BIOÉTICA

NO

SÉCULO XXI

ANA FIGUEIREDO SOL

&

STEVEN S. GOUVEIA

13. BIOMETRIA E PRIVACIDADE: DESAFIOS BIOÉTICOS NA COOPERAÇÃO POLICIAL E JUDICIAL NA UNIÃO EUROPEIA

Sara Matos[1]

Resumo: A cooperação policial e judicial na União Europeia tem assentado crescentemente na partilha transnacional de dados biométricos, nomeadamente, de perfis genéticos e dados pessoais com o objetivo de combater a criminalidade. Este fenómeno gera desafios bioéticos complexos que conduzem à necessidade de um debate urgente em torno de orientações que respeitem um equilíbrio entre, por um lado, a proteção da privacidade e presunção de inocência, e, por outro, a necessidade coletiva de segurança. O debate agudiza-se num contexto histórico em que se assiste a uma intensificação e legitimação do recurso a tecnologias biométricas de vigilância a operar a uma escala global.

Os discursos tecno-científicos que legitimam estes sistemas tecnológicos neutralizam as diferenças legais, culturais e políticas entre os países a partir de regulações europeias que estabelecem um *standard* mínimo para a privacidade e a proteção de dados. Contudo, esses padrões são localmente reconstruídos, assistindo-se a práticas diferenciadas entre países. Num contexto de diversidade legislativa e jurisdicional dos Estados-Membros relativa à recolha, processamento e transmissão de dados de cidadãos, conduzindo a processos sociais de co-construção entre ciência/biotecnologia e controlo de populações criminalizadas.

Palavras-chave: biometria; privacidade; proteção de dados; cooperação policial e judicial; desafios éticos.

[1] Centro de Estudos de Comunicação e Sociedade da Universidade do Minho.

Introdução

Em junho do ano de 2013 vários órgãos de comunicação social, como o *The Guardian*[2,3] e o *The New York Times* [4], revelaram, sem precedentes, detalhes pormenorizados de atividades de vigilância operadas pela *US National Security Agency* (NSA) 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, empregado contratado pelos Estados Unidos para trabalhar nos serviços de inteligência do país, um nome até então desconhecido por todos (Dijck, 2014: 197; Wright & Kreissl, 2015: 6).

A divulgação destas informações confidenciais, por parte de Snowden, 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, entre outros. A deterioração do diálogo entre os países que mantinham relações com os EUA deveu-se às informações contidas nos documentos que originaram a fuga de informação sobre as ações de vigilância que os EUA levaram a cabo durante vários anos. Os documentos revelaram as extensas e intensas atividades de vigilância que incidiram em populações, bem como em líderes políticos, oficiais das Nações Unidas e empresas como a Google e a Petrobras, entre outras (Wright & Kreissl, 2015: 6).

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 e outras empresas que autorizaram a NSA a aceder às suas redes – foi-se deteriorando à medida que se divulgaram os documentos de Snowden, em grande medida, devido à falta de segurança e proteção de dados dos utilizadores que estas empresas revelaram no processo. O *The Washington Post* revelou ainda que a NSA tinha na sua posse um programa secreto chamado PRISM que visava precisamente a recolha de e-mails,

[2] 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.
[3] 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.
[4] 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 28 de maio de 2017.

chamadas telefónicas (na Internet), fotos, vídeos, ficheiros transferidos e dados oriundos de redes sociais recolhidos através das empresas supramencionadas (*idem*: 6-7).

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 operada em cidadãos que nunca tinham cometido crimes nem tampouco tinham sido suspeitos de terem cometido algum crime. Neste sentido, 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, sendo de realçar que em momento algum revelou informações que pudessem colocar em perigo os agentes operacionais que estavam responsáveis pela vigilância (*idem*: 8, 23).

Este acontecimento gerou várias respostas institucionais por parte dos países europeus que se viram alvo da vigilância em massa. No seguimento das revelações Snowden, a União Europeia começou a repensar os acordos realizados com os Estados Unidos para a partilha de dados financeiros e de tráfego, bem como os acordos mais restritos de proteção de dados como forma de repúdio pelo comportamento abusivo. 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 "nós" e os "outros" pode ser difícil de gerir, pois encontramo-nos numa era caraterizada pela globalização, pelo multiculturalismo e pela cooperação transnacional (*idem*: 36).

