência de perfis de ADN. *Revista Do Ministério Público*, 120(Oct/Dez), 145–156.
- Mostert, M., Bredenoord, A., van der Slootb, B., & van Delden, J. (2017). From privacy to

- data protection in the EU: Implications for big data health research. *European Journal of Health Law*, 25(1), 43–55. <https://doi.org/10.1163/15718093-12460346>
- Murphy, E. (2007). The new forensics: Criminal justice, false certainty, and the second generation of scientific evidence. *California Law Review*, 95(3), 721–797. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/calr95&section=24
- Murphy, E. (2018). Forensic DNA typing. *Annual Review of Criminology*, 1(October 2017), 13.1–13.19. Retrieved from <http://www.annualreviews.org/doi/10.1146/annurev-criminol-032317-092127>
- Murtuja, B., Adris, K., & Ahmed, J. (2008). *A Citizens' Inquiry into the Forensic Use of DNA and the National DNA database*. Citizens' Report. Blackburn, UK.
- Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: The Challenges of Information Technology. *Ethics and Behavior*, 7(3), 207–219.
- Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of privacy in Public. *Law and Philosophy*, 17, 559–596.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.
- Nuffield Council on Bioethics. (2007). *The forensic use of bioinformation: Ethical issues*. London.
- Nunes, J. (1992). *As teias da família: A construção interaccional das solidariedades primárias*. Coimbra: Dissertação de Doutoramento apresentada à Universidade de Coimbra.
- O'Connell, J. (1993). Metrology: The creation of universality by the circulation of particulars. *Social Studies of Science*, 23(1), 129–173. <https://doi.org/10.1177/030631293023001005>
- O'Neill, M. (2010). The issue of data protection and data security in the (Pre-Lisbon) EU Third Pillar. *Journal of Contemporary European Research*. Retrieved from <http://www.jcer.net/index.php/jcer/article/view/264>
- O'Neill, M., & Loftus, B. (2013). Policing and the surveillance of the marginal: Everyday contexts of social control. *Theoretical Criminology*, 17(4), 437–454. <https://doi.org/10.1177/1362480613495084>
- Paton-Simpson, E. (2000). Privacy and the reasonable paranoid: The protection of privacy in public places. *University of Toronto Law*, 50(3), 305–346.
- Pattberg, P. (2007). *Private institutions and global governance. The new politics of environmental sustainability*. Cheltenham: Edward Elgar.
- Patyn, A., & Dierickx, K. (2010). Forensic DNA databases: Genetic testing as a societal choice. *Journal of Medical Ethics*, 36(5), 319–320. <https://doi.org/10.1136/jme.2009.033829>
- Perras, C. (2017). Transnational policing and its contexts: flexibility and (dis)trust. In S. Hufnagel & C. McCartney (Eds.), *Trust in International Police and Justice Cooperation* (pp. 221–240). Oxford and Portland, Oregon: Bloomsbury.
- Pfotenhauer, S., & Jasanoff, S. (2017). Panacea or diagnosis? Imaginaries of innovation and the 'MIT model' in three political cultures. *Social Studies of Science*, 47(6), 783–810. <https://doi.org/10.1177/0306312717706110>
- Pickersgill, M. (2011). Connecting neuroscience and law: Anticipatory discourse and the role of sociotechnical imaginaries. *New Genetics and Society*, 30(1), 27–40. <https://doi.org/10.1080/14636778.2011.552298>
- Police Staff Council. (2018). Joint Circular 96: Contamination elimination database (CED) -

- DNA profiling. Retrieved from [https://www.local.gov.uk/sites/default/files/documents/PSC Joint Circular 96 FINAL.pdf](https://www.local.gov.uk/sites/default/files/documents/PSC_Joint_Circular_96_FINAL.pdf)
- Porter, T. (1992). Objectivity as standardization: the rhetoric of impersonality in measurement, statistics, and cost-benefit analysis. *Annals of Scholarship (Special Issue on Objectivity)*, 9, 19–59.
- Porter, T. (1995). *Trust in numbers: The pursuit of objectivity in science and public life*. Princeton, NJ: Princeton University Press.
- Post, R. (2001). Three concepts of privacy. *The Georgetown Law Journal*, 89(6), 2087–2098.
- Poster, M. (1990). *The mode of information: Poststructuralism and social context*. Cambridge: Polity Press.
- Powell, W., & DiMaggio, P. (Eds.). (1991). *The new institutionalism in organizational analysis*. Chicago, USA: The University of Chicago Press.
- Power, M. (1997). *The Audit Society*. Oxford: Oxford University Press.
- Prainsack, B. (2010). Key issues in DNA profiling and databasing: Implications for governance. In R. Hindmarsh & B. Prainsack (Eds.), *Genetic suspects: Global governance of forensic DNA profiling and databasing* (pp. 153–174). Cambridge: Cambridge University Press.
- Prainsack, B., & Aronson, J. (2015). Forensic genetic databases: Ethical and social dimensions. *International Encyclopedia of the Social & Behavioral Sciences*, 9, 339–345. <https://doi.org/10.1016/B978-0-08-097086-8.82062-0>
- Prainsack, B., & Buyx, A. (2016). Thinking ethical and regulatory frameworks in medicine from the perspective of solidarity on both sides of the Atlantic. *Theoretical Medicine and Bioethics*, 00(00), 1–13. <https://doi.org/10.1007/s11017-016-9390-8>
- Prainsack, B., & Toom, V. (2010). The Prüm regime. Situated dis/empowerment in transnational DNA profile exchange. *British Journal of Criminology*, 50(6), 1117–1135. <https://doi.org/10.1093/bjc/azq055>
- Prainsack, B., & Toom, V. (2013). Performing the Union: The Prüm decision and the European dream. *Studies in History and Philosophy of Biological and Biomedical Sciences*, 44(1), 71–79. <https://doi.org/10.1016/j.shpsc.2012.09.009>
- Pratt, T., Gaffney, M., Lovrich, N., & Johnson, C. (2006). This isn't CSI: Estimating the national backlog of forensic DNA cases and the barriers associated with case processing. *Criminal Justice Policy Review*, 17(1), 32–47. <https://doi.org/10.1177/0887403405278815>
- Protection of Freedoms Act. (2012). London: The Stationery Office. Retrieved from http://www.legislation.gov.uk/ukpga/2012/9/pdfs/ukpga_20120009_en.pdf
- Pugliese, J. (2012). *Bodies, technologies, biopolitics*. New York and London: Routledge.
- Quack, S. (2010). Law, expertise and legitimacy in transnational economic governance: An introduction. *Socio-Economic Review*, 8, 3–16.
- Raab, C. (2008). Vigilância e Privacidade: as opções de regulação. In C. Frois (Ed.), *A sociedade vigilante: Ensaios sobre privacidade, identificação e vigilância* (pp. 79–110). Lisboa: Imprensa de Ciências Sociais.
- Raab, C. (2015). Effects of surveillance on civil liberties and fundamental rights in Europe – surveillance: effects on privacy, autonomy and dignity. In David Wright & R. Kreissl (Eds.), *Surveillance in Europe*. London: Routledge.
- Reed, K., & Syndercombe-Court, D. (2016). *A comparative audit of legislative frameworks within the European Union for the collection, retention and use of forensic DNA profiles*.