Discutir as questões sobre privacidade e proteção de dados elencadas por situações com esta dimensão revela-se pertinente, pois é necessário assegurar que a vigilância operada pelo Estado ou por outros órgãos institucionais seja equitativa e proporcional (Craig & Burca, 2008) quando se remete o debate para o equilíbrio entre o bem coletivo e os direitos individuais. Em particular, a análise dos desafios da proteção de dados genéticos no combate à criminalidade na União Europeia permite compreender as dinâmicas sociais e as relações de poder nas sociedades europeias liberais. Neste sentido, a presença de assimetrias de poder pode ser encarada como potencial geradora de desigualdades sociais, que estão muitas vezes acompanhadas pela criminalização e vulnerabilização de certas populações devido a novas configurações de identidades suspeitas que são construídas através do recurso a tecnologias de vigilância em massa que visam, grosso modo, o controlo social e apresentam-se como um desafio à democracia, devido à invisibilidade caraterística na recolha de dados de cidadãos.

O debate em torno da temática da vigilância generalizada dos cidadãos demonstra que a nova configuração da vigilância moderna coloca sérios problemas em relação à "privacidade, autonomia, dignidade, liberdade de discurso, liberdade de associação, liberdade de movimento, não discriminação, integração social, processo legal e presunção de inocência" (tradução livre da autora; Raab, 2015: 259). Como resultado, Raab (2015) enuncia três preocupações que advêm dos impactos da vigilância nas várias esferas da sociedade (*idem*: 261). A primeira remete para a visibilidade, pois a vigilância pode ser visível ou invisível, pelo que os cidadãos, muitas vezes, não sabem se estão a ser vigiados. A segunda tem que ver com a legalidade, na medida em que nem sempre é claro que determinada prática seja legal, sendo que a sua legitimidade varia consoante a jurisdição em que é utilizada. 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, sendo que as relações entre vigiados e vigilantes são bastantes complexas e colocam os primeiros em desvantagem perante os segundos, muitas vezes consequência de dados recolhidos previamente através do aparato tecnológico.

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 e partilha de dados pessoais. Neste sentido, a partilha transnacional automatizada de perfis genéticos e de dados pessoais com o objetivo de combater a criminalidade tem gerado intenso debate em diferentes esferas da sociedade relativamente à necessidade de um equilíbrio entre os direitos civis e a necessidade coletiva de segurança.

Proteção de dados pessoais na União Europeia

O exponencial desenvolvimento tecnológico ao nível dos sistemas de informação tem potenciado várias mudanças estruturais no que concerne ao acesso, processamento e troca de dados pessoais dos cidadãos. Considere-se que na era da economia da informação os dados pessoais dos cidadãos passam a ser equacionados enquanto moeda de troca de forma a garantir o acesso 'gratuito' (Dijck, 2014: 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. Dito isto, o conceito de proteção de dados 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: 693). Neste sentido, a União Europeia tem vindo a desenvolver um conjunto de instrumentos legislativos para que os cidadãos tenham o seu direito à proteção de dados e à privacidade protegidos.

A Declaração Universal dos Direitos Humanos consagra no artigo 12.º o direito à privacidade e ressalva ainda 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: 692). No plano europeu tem-se a Carta dos Direitos Fundamentais da União Europeia 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 Lisboa e é juridicamente vinculativa nas instituições e órgãos da União e nos Estados-Membros quando estes aplicam legislação da UE. A Convenção Europeia dos Direitos Humanos reconhece, no artigo 8.º, o direito ao respeito pela vida privada e familiar. Atualmente, tem-se ainda a Diretiva Europeia de Proteção de Dados Pessoais (Diretiva 95/46/CE) 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, regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos, que será revogada em maio de 2018. Estabeleceram-se vários princípios que devem ser cumpridos pelas entidades/organizações públicas e privadas que os controlam e processam. Nomeadamente, a (1) limitação da finalidade, 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, que tem por objetivo que não seja recolhida informação pessoal para além da necessária para o fim específico. A (3) proporcionalidade, 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, que tem que ver com a responsabilização do Estados-Membros da UE quanto à supervisão do processamento dos dados pessoais (Brown, 2009; European Data Protection Supervisor, 2006; Gamero et al., 2008; Gonçalves & Jesus, 2012, 2013; Harbo, 2010; Hert, 2005). Pretendeu-se com a redação deste instrumento legislativo a criação de um critério mínimo de proteção de dados pessoais entre os países da União Europeia. Contudo, 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; Brown, 2009; Gilbert, 2007).

No entanto, com a evolução tecnológica, a crescente globalização dos mercados (Lyon, 2004) e as diferentes aplicações, por parte dos Estados-Membros, das normas previstas na Diretiva supramencionada, a Comissão apresentou, 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 estre Estados e a diminuição dos dispendiosos encargos administrativos. Neste sentido, foi apresentada a proposta para o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 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 revoga 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 Conselho, de 27 de novembro de 2008, a revogar 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 Conselho, de 27 de abril de 2016, 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.

Apesar de todos os esforços para a 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 para o Estado, pois pode inibir o fluxo de informação. Sexto, e último, a reflexão sobre o 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 (*idem*: 257-258).

Privacidade social

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 e recolher informação sobre as pessoas permitindo segui-las através do tempo e do espaço. Os desenvolvimentos que permitem este tipo de práticas de vigilância ocorreram em três grandes áreas científicas, nomeadamente, nas bases de dados computadorizadas (Goos et al., 2015: 56; Nissenbaum, 2010: 36), no avanço da ciência e da engenharia das redes de comunicação digitais e no desenvolvimento das técnicas de análise de dados. Estes avanços foram também sistematizados, com base na mesma

argumentação, por Solove (2006), citando o autor, "o poder e o alcance da agregação são diferentes na Era da Informação; os dados que são recolhidos das pessoas são significativamente mais extensos, o seu processo de combinação é muito mais fácil, e as tecnologias informáticas que os analisam são mais sofisticadas e poderosas" (tradução livre da autora; *idem*: 506).

Tendo como pano de fundo os avanços científicos supramencionados, existem várias posições no que concerne à proteção da privacidade. Por um lado, defende-se 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: 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 de informação unidirecional, na verdade, encontram-se mais interessados em assegurar o uso adequado dos seus dados pessoais. 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*: 2).

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 privacidade de associação que remete para a privacidade de grupo (*idem*: 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. 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 caráter 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 de forma mais

adequada, com o objetivo último de equilibrar a necessidade coletiva de segurança e o direito à privacidade do indivíduo.

De forma mais genérica e também complementar às categorizações acima explanadas, Allen (1999) defende que a privacidade pode ser entendida sob três dimensões, nomeadamente, a privacidade física, a privacidade informacional e, por último, a privacidade proprietária (*idem*: 713). As dimensões apresentadas 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.

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: 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. 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 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. 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 (*idem*: 433).

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 "é um valor inerente à sociedade liberal" (Raab, 2015: 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. 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 o "pilar fundamental da democracia política e de uma panóplia de direitos humanos ou civis" (tradução livre da autora; *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), "a invasão da privacidade causa danos porque somos socializados de modo a experienciar normas comuns enquanto pré-requisitos essenciais da nossa própria identidade e autorrespeito" (tradução livre da autora; *idem*: 2094).

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, que 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 (*idem*: 86). 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 (*idem*: 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, caraterística 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, isto é, os investigadores alegam que este tipo de técnicas pode ser extremamente útil na identificação precoce de terroristas (Hauge et al., 2016: 5 apud Metcalf & Crawford, 2016: 2). 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, 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*: 2).

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* (*ibidem*). 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 nas bases de dados.

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 (Gandy, 1993; Cohen, 2000; Lyon, 2007; Solove & Rotenberg 2003; Solove 2004), apresentando-se como potenciais ameaças à privacidade dos indivíduos. A aparente falta de questionamento sobre as questões que têm vindo a ser enunciadas pode estar relacionadas com o facto de ciências como a ciência computacional, a estatística e a matemática aplicada descurarem a dimensão social, ética e política dos dados que analisam, encarando-os enquanto neutros. Esta posição não permitiu que o desenvolvimento e a criação da tecnologia e dos *softwares* fossem realizados com base nos princípios de *privacy by design* (Jones & Raab, 2015; Schaar, 2010), que pretendem uma avaliação de riscos previamente à conclusão do sistema, com o objetivo último de evitar consequências, como discriminação social, para os indivíduos que estão à sua mercê. Através de um maior recurso à construção de tecnologia através 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 esta secção com a tese defendida por Nissenbaum, citando:

> Nós temos o direito à privacidade, mas não é nem o direito de controlar a informação pessoal nem o direito de restringir o acesso a essa informação. Em vez disso, é o direito de viver num mundo no qual as nossas expetativas sobre o fluxo de informação pessoal são, na sua maioria, atendidas; expetativas que são moldadas não só pela força do hábito e da convenção,

> como também pela confiança generalizada no apoio mútuo que estes fluxos proporcionam para os princípios-chave organizadores da vida social, incluindo os políticos e os morais. Este é o direito que eu chamo de integridade contextual, alcançada através do equilíbrio harmonioso de regras sociais, ou normas, com valores locais e gerais, fins e propósitos. (tradução livre da autora; Nissenbaum, 2010: 231).