- London. Retrieved from https://www.eurofor.gen.eu/fileadmin/websites/eurofor.gen/images/Dissemination_Documents/WP4/Reed_and_Syndercombe_Court_2016_Legal_Audit.pdf
- Regan, P. (1995). *Legislating privacy*. Chapel Hill: University of North Carolina Press.
- Reiman, J. (1976). Privacy, Intimacy and Personhood. *Philosophy and Public Affairs*, 6(1), 26–44.
- Roberts, P. (1996). What Price a Free Market in Forensic Science Services? The Organization and Regulation of Science in the Criminal Process. *British Journal of Criminology*, 36, 37–60.
- Rose, N. (2008). Race, risk and medicine in the age of ‘your own personal genome.’ *BioSocieties*, 3(4), 423–439. <https://doi.org/10.1017/S1745855208006339>
- Rose, N., & Miller, P. (1992). Political power beyond the State: Problematics of government. *The British Journal of Sociology*, 43(2), 173. <https://doi.org/10.2307/591464>
- Rose, N., & Novas, C. (2005). Biological citizenship. In S. J. Collier & A. Ong (Eds.), *Global assemblages: Technology, politics, and ethics as anthropological problems* (pp. 439–463). Malden, MA: Blackwell Publishers.
- Rosenau, J. (2003). *Distant proximities. Dynamics beyond globalization*. Princeton: Princeton University Press.
- Røvik, K. (2002). The Secrets of the Winners: Management Ideas that Flow. In K. Sahlin-Anderson & L. Engwall (Eds.), *The expansion of management knowledge*. Stanford University Press.
- Sahlin-Andersson, K. (2004). Emergent Cross-Sectional Soft Regulations: Dynamics at Play in the Global Compact Initiative. In U. Mörtz (Ed.), *Soft Law in Governance and Regulation An Interdisciplinary Analysis* (pp. 129 – 154). Cheltenham: Edward Elgar Publishing.
- Said, E. (1978). Imaginative geography and its representations: orientalizing the oriental. In *Orientalism* (pp. 49–73). London: Routledge & Kegan Paul.
- Sallavaci, O. (2017). Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange. *European Journal on Criminal Policy and Research*, 1–17. <https://doi.org/10.1007/s10610-017-9355-0>
- Santos, B., Marques, M., Pedroso, J., & Ferreira, P. (1996). Os tribunais nas sociedades contemporâneas: O caso português. Porto: Afrontamento.
- Santos, F. (2017). The transnational exchange of DNA data: Global standards and local practices. In K. Jakobs & K. Blind (Eds.), *Proceedings of the 22nd EURAS annual standardisation conference. Digitalisation: Challenge and opportunity for standardisation* (pp. 305–322). Aachen: Verlag Mainz.
- Santos, F., Costa, S., & Machado, H. (2012). A base de dados de perfis de DNA em Portugal: Questões sobre a sua operacionalização. In S. Costa & H. Machado (Eds.), *A ciência na luta contra o crime: Potencialidades e limites* (pp. 99–118). Vila Nova de Famalicão: Húmus.
- Santos, F., & Machado, H. (2017). Patterns of exchange of forensic DNA data in the European Union through the Prüm system. *Science & Justice*, 57(4), 307–313. <https://doi.org/10.1016/j.scijus.2017.04.001>
- Santos, F., Machado, H., & Silva, S. (2013). Forensic DNA databases in European countries: Is size linked to performance? *Life Sciences, Society and Policy*, 9(12), 1–13. <https://doi.org/10.1186/2195-7819-9-12>
- Sarewitz, D. (1996). *Frontiers of illusion: Science, technology, and the politics of progress*. Philadelphia: Temple University Press.

- Schaar, P. (2010). Privacy by design. *Identity in the Information Society - Special Issue*, 3(2), 267–274. <https://doi.org/10.1007/s12394-010-0055-x>
- Schmidt, P. (2004). Law in the Age of Governance: Regulation, Networks and Lawyers. In J. Jordana & D. Levi-Faur (Eds.), *The Politics of Regulation* (pp. 273–295). Cheltenham, UK: Edward Elgar.
- Schmidt, S., & Werle, R. (1998). *Coordinating technology – studies in the international standardization of telecommunications*. Cambridge, MA, USA: The MIT Press.
- Schoeman, F. (1992). *Privacy and social freedom*. Cambridge: Cambridge University Press.
- Schroeder, D., & White, M. (2009). Exploring the use of DNA evidence in homicide investigations: Implications for detective work and case clearance. *Police Quarterly*, 12(3), 319–342. <https://doi.org/10.1177/1098611109339894>
- Scholte, J. (2005). Civil society and democratically accountable global governance. In D. Held & M. Koenig-Archibugi (Eds.), *Global governance and public accountability* (pp. 87–109). Oxford: Blackwell Publishing.
- Schwartz-Marín, E., & Wade, P. (2015). Explaining the visible and the invisible: Public knowledge of genetics, ancestry, physical appearance and race in Colombia. *Social Studies of Science*, 45(6), 886–906. <https://doi.org/10.1177/0306312715621182>
- Scott, C. (2004). Regulation in the Age of Governance: The Rise of the Post-Regulatory State. In J. Jordana & D. Levi-Faur (Eds.), *The Politics of Regulation* (pp. 145–174). Cheltenham, UK: Edward Elgar.
- Shapin, S. (2001). Truth and credibility: Science and the social study of science. In N. Smelser & P. Baltes (Eds.), *International encyclopedia of social and behavioral sciences* (p. 15926). Oxford, UK: Cambridge University Press.
- Shapin, S., & Shaffer, S. (1985). *Leviathan and the Air-Pump*. Princeton, NJ: Princeton University Press.
- Simoncelli, T. (2006). Dangerous excursions: The case against expanding forensic DNA databases to innocent persons. *Journal of Law, Medicine & Ethics*, 34(2), 390–397. Retrieved from <http://www3.interscience.wiley.com/journal/118589899/abstract>
- Skinner, D. (2013). “The NDNAD has no ability in itself to be discriminatory”: Ethnicity and the governance of the UK National DNA Database. *Sociology*, 47(5), 976–992. <https://doi.org/10.1177/0038038513493539>
- Skinner, D. (2018). Race, Racism and Identification in the Era of Technosecurity. *Science as Culture*, 1–23. <https://doi.org/10.1080/09505431.2018.1523887>
- Smith, J. (2005). Globalization and transnational social movement organizations. In G. F. Davis, D. McAdam, R. W. Scott, & N. Z. Mayer (Eds.), *Social movements and organization theory* (pp. 226–248). Cambridge University Press.
- Smith, J. (2008). *Social Movements for Global Democracy*. Baltimore: John Hopkins University Press.
- Smith, M. (2006). Let’s make the DNA identification database as inclusive as possible. *Journal of Law, Medicine & Ethics*, 34(2), 385–389. <https://doi.org/10.1111/j.1748-720X.2006.00044.x>
- Soleto, H. (2014). DNA data in criminal procedure in the European fundamental rights context. *Recent Advances in DNA and Gene Sequences*, 8(2), 91–97. Retrieved from <http://www.embase.com/search/results?subaction=viewrecord&from=export&id=L605229547>
- Solove, D. (2004). *The Digital person: Technology and privacy in the information age*. New York: New York University Press.

- Solove, D. (2006). A Taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564.
- Solove, D., & Rotenberg, M. (2003). *Information Privacy Law*. New York: Aspen publishers.
- Spapens, T. (2017). Building trust and more: the importance of police cooperation networks in the European Union. In S. Hufnagel & C. McCartney (Eds.), *Trust in International Police and Justice Cooperation* (pp. 149–168). Oxford and Portland, Oregon: Bloomsbury.
- Star, S. (1985). Scientific work and uncertainty. *Social Studies of Science*, 15(3), 391–427. <https://doi.org/10.1177/030631285015003001>
- Strange, S. (1996). *The Retreat of the State*. Cambridge: Cambridge University Press.
- Strauss, A. , & Corbin, J. (1990). *Basics of qualitative research. Grounded theory procedures and techniques*. Newbury Park, CA: Sage Publications.
- Streeck, W., & Schmitter, P. (1985). Community, market, state – and associations? The prospective contribution of interest governance to social order. In W. Streeck & P. Schmitter (Eds.), *Private interest government. Beyond market and state* (pp. 1–29). London: Sage.
- Sulca, D. (2017). Intelligence-led use of international forensic exchange channels. In S. Hufnagel & C. McCartney (Eds.), *Trust in International Police and Justice Cooperation* (pp. 241–254). Oxford and Portland, Oregon: Bloomsbury.
- Taylor, C. (2004). *Modern social imaginaries*. Durham: Duke University Press.
- Tenner, E. (1996). *Why things bite back: Technology and the revenge of unintended consequences*. New York: Vintage Books.
- Thévenot, L. (2009). Governing life by standards: a view from engagements. *Social Studies of Science*, 39, 793–813.
- Thompson, W., & Ford, S. (1991). The Meaning of a Match: Sources of Ambiguity in the Interpretation of DNA Prints. In M. Farley & J. Harrington (Eds.), *Forensic DNA Technology* (pp. 93–152). Chelsea, MI: Lewis Publishers.
- Thorogood, A., & Zawati, M. (2015). International guidelines for privacy in genomic biobanking (or the unexpected virtue of pluralism). *Journal of Law, Medicine & Ethics*, 43(4), 690–702. <https://doi.org/10.1111/jlme.12312>
- Timmermans, S., & Berg, M. (1997). Standardization in action: Achieving local universality through medical protocols. *Social Studies of Science*, 27(2), 273–305. <https://doi.org/10.1177/030631297027002003>
- Timmermans, S., & Epstein, S. (2010). A World of Standards but Not a Standard World: Toward a Sociology of Standards and Standardization. *Annual Review of Sociology*, 36, 69–89.
- Tolbert, P., & Zucker, L. (1983). Institutional sources of change in the formal structure of organizations: the diffusion of civil service reform, 1880-1935. *Administrative Science Quarterly*, 28, 22–39.
- Toom, V. (2012). Bodies of science and law: Forensic DNA profiling, biological bodies, and biopower. *Journal of Law and Society*, 39(1), 150–166. <https://doi.org/10.1111/jols.2012.39.issue-1/issuetoc>
- Toom, V. (2018). *Cross-border exchange and comparison of forensic DNA data in the context of the Prüm Decision. Civil liberties, justice and home affairs*. Retrieved from [http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU\(2018\)604971](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604971)
- Toom, V., Granja, R., & Ludwig, A. (2019). The Prüm Decisions as an aspirational regime:

- Reviewing a decade of cross-border exchange and comparison of forensic DNA data. *Forensic Science International: Genetics*, 41, 50–57. <https://doi.org/10.1016/j.fsigen.2019.03.023>
- Toom, V., Wienroth, M., M'charek, A., Prainsack, B., Williams, R., Duster, T., ... Murphy, E. (2016). Approaching ethical, legal and social issues of emerging forensic DNA phenotyping (FDP) technologies comprehensively: Reply to 'Forensic DNA phenotyping: Predicting human appearance from crime scene material for investigative purposes' by Manfred Kayser. *Forensic Science International: Genetics*, 22, e1–e4. <https://doi.org/10.1016/j.fsigen.2016.01.010>
- Tsekeris, C. (2007). Performativity. In G. Ritzer (Ed.), *Blackwell Encyclopedia of Sociology*. Blackwell Publishing.
- Tseloni, A., & Pease, K. (2010). DNA retention after arrest: Balancing privacy interests and public protection. *European Journal of Criminology*, 8(1), 32–47. <https://doi.org/10.1177/1477370810372133>
- Tutton, R., & Levitt, M. (2010). Health and wealth, law and order: banking DNA against disease and crime. In R. Hindmarsh & B. Prainsack (Eds.), *Genetic suspects: Global governance of DNA profiling and databasing* (pp. 85–104). Cambridge: Cambridge University Press.
- Union, C. of the E. (2008) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 2008 § (2008). Official Journal of the European Union. Retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF>
- Union, C. of the E. (2015). Implementation of the provisions on information exchange of the “Prüm Decisions” - 5010/3/15. Brussels, 23 April. Retrieved from <http://data.consilium.europa.eu/doc/document/ST-5010-2015-REV-3/en/pdf>
- Union, C. of the E. (2017). Implementation of the provisions on information exchange of the “Prüm Decisions” - 5081/1/17. Brussels, 31 January. Retrieved from <http://data.consilium.europa.eu/doc/document/ST-5081-2017-INIT/en/pdf>
- Van Camp, N., & Dierickx, K. (2007). National forensic databases: Social-ethical challenges & current practices in the EU. Leuven: European Ethical-Legal Papers n°9. Retrieved from http://www.academia.edu/attachments/6227872/download_file
- Van Camp, N., & Dierickx, K. (2008). The retention of forensic DNA samples: A socio-ethical evaluation of current practices in the EU. *Journal of Medical Ethics*, 34(8), 606–610. <https://doi.org/10.1136/jme.2007.022012>
- Van der Beek, K. (2011). Forensic DNA profiles crossing borders in Europe (Implementation of the Treaty of Prüm). The Hague: Netherlands Forensic Institute. Retrieved from <https://worldwide.promega.com/resources/profiles-in-dna/2011/forensic-dna-profiles-crossing-borders-in-europe/>
- Waddell, S., & Khagram, S. (2007). Multi-stakeholder global networks: Emerging systems for the global common good. In P. Glasbergen, F. Biermann, & A. Mol (Eds.), *Partnerships, Governance and Sustainable Development* (pp. 261–287). Cheltenham: Edward Elgar.
- Wallace, H., Jackson, A., Gruber, J., & Thibedeau, A. (2014). Forensic DNA databases: Ethical and legal standards - A global review. *Egyptian Journal of Forensic Sciences*, 4(3), 57–63. <https://doi.org/10.1016/j.ejfs.2014.04.002>
- Wayman, J. (2000). When bad science leads to good law: The disturbing irony of the Daubert hearing in the case of U.S V. Byron C. Mitchell. U.S. National Biometric Test

- Center. Retrieved from
http://www.engr.sjsu.edu/biometrics/publications_daubert.html
- Wayman, J., & Nuger, K. (2005). Biometrics and the US Constitution. In J. Wayman, A. Jain, D. Maltoni, & D. Maio (Eds.), *Biometric Systems* (pp. 311–333). London: Springer. https://doi.org/10.1007/1-84628-064-8_11
- Weber, M. (1919/1977). *Vetenskap och politik*. Gothenburg, Sweden: Korpen
- Weber, M. (1947). *The theory of social and economic organization*. (T. Parsons, Ed.). New York: Oxford University Press.
- Weber, M. (1968). *Economy and society: An outline of interpretive sociology*. Berkeley, CA: University of California Press.
- Werle, R., & Iversen, E. (2006). Promoting legitimacy in technical standardization. *Science, Technology & Innovation Studies*, 2, 19–39.
- Westin, A. (1967). *Privacy And Freedom*. New York: Washington and Lee Law Review.
- Williams, R. (1983). *Keywords: A vocabulary of culture and society*. New York: New York: Oxford University Press. <https://doi.org/10.1057/9780230373464>
- Williams, R. (2010). DNA databases and the forensic imaginary. In R. Hindmarsh & B. Prainsack (Eds.), *Genetic suspects: Global governance of DNA profiling and databasing* (pp. 131–152). Cambridge: Cambridge University Press.
- Williams, R., & Johnson, P. (2004a). Circuits of surveillance. *Surveillance & Society*, 2(1), 1–14. <https://doi.org/10.1901/jaba.2004.2-1>
- Williams, R., & Johnson, P. (2004b). “Wonderment and dread”: Representations of DNA in ethical disputes about forensic DNA databases. *New Genetics and Society*, 23(2), 205–223. <https://doi.org/10.1080/1463677042000237035>
- Williams, R., & Johnson, P. (2005). *Forensic DNA databasing: A european perspective*. Durham. Retrieved from
<http://www.dur.ac.uk/resources/sass/WilliamsandJohnsonInterimReport2005-1.pdf>
- Williams, R., & Johnson, P. (2008). *Genetic policing: The use of DNA in criminal investigations*. Cullompton: Willan Publishing.
- Williams, R., Johnson, P., & Martin, P. (2004). *Genetic information and crime investigation: Social, ethical and public policy aspects of the establishment, expansion and police use of the National DNA Database* (Vol. 44). Durham.
- Williams, R., & Wienroth, M. (2014). *Ethical, social and policy aspects of forensic genetics: A systematic review*. Newcastle upon Tyne, UK.
- Wilson, T. (2016). Criminal justice and global public goods: The Prüm forensic biometric cooperation model. *The Journal of Criminal Law*, 80(5), 303–326. <https://doi.org/10.1177/0022018316668450>
- Wilson-Kovacs, D., Wyatt, D., & Hauskeller, C. (2012). “A Faustian bargain?” Public voices on forensic DNA technologies and the National DNA Database. *New Genetics and Society*, 31(3), 285–298. Retrieved from
<http://www.tandfonline.com/doi/abs/10.1080/14636778.2012.687085>
- Winner, L. (1986). Do artifacts have politics? In *The whale and the reactor: a search for limits in the age of high technology* (pp. 19–39). Chicago: University of Chicago Press.
- Woodward, J. (1997). *Biometrics: Identifying law & policy concerns*. Retrieved from
<http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf>
- Woodward Jr., J., Orlans, N., & Higgins, P. (2003). *Biometrics: Identity assurance in the information age*. Berkeley, CA: McGraw-Hill/Osborne Media.
- Wright, D., & Kreissl, R. (2015). European responses to the Snowden revelations. In David