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 (Lessig, 1999 apud Lyon, 2007: 35), que passa por perceber quais são os argumentos utilizados para legitimar a sua aplicação generalizada ao "corpo" dos cidadãos. Neste sentido, 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, "eliminar os problemas antes de emergirem, absolutamente antes de eles terem a oportunidade de se tornarem problemas" (tradução livre da autora; *idem*: 60). Através dos discursos que incidem sobre o risco tem-se verificado o desenvolvimento do pânico moral (Cohen, 2002; Garland, 2008; Goode & Bem-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, sendo que esta disseminação do terror é realizada através dos meios de comunicação social (Altheide, 2006; Amoore 2006, 2007 apud Frois, 2008: 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: 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*: 6). 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: 154), os Governos têm criado uma panóplia de respostas que pretendem erradicar qualquer ato desviante, estas medidas incluem "leis com tolerância zero, forças privadas de segurança, comunidades fechadas e vigilância tecnológica" (*idem*: 1).

No pacote de medidas adotado pode incluir-se a expansão das tecnologias de identificação biométrica humana, também conhecidas como biotecnologias, pós 11 de setembro de 2001. Importará, portanto, perceber de que forma estes sistemas contribuem para o aparelho de vigilância, de que modo se encontram relacionados com formas de biopoder e quais as questões levantadas quanto à possível ameaça de direitos civis. A biometria tem como finalidade o estudo das caraterísticas 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 et al., 2004; Liu, 2013: 29). Segundo Bateman (1998) as tecnologias biométricas podem ser encaradas de acordo com três grupos genéricos, respetivamente, para fins de aplicação comercial, de aplicação governamental e de aplicação forense (apud Liu, 2013: 49).

Pugliese (2012), no seu livro, apreende as tecnologias biométricas através do conceito de 'conhecimento situado' cunhado por Haraway (1991: 188) e pretendeu analisar as dimensões sociais e políticas inscritas nas mesmas (Pugliese, 2012: 5). Prossegue argumentando que estas tecnologias são "instrumentos contemporâneos da biopolítica" (*idem*: 2) e, como tal, encontram-se inscritas e enquadradas nas infraestruturas das relações de poder. Podem ainda observar-se caraterísticas da sociedade disciplinar na medida em que a autentificação e verificação da identidade dos indivíduos dá-se através de categorias normativas pré-definidas, como o género, a raça, a classe social, entre outros (*ibidem*). Nas palavras do autor estes aparelhos operam no sentido da "individualização, identificação, classificação e distribuição de modelos de sujeitos biometricamente inscritos" (*ibidem*) 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 a privacidade, valores democráticos, dos indivíduos (Nuger & Wayman, 2004).

A biovigilância é o resultado do desenvolvimento das tecnologias biométricas aliada 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 vulnerabilização. Considerando que existe o risco de se criminalizarem estas populações mesmo antes da ocorrência de qualquer crime, com base na lógica da prevenção de delitos (Pugliese, 2012: 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 Clark (2001), as tecnologias biométricas, entre as que fazem parte do aparelho de vigilância, apresentam-se como as que mais riscos acarretam para a liberdade 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, pois quando combinadas com técnicas criptográficas, estas podem, inclusive, preservar e proteger a identidade e integridade dos indivíduos (apud Liu, 2013: 5).

O debate supramencionado abarca também 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 ameaças à 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 (*idem*: 1). Nesta linha de pensamento, as limitações que têm vindo a ser impostas à privacidade dos indivíduos podem conduzir ao reforço e/ou desenvolvimento de problemas 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 (*idem*: 64). Uma outra fragilidade que pode estar na origem de situações que degradam os direitos humanos e civis dos vigiados tem que ver com a possibilidade de ocorrer *function creep* (Dahl & Sætnan, 2009). A digitalização das informações e a focalização nas componentes biológicas do ser humano revelam-se outro aspeto sobre o qual se deve refletir, na medida em que a priorização dos fatores biológicos relega por completo aspetos que não são passíveis de ser medidos por estas tecnologias, como por exemplo, a personalidade do indivíduo vigiado (Feldman, 2003: 666). A tendência tem sido a de uma sociedade que cada vez mais reduz os seus atores sociais a uma panóplia de caraterísticas biológicas 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, efetivos 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 (*idem*: 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 privacidade (Liu, 2013: 72). 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*: 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*: 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*: 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 são explicativos da aparente falta de debate público sobre a sua eficácia. Wayman (2000) avança com outro ponto que deve ser tomado em consideração quando se abarca o tema do avanço tecnológico estando relacionado 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 (*idem*: 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 de determinada 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 esta tentativa de solução no novo pacote de medidas adotadas pela União Europeia protetoras das informações pessoais, nomeadamente, através da redação de um Regulamento vinculativo para todos os Estados-Membros e a apresentação de Diretivas sobre, por exemplo, a esfera da investigação criminal.

Bases de dados forenses de perfis de DNA

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: 103). Atualmente, os Governos vertem da ciência sistemas mais sofisticados que permitem a continuação deste tipo de práticas numa escala até então impossível (Miranda, 2015: 430; Pugliese, 2012: 17). Citando Anthony Burke (2001), o conceito de segurança deve ser teorizado enquanto "tecnologia política" que encerra em si um conjunto de "rede de práticas e técnicas que produzem e manipulam identidades, sociedades, espaços e fluxos" (*idem*: xxxiv). Portanto, com o desenvolvimento de tecnologias biométricas de vigilância assiste-se à intensificação da vigilância digital do corpo dos cidadãos (Aas, 2006: 144) através de técnicas e procedimentos de instrumentalização (Pugliese, 2012: 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: 144; Campbell & Van Brakel, 2015; Pugliese, 2012: 55).

A utilização de informações genéticas como ferramenta de identificação de indivíduos suspeitos conduziu à criação de bases de dados nacionais de perfis genéticos de DNA para fins forenses. 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 digitais ou biológicos. 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 (Machado, Alves & Silva, 2015: 62), bem como para estimular a confiança pública relativamente à transparência das leis e utilização de dados pessoais (European Data Protection Supervisor, 2006; Williams, Johnson, & Martin, 2004: 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 permitem encontrar conexões com casos arquivados e entre diferentes cenas de crime; identificar através de *hits* delinquentes e perpetuadores de crimes; garantir a identificação mais rápida de ofensores, prevenindo atividades criminosas; o DNA pode oferecer pistas que ajudem na identificação de um indivíduo; têm um efeito dissuasor (premissa muito discutida); e, 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).

Colocando em retrospetiva 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, 2000; Hindmarsh & Prainsack, 2010; Krimsky & Simoncelli, 2011; Lazer, 2004; Machado & Silva, 2016; Machado, Silva & Santos, 2008: 135-137; McCartney, 2006; 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 imaginário 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, Lemke, & Prainsack, 2012; Lynch, Cole, McNally, & Jordan, 2008; Maciel & Machado, 2014: 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, Wilson & Williams, 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 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*, onde na decisão constou que a retenção ilimitada de perfis de DNA não é justificável, constituindo-se como uma violação do direito à privacidade (Annas, 2009; Tseloni & Pease, 2010). 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: 69; Machado, Silva & Santos, 2008: 136; Maras, 2012; McCartney, 2006, 2012; Thorogood & Zawati, 2015: 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: 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 desadequado 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: 13; Wallace, Jackson, Gruber & Thibedeau, 2014: 58).

Face à discussão no âmbito da utilização das bases de dados forenses, 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 caraterizado 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, 2008: 155-161; Williams & Johnson, 2004b: 211-219).

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: 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 (*ibidem*). No entanto, é de salientar a escassez de estudos empíricos 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.

Partilha transnacional de dados genéticos para fins forenses

O Tratado de Schengen (1997) 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 atravessou 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: 243-244; O'Neill, 2010).