- Wright & R. Kreissl (Eds.), *Surveillance in Europe* (pp. 6–50). London: Routledge.
- Wynne, B. (1987). *Risk management and hazardous waste: Implementation and the dialectics of credibility*. Berlin: Springer-Verlag.
- Yin, R. (1994). *Case study research: Design and methods*. London: Sage Publications.
- Yin, R. (2011). *Qualitative Research from Start to Finish* (First Edit). Guildford Press.
- Young, J. (1994). Outlining regulatory space; Agenda issues and the FASB. *Accounting, Organizations and Society*, 19(1), 83–109.
- Zaiotti, R. (2007). Revisiting Schengen: Europe and the emergence of a new culture of border control. *Perspectives on European Politics and Society*, 8(1), 31–54.
<https://doi.org/10.1080/15705850701204087>

ANEXOS

Anexo 1 – Guião de entrevista - Pontos de Contacto Nacionais (NCP)

NCP Script

Prüm Implementation

1. Could you please tell us about your professional background? How did you become a National Contact Point for Prüm DNA?
2. Could you please describe what are the main functions and responsibilities of a National Contact Point? [In countries where there are two contacts or institutions for NCP ask about tasks' division]
3. Could you please tell us about the functioning and characteristics of your country's national DNA database? [Specify issues like governing legislation and criteria for inclusion and exclusion, custody, rules of access, storage policy of biological samples, workflow with the criminal justice system, and approximate number of profiles]
4. Regarding the personal data collected that is associated with profiles, what kind of categories does your country include? [i.e. demographic data, ethnic appearance or ethnic group, gender, type of crime]
5. In your opinion, what is the main goal of Prüm? Why do you think it was important for your country to join Prüm? [Specify issues like: How do you see the role of Prüm in terms of the integration (harmonisation) of the European Union?]
6. What were the national arrangements regarding DNA data exchange with other countries before Prüm? With which countries did you exchange information more frequently? And now that you are in Prüm? [Specify issues like which countries; There were or are there still bi-lateral agreements with third party countries; how did the implementation of Prüm altered the relations with other countries]
7. What can you tell us about the process of implementation of Prüm in your country? [Cover issues such as historical process of implementation; obstacles and easy tasks; initial “test partners” and reasons for choice; staff training; changes of previous national practices; current situation; new possibilities in the criminal inquiry brought by Prüm]
8. What is your perspective on the implementation of Prüm in other European countries? [Specify and explain issues like mandatory nature, transparency, democracy, consensus, disparate legal regimes, database size, criteria for inclusion and exclusion, custody and access issues]

Prüm Challenges

9. What is your opinion regarding the risks and benefits of Prüm? [Focus on technical, scientific, financial and legal issues, according to interviewee profile; Specify topics related to the presumed “infallibility” of DNA and its value in relation to other forensic instruments for the purpose of combating crime]
10. What is your experience so far regarding the operation of Prüm's so-called Step 1? [Specify the description of the process of assessing matches; How do you deal with near matches?; What safeguards do you employ to ensure that the level of adventitious hits is

kept within acceptable and manageable levels, safeguards to maintain data quality and data security, safeguards to transparency and accountability of the governance of data exchange? NCP2: Do you handle specific requests from the authorities?]

11. Could you please describe what kind of procedures follow a positive match? [How do you know that the information is reliable? Do you ever receive requests regarding unconfirmed matches? Do you have feedback from the cases? Specify issues related to mutual assistance on sharing personal data, reasons for choice of channel, data protection measures, type of information that is shared, what crimes justify follow-up]

12. What do you expect from Prüm with regards to its contribution to criminal investigation? What is your expectation about the kind of crimes that may be solved with the help of Prüm DNA exchange?

13. Prüm aims to fight crime, terrorism and illegal immigration: Could you explain how you see that it links to all three types of threats? What are the potential challenges brought by the role of DNA technologies and DNA data exchange in addressing these goals?

14. How do you see DNA technologies and DNA forensic databases in comparison to other identification technologies and data exchange systems in Europe?

15. What is your opinion on the privatization of forensic services? And how do you see the role of the biotech industry in the design and provision of forensic equipment?

16. Can you tell us about any criminal cases in your country that were solved because of intelligence provided by Prüm? [Specify where can we get more information about that case and with whom should we speak]

Prüm Ethical Issues and General Public

17. What sort of measures are implemented in your country to protect the data of the individuals included in the DNA database? Did Prüm bring about any changes in data protection policies?

18. What kind of quality and ethical supervision is exercised over the activities of the national DNA database and Prüm operations? [Could you describe the activities of the supervisory board?]

19. What are, in your opinion, the main challenges to civil liberties brought by Prüm? [According to interviewee profile specify issues like human rights, informed consent, forensic research, other uses of DNA databases]

20. There have been developments on DNA technology that allow going beyond individual matching in databases, like familial searching. What sort of ethical challenges do you think are raised by familial searching? [Do you know if familial searching was ever used in any criminal case in your country? Thinking about concrete cases, what is your opinion on the potential and eventual challenges of this technique?]

21. More recent developments in DNA technology relate to the use of Ancestry Informative Markers and the prediction of Externally Visible Characteristics through DNA. What are your views on the potential benefits and risks of these technologies? [Specify issues like: Were

these technologies were ever used in your country? What is your opinion on the creation of DNA photofits of suspects?

22. And how do you see the role of Massive Parallel Sequencing (MPS) or Next Generation Sequencing (NGS) in forensic DNA profiling? What possible impacts do you think this technology can have in the future?

23. In your opinion, what are the relevant challenges of the uses of technologies such as “rapid DNA profiling”? And what about Y_STR profiling? (short tandem repeat” on the Y-chromosome)?

24. Has your country ever conducted a DNA mass screen (or DNA dragnet)? What would you say are the main challenges in performing a mass screen? [Defining geographical area? Defining the type of individuals to be sampled? Capacity for processing the samples?]

25. Besides forensic DNA databases, there are genetic databases for medical research and other biometric databases. What is your perspective on the interoperability of these databases for criminal investigation purposes? [for example, databases for medical research and medical purposes; integration of forensic DNA databases with police and criminal justice databases; and vice-versa]

26. What is your opinion about potential uses of big data? [for example, probabilities of vast amounts of biometric information being analysed and associated with patterns of behaviour or mapping of propensity for diseases]

27. What kind of involvement do you have with civil society stakeholders specifically interested in issues about Prüm? [Specify issues and what kind of concerns]

28. How are citizens, or generally the public, affected by Prüm? To what extent do you think the general public in your country is informed about what Prüm is and does? [If the questions don’t “work”: how you perceive the relations between the general public and the national DNA database]

29. As a NCP of Prüm are you involved in any kind of actions to share information with the general public concerning the operation of the database and information sharing within Prüm? [Cover issues such as transparency, accountability and public trust]

30. How do you see the near future of Prüm?

31. Would you like to add something further or ask us any questions?

Anexo 2 – Guião de entrevista – Geneticistas forenses

Forensic geneticist Script

- 1.** Could you please tell us about your professional background? How did you become a forensic expert? [question adapted to professional profile]
- 2.** Could you please describe what are your main functions and responsibilities?
- 3.** Could you please explain the main activities of this institute regarding forensic genetics? Does the institute provide services for private clients?
- 4.** How would you describe the most common and uncommon type of work that the forensic genetics department does?
- 5.** Could you please explain how the provision of forensic genetics services are organized in your country? [Are there other forensic institutes/laboratories? Understand distribution among other institutes/laboratories. How is this institute's workflow with the criminal justice system?]
- 6.** Regarding the personal data collected that is associated with profiles, what kind of categories does your country include? [i.e. demographic data, ethnic appearance or ethnic group, gender, type of crime]
- 7.** How do you see the role of DNA technologies in fighting crime? [specify topics related to the presumed “infallibility” of DNA and its value in relation to other forensic instruments for the purpose of combating crime]
- 8.** How do you see the communication between forensic geneticists and police officers and/or other members of the criminal justice? What are the main challenges?
- 9.** How do you see DNA technologies and DNA forensic databases in comparison to other identification technologies and data exchange systems in Europe?
- 10.** What are, in your opinion, the privacy issues/ethical challenges emerging from DNA analysis in criminal cases?
- 11.** What is your opinion regarding the Prüm Decisions of European Union, that is, the sharing of DNA and other data in order to fight crime, terrorism and illegal immigration? [Could you explain how you see that DNA links to all three types of threats? What are the potential challenges brought by the role of DNA technologies and DNA data exchange in addressing these goals?]
- 12.** Can you tell us about a criminal case in your country that could was solved with intelligence provided by DNA technologies? [Where can we get more information about that case and with whom should we speak]
- 13.** In your opinion, how did the exchange of DNA data among European countries to fight crime affect the development of forensic genetics in Europe?
- 14.** What is your opinion on the privatization of forensic services? And how do you see the role of the biotech industry in the design and provision of forensic DNA equipment?
- 15.** What is your opinion on the private companies that are increasingly offering services related to DNA analysis? Such as Parabon Nanolabs (FDP), Identitas (FDP), 23 and Me (ancestry), Illumina (NGS) and ThermoFisher (FDP and ancestry). [explore issues related to

the boundaries of academic research - peer-review – and private companies; open sources versus proprietary rights; impacts of the promises about the capacities of the services in public perception of DNA technologies]

16. There have been developments on DNA technology that allow going beyond individual matching in databases, like familial searching. What sort of ethical challenges do you think are raised by familial searching? [Do you know if familial searching was ever used in any criminal case in your country? Thinking about concrete cases, what is your opinion on the potential and eventual challenges of this technique?]

17. More recent developments in DNA technology relate to the use of Ancestry Informative Markers and the prediction of Externally Visible Characteristics through DNA. What are your views on the potential benefits and risks of these technologies? [Specify issues like: Were these technologies ever used in your country? What is your opinion on the creation of DNA photofits of suspects?]

18. And how do you see the role of Massive Parallel Sequencing (MPS) or Next Generation Sequencing (NGS) in forensic DNA profiling? What possible impacts do you think this technology can have in the future?