O Tratado de Prüm foi assinado com o objetivo de garantir o acesso mútuo às bases de dados nacionais de perfis genéticos, tal como de impressões digitais e de registos de veículos através de um sistema de *hit/no hit*. Assim, quando um Estado-Membro confirma a correspondência do perfil de DNA da sua base de dados com a de outro Estado-Membro (o chamado *step* 1), se solicitado, segue-se a partilha de mais informações sobre o indivíduo suspeito de acordo com a lei de Proteção de Dados dos países envolvidos nesta troca de informações, bem como os critérios mínimos estabelecidos pela Comissão Europeia para a proteção de dados (o chamado *step* 2) (Machado & Silva, 2010; Prainsack, 2010). Saliente-se que este processo permite avaliar a legislação nacional e perceber se a troca está 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: 316; Prainsack & Toom, 2010). A argumentação em torno da legitimação deste sistema de vigilância genética segue os mesmos contornos dos restantes aparelhos tecnológicos, na medida em que 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: 92).

A transposição do Tratado de Prüm para a lei da União Europeia, em 2008, gerou intenso debate em torno da proteção de dados (Decisão 2008/615/JHA de 23 de junho) (Kierkegaard, 2008: 243-244; Maciel & Machado, 2014: 149). O Tratado teve como ambição a uniformização técnica e científica, mas também legislativa de forma a garantir o cumprimento do direito humano à privacidade. 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). Pensando no enquadramento social e legal do Tratado de 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 (*idem*: 204). O autor aponta fragilidades ao sistema quanto à proteção de dados, pois as negociações sobre Prüm careceram do envolvimento das autoridades nacionais de proteção de dados, bem como da presença da Autoridade Europeia para a Proteção de Dados (*idem*: 205).

A implementação da partilha de dados pessoais tem enfrentado problemas, por um lado, devido à falta de confiança entre as autoridades do Estados-Membros (Hijmans, 2006: 2-3), por outro, devido à propriedade dos dados (Bigo et al., 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 sem que o tema seja debatido no plano nacional, quer por parte da opinião pública quer pelo parlamento (Bellanova, 2008: 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*: 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, nomeadamente, de que forma é que se pode avaliar a proporcionalidade das medidas aplicadas à supressão da privacidade, se os atores mais relevantes no processo "são marginalizados no campo em disussão" (*idem*: 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 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 Tratado 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, 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: 130; Prainsack & Toom, 2013).

O Tratado de Prüm, ao implementar no Espaço da União Europeia a partilha transnacional e automatizada de perfis genéticos, apoiou-se na ideia de harmonização e estandardização técnico-científica, com o objetivo de neutralizar as diferenças legais, culturais e políticas entre os diferentes países (Lampland & Star, 2009: 4-5; Prainsack & Toom, 2010, 2013). A partilha e a circulação de dados no contexto de Prüm deve-se também à criação de *standards* que visam garantir a interoperabilidade (Balzacq et al., 2006; Bigo, 2008: 105; De Hert & Gutwirth, 2006; McCartney 2014a, 2014b) tecnológica das bases de dados dos países signatários. Concretamente, a harmonização da cooperação policial e judiciária em Prüm, tem-se deparado com divergências nas práticas dos países da União Europeia, nomeadamente ao nível dos dados pessoais que são partilhados no step 2. Todo o processo de criação de *standards* significa "codificar, incorporar ou prescrever éticas e valores" (Lampland & Star, 2009: 4-5), que suporta uma componente fortemente normativa, que permite e justifica 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. Portanto é fulcral que se desconstrua 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; bem como, 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. Portanto, a estandardização mais do que uma homogeneização pode significar modalidades heterogéneas de (d)estandardização da privacidade.

Agradecimentos

Este trabalho recebeu financiamento do Conselho Europeu de Investigação (ERC) sob o programa de pesquisa e inovação da União Europeia Horizonte 2020 (Contrato N.º [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 Helena Machado e sedeado no

Centro de Estudos de Comunicação e Sociedade da Universidade do Minho. Agradeço o apoio do projeto EXCHANGE, bem como os comentários críticos de Helena Machado tecidos durante a redação do presente capítulo.

Referências bibliográficas

AAS, K. F. (2006) "'The body does not lie': Identity, risk and trust in technoculture", Crime, Media, Culture, 2(2), pp. 143-158.

AAS, K. F. (2009) "Commentary - Surveillance: Citizens and the state", Surveillance & Society, 6(3), pp. 317-321.

AAS, K. F. (2013) Globalization and crime, Vol. I-III, London: Sage.