19. In your opinion, what are the relevant challenges of the uses of technologies such as “rapid DNA profiling”? And what about Y-STR profiling? (short tandem repeat” on the Y-chromosome)?

20. Has your country ever conducted a DNA mass screen (or DNA dragnet)? What would you say are the main challenges in performing a mass screen? [Defining geographical area? Defining the type of individuals to be sampled? Capacity for processing the samples?]

21. Besides forensic DNA databases, there are genetic databases for medical research and other biometric databases. What is your perspective on the interoperability of these databases for criminal investigation purposes? [for example, databases for medical research and medical purposes; integration of forensic DNA databases with police and criminal justice databases; and vice-versa]

22. From your point of view, what are the probabilities and potential risks of the use of the available and future biometric information as big data? [For example, do you think the vast amounts of biometric information can be analysed and associated with patterns of behaviour or mapping of propensity for diseases?]

23. To what extent do you think the general public in your country is informed about forensic genetics? [Specify issues and what kind of concerns and involvement is made with civil society and stakeholders]

24. How do you see the near future of forensic DNA technologies in Europe?

25. Would you like to add something further or ask us any questions?

Anexo 3 – Guião de entrevista – Stakeholders

Stakeholders Script

Personal background and institution

1. Could you please tell us about your professional background? How did you become a forensic expert? [question adapted to professional profile]
2. Could you please describe what are your main functions and responsibilities?
3. How does your role relate to: forensic DNA data and the protection of personal data in this context; the use of technology to fight crime? [question adapted to professional profile]

National DNA forensic database, Prüm decisions and the transnational exchange of DNA data in the EU

4. In general terms, what do you think that is the role of the [country's] national DNA forensic database? [explore issues related to the specific development situation of each country: balance and assessment of the database since its creation]
5. What is your opinion regarding the costs and benefits of Prüm?
6. What do you expect from Prüm with regards to its contribution to criminal investigation?
7. What is your expectation about the kind of crimes that may be solved with the help of Prüm DNA exchange?
8. Which safeguards do you think should be added to address – for Prüm – concerns about risks of international data exchange? How do you evaluate them?
9. [Explore the country] situation of data protection with regards to DNA data exchange in the EU.
10. In your opinion, what does Prüm add to the existing biometric and identification data exchange in Europe?
11. Prüm aims to fight crime, terrorism and illegal immigration: Could you explain how you see that it links to all three types of threats? What are the potential challenges brought by the role of DNA technologies and DNA data exchange in addressing these goals?
12. How do you see DNA technologies and DNA forensic databases in comparison to other identification technologies and data exchange systems in Europe?
13. In your opinion what are the main challenges to civil liberties brought by Prüm? How are citizens or the general public affected by the implementation of Prüm?
14. How would you describe the public debate and public consultation accompanying the process of implementing the Prüm Decisions?
15. What are your perceptions about the media coverage of the uses of forensic DNA data in general and the Prüm process in particular?
16. Do you think that some countries in Europe are more concerned than others in relation to maintain data protection standards and to protect human rights in the context of forensic DNA databases and other biometrics materials? Could you please give some examples?

Particular aspects related to the national DNA database and to the use of new technologies
[questions adapted to the specificities of each country]

- 17.** In your opinion what are the main challenges related to the governance of police databases holding DNA information?
- 18.** What do you think could be any specific ethical challenges related to the national DNA database?
- 19.** What main issues do you see in regard to the process of taking consent and providing better consent?
- 20.** What main issues do you foresee in regards to rights of children, young people and other vulnerable people?
- 21.** More recent developments in DNA technology relate to the use of Ancestry Informative Markers and the prediction of Externally Visible Characteristics through DNA. What are your views on the potential benefits and risks of these technologies? Specify issues like: Were these technologies ever used in your country? What is your opinion on the creation of DNA photofits of suspects?
- 22.** [if not covered in the previous question] In your opinion, what type of crimes could justify the use of DNA analysis to infer ancestry and externally visible physical characteristics of criminal suspects?
- 23.** There have been also developments on DNA technology that allow going beyond individual matching in databases, like familial searching. What sort of ethical challenges do you think are raised by familial searching? [Do you know if familial searching was ever used in any criminal case in your country? Thinking about concrete cases, what is your opinion on the potential and eventual challenges of this technique]?
- 24.** In your opinion, what are the relevant challenges of the uses of technologies such as “rapid DNA profiling”? And what about Y_STR profiling? (short tandem repeat” on the Y-chromosome)?
- 25.** Besides forensic DNA databases, there are genetic databases for medical research and other biometric databases. What is your perspective on the interoperability of these databases for criminal investigation purposes? [for example, databases for medical research and medical purposes; integration of forensic DNA databases with police and criminal justice databases; and vice-versa]
- 26.** From your point of view, what are the probabilities and potential risks of the use of the available and future biometric information as big data? [For example, do you think the vast amounts of biometric information can be analysed and associated with patterns of behaviour or mapping of propensity for diseases?]
- 27.** To what extent do you think the general public in your country is informed about forensic genetics? [Specify issues and what kind of concerns and involvement is made with civil society and stakeholders]
- 28.** What is your opinion on the privatization of forensic services? And how do you see the role of the biotech industry in the design and provision of forensic equipment?

- 29.** How do you see the near future of forensic DNA technologies in Europe?
- 30.** Would you like to add something further or ask us any questions?