ALLEN- CASTELLITTO, A. (1999) "Coercing Privacy", William and Mary Law Review, 40, pp. 723-757.

ALTHEIDE, D. (2006) Terrorism and the Politics of Fear, Lanham, MD: Altamira Press.

AMOORE, L. (2006) "Biometric borders: governing mobilities in the war on terror", Political Geography, 25, pp. 336-351.

AMOORE, L. (2007) "Vigilant visualities: the watchful politics on the war on terror", Security Dialogue, 38, pp. 215-232.

ANIL, K., ROSS, A. & PRABHAKAR, S. (2004) "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, n. 1, pp. 40-20.

ANNAS, G. (2009) "Protecting privacy and the public: Limits on police use of bioidentifiers in Europe", New England Journal of Medicine, 361(2), pp. 196-201.

BALZACQ, T. (2005) "From a Prüm of 7 to a Prüm of 8 +: What are the implications ?", Policy Department C Citizens Rights and Constitutional Affairs, pp. 1-7.

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", n. 234. Retrieved from http://www.libertysecurity.org/IMG/pdf/WD234_e-version.pdf

BARAD, K. (2003) "Posthumanist performativity: Toward an understanding of how matter comes to matter", Signs: Journal of Women in Culture and Society, 28(3), pp. 801-831.

BATEMAN, S. (1998) "Biometrics initiatives signal need for digital identification", Computer Shopper.

BELLANOVA, R. (2008) "The 'Prüm Process': The Way Forward for EU Police Cooperation and Data Exchange?" in GUILD E. & GEYER F. (orgs.) Security versus Justice? Police and judicial cooperation in the European Union, Farnham: Aldershot Ashgate, pp. 203-221.

BIGO, D. (2008) "EU Police Cooperation: National Sovereignty Framed by European Security?" in GUILD E. & GEYER F. (orgs.) Security versus Justice? Police and judicial cooperation in the European Union, Farnham: Aldershot Ashgate, pp. 91-108.

BIGO, D., BRUGGEMAN, W, BURGESS, P. & MITSILEGAS, V. (2007), "The Principle of Information Availability", Paris: CHALLENGE.

BOGARD, W. (2007) "Welcome to the Society of Control: The Simulation of Surveillance Revisited" in HAGGERTY K. & ERICSON R. (orgs.) The new politics of surveillance and visibility, Toronto: University of Toronto Press, pp. 55-78.

BROWN, M. B. (2009) Science in democracy: Expertise, institutions, and representation, Cambridge, MA and London: MIT Press.

BURKE, A. (2001) In fear of security, Annandale, NSW: Pluto Press

BYGRAVE, L. A. (2002) Data Protection Law: Approaching Its Rationale, Logic and Limits, The Hague: Kluwer Law International.

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), pp. 39-46.

CAVOUKIAN, A. (2001) Public safety is paramount - but balanced against privacy.

CLARK, R. (2001) Biometrics and Privacy. Disponível em: http://www.rogerclarke.com/DV/Biometrics.html

COHEN, J. (2000) "Examined Lives: Informational Privacy and the Subject as Object", Stanford Law Review, 52, pp. 1373-1437.

COSTA, S. & NUNES, J. A. (2001) "As atribulações da ciência «impura»: A harmonização da biologia forense e a diversidade dos sistemas jurídicos" in NUNES J. A. & GONÇALVES M. E. (orgs.) Enteados de Galileu? A semiperiferia no sistema mundial da ciência, Porto: Afrontamento, pp. 107–141.

CRAIG, P. & BURCA, G. D. (2008) EU law, Oxford: Oxford University Press.

DAHL, J. Y. & SÆTNAN, A. R. (2009) "'It all happened so slowly' – On controlling function creep in forensic DNA databases", International Journal of Law, Crime and Justice, 37(3), pp. 83–103.

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), pp. 21–35.

DIERICKX, K. (2008), "A Belgian perspective - Forum on the Nuffield report 'The forensic use of bioinformation: Ethical Issues.'", BioSocieties, 3(1), pp. 97–99.

DIJCK, J. van. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, 12(2), 197–208.

DUSTER, T. (2004) "Selective arrests, an ever-expanding DNA forensic database, and the specter of an early-twenty-first-century equivalent of phrenology" in LAZER D. (org.) The technology of justice: DNA and the criminal justice system, Cambridge: MIT Press, pp. 315–334.