Anexo 4 – Consentimento informado

Consent form

The material gathered during this research will be treated as confidential and securely stored. Please answer each statement concerning the collection and use of the research data (please tick the applicable box):

- | | | |
|---|------------------------------|-----------------------------|
| I have read and understood the information sheet | YES ☐ | NO ☐ |
| I have been given the opportunity to ask questions about the study | YES ☐ | NO ☐ |
| I have had my questions answered satisfactorily | YES ☐ | NO ☐ |
| I agree to the interview being recorded and to its contents being exclusively used for research purposes | YES ☐ | NO ☐ |
| I understand that my identity will be protected when the research is published, and that the interview will be anonymised | YES ☐ | NO ☐ |

Name: _____

(Please print)

Signature: _____

Date: _____

For more information, please contact:

Dr. Helena Machado (Principal Investigator)

Institute of Social Sciences – University of Minho

4710-057 Campus de Gualtar, Braga, Portugal

Tel.: +351253604212 | +351253604280 | Fax: +351253604697

E-mail: hmachado@ics.uminho.pt

Website: exchange.ics.uminho.pt

Anexo 5 – Folheto informativo

Information Sheet

We would like to invite you to participate into the EXCHANGE project (exchange.ics.uminho.pt), which aims to develop a sociological study on the current state of forensic genetics in the European Union (EU).

What are we studying?

Today we are living in the “genetic age” of criminal investigation. There is a widespread cultural belief that DNA technology has the unrivalled capacity to identify authors of crimes. EU Law (Prüm Decision, 2008) obliges all Member States to create the conditions for the reciprocal automated searching and comparison of information on DNA data for the purpose of combating cross-border crime, terrorism and illegal immigration.

This research project aims to study the current state of forensic genetics in the European Union (EU) by developing an in-depth knowledge of the Research and Innovation being developed within forensic genetics, the use of DNA technologies in criminal justice systems and the role of private companies in the provision of forensic equipment and services.

EXCHANGE stimulates interdisciplinary dialogue between the social sciences and the forensic genetics.

Who are we studying?

We want to talk to people working in forensic laboratories and to other relevant stakeholders involved in the operation of the transnational exchange of DNA data in Germany, The Netherlands, Poland, Portugal and the UK, like:

- Forensic geneticists and laboratory staff
- Members of ethical boards of forensic DNA databases
- Representatives of judicial authorities
- Representatives of the ministries of Justice
- Representatives of national data protection authorities
- Representatives of civil society stakeholders accompanying forensic DNA databases

What does your participation imply?

The interview, which will be audio recorded, takes between one and two hours, and involves questions concerning your opinion on DNA technology and its impact on the developing EU cooperation in fighting crime and terrorism, as well as on the changes and ethical risks brought about by the Prüm Decision, and on your country’s positioning and development with regard to the forensic uses of DNA technology and the exchange of DNA data.

The interview will be conducted in English, and can take place anywhere of your choosing, and we can arrange the time to suit your convenience. During the interview, if you feel that

you are incurring in any inconvenient disclosure of classified, or otherwise sensitive data, you may interrupt or stop the interview at any time. As an alternative, you may signal the interviewer in order to omit or anonymise a particular segment of the interview.

You may also decide to withdraw from participating in the study at any stage of the research. All you need to do is to inform the Principal Investigator that you no longer wish to take part and any data regarding your interview will not be included (please see contact information at the end of this document).

Policy for future publication of the project's findings

In written reports, public papers, scientific articles, and other project documents, the anonymity of the interviewees and participants will be guaranteed and the confidentiality over the data gathered respected. Any unanticipated issue will be dealt with through referral to professional codes of ethics and national and international legal frameworks.

Who funds this study?

This research is funded by the European Research Council – ERC (ERC Consolidator Grant nº 648608) and is hosted at the Communication and Society Research Centre (CECS), University of Minho, Portugal. The Principal Investigator is Professor Helena Machado.

The ERC does not share responsibility regarding the developments or findings of this project.

For more information, please contact:

Dr. Helena Machado (Principal Investigator)
Institute of Social Sciences – University of Minho
4710-057 Campus de Gualtar, Braga, Portugal
Tel.: +351253604212 | +351253604280 | Fax: +351253604697
E-mail: hmachado@ics.uminho.pt
Website: exchange.ics.uminho.pt

Anexo 6 - Acordo de confidencialidade para profissionais contratados para a realização das transcrições

Confidentiality Agreement - Exchange Project

EXCHANGE: Forensic Geneticists and the Transnational Exchange of DNA data in the EU: Engaging Science with Social Control, Citizenship and Democracy, is funded by the European Research Council – ERC (ERC Consolidator Grant nº 648608; hereinafter: Exchange) and is hosted at the Communication and Society Research Centre – University of Minho, Portugal. The Principal Investigator (hereinafter: PI) is Dr. Helena Machado.

This is a confidentiality agreement that refers to the transcription of interviews carried out under the project.

I, _____ transcriptionist for the Exchange Project, understand that I will be hearing recordings of confidential interviews. The information contained in these recordings have been revealed by interviewees who agreed to participate in this research on the condition that their interviews would remain strictly anonymous and confidential. I understand that I have a responsibility to honour this confidentiality agreement. Therefore, I agree:

1. To maintain full confidentiality with regards to any and all audio recordings and documentations received from the Exchange project;
2. To hold in strictest confidence the identification of any individual that may be inadvertently revealed during the transcription of recorded interviews, or in any associated documents;
3. To not make copies of any audio files or transcribed interviews texts, unless specifically requested to do so by the Exchange Project PI, Dr. Helena Machado;
4. To not share any information, about any party, with anyone but the project's PI and/or Exchange team members, namely: Dr. Rafaela Granja, Dr. Sheila Khan, Dr. Nina Amelung, Dr. Sara Matos, Dr. Filipa Queirós, Dr. Marta Martins and Dr. Ana Francisca Monteiro;
5. To store all audio files and related materials in a safe, secure location as long as they are in my possession;
6. To not upload, store and/or share any of the above-mentioned files online, in e-mail boxes, storage clouds and/or other virtual archives or servers;
7. To return all materials to the PI in their entirety, and within the agreed period;
8. To permanently delete or destroy all physical and/or electronic files and documents containing the interviews' audio, transcriptions and any related information from my computer's hard-drive and any back-up devices.

I am aware that I can be held legally responsible for any infringement of this confidentiality agreement, and for any harm incurred by individuals, due to the disclosure of information contained in the audio files and/or files to which I will have access.

Transcriber's name _____

Transcriber's signature _____

Date and Location _____