DUSTER, T. (2006) "The molecular reinscription of race: Unanticipated issues in biotechnology and forensic science", Patterns of Prejudice, 40(4–5), pp. 427–441.

EUROPEAN DATA PROTECTION SUPERVISOR. (2006) Annual report: Consolidating the EDPS. European Data Protection Supervisor, Vol. 34, Luxembourg. Disponível em http://www.ncbi.nlm.nih.gov/pubmed/20536774

FELDMAN, R. (2003) "Considerations on the emerging implementation of biometric technology", Hastings Communications & Entertainment Law Journal, 25, pp. 653-82.

FINN, R., WRIGHT, D. & FRIEDEWALD M. (2013) "Seven types of privacy", in GUTWIRTH S., LEENES R., DE HERT P. et al. (orgs.), European data protection: Coming of age?, Springer: Dordrecht.

FIODOROVA, A. (2014) "DNA for crime investigation: European co-operation model". Recent Advances in DNA and Gene Sequences, 8, pp. 126–133.

FROIS, C. (org.) (2008) A sociedade vigilante: Ensaios sobre privacidade, identificação e vigilância, Lisboa: Imprensa de Ciências Sociais, pp. 67–81.

GAMERO, J.-J., ROMERO, J.-L., PERALTA, J.-L., CORTE-REAL, F., GUILLÉN, M. & ANJOS, M.-J. (2008) "A study of Spanish attitudes regarding the custody and use of forensic DNA databases", Forensic Science International, 2(2), pp. 138–149.

GANDY, O.H. (1993) The panoptic Sort: A Political Economy of personal Information, Boulder, CO: Westview Press.

GARLAND, D. (2008) "On the concept of moral panic", Crime, Media, Culture, 4 (1), pp. 9-30.

GILBERT, N. (2007) Dilemmas of privacy and surveillance: Challenges of technological change, London.

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), pp. 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), pp. 255–263.

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, Vol. 1, n. 4, 2009.

GOOS, K., FRIEDEWALD, M., WILLIAM, C., WEBSTER, R. & LELEUX, C. (2015) "The co-evolution of surveillance technologies and surveillance practices" in WRIGHT D. & KREISSL R. (orgs.) Surveillance in Europe, London: Routledge, pp. 51-100.

GUILLÉN, M., LAREU, M. V., PESTONI, C. & SALAS, A. (2000) "Ethical-legal problems of DNA databases in criminal investigation", Journal of Medical Ethics, 26, pp. 266–271.

HARAWAY, D. (1991) Simians, Cyborgs, and Women: The Reinvention of Nature, New York: Routledge.

HARBO, T. (2010) "The Function of the Proportionality Principle in EU Law", European Law Journal, 16 (2), pp. 158-185.

HAUGE M., STEVENSON M., ROSSMO D., et al. (2016) "Tagging Banksy: Using geographic profiling to investigate a modern art mystery", Journal of Spatial Science, 61(6), pp. 185–190.

HEINEMANN, T., LEMKE, T. & PRAINSACK, B. (2012) "Risky profiles: Societal dimensions of forensic uses of DNA profiling technologies", New Genetics and Society, 31(3), pp. 249–258.

HERT, P. (2005) Biometrics: Legal issues and implications, Sevilla.

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. & PRAINSACK, B. (orgs.) (2010) Genetic suspects: Global governance of forensic DNA profiling and databasing, Cambridge: Cambridge University Press.

HOUSE OF LORDS. (2007) Prüm: An effective weapon against terrorism and crime?, Home Office, London.

HOVEN (2001) "Privacy and the Varieties of Moral Wrongdoing in an information age", Computers and Society In SIGCAS Comput. Vol. 27, n. 3.

HUMAN GENETICS COMMISSION. (2001) "Whose hands on your genes? A discussion document on the storage protection and use of personal genetic information", London.

HUSTINX, P. (2010) EU data protection law - Current state and future perspectives, Ethical Dimensions of Data Protection and Privacy, Tallin, Estonia

INTERPOL (2009) Interpol handbook on DNA data exchange and practice.

JASANOFF, S. (org.) (2011). Reframing rights. Bioconstitutionalism in the genetic age, Chicago: MIT Press.

JOHNSON, P., & WILLIAMS, R. (2007) "Internationalizing new technologies of crime control: Forensic DNA databasing and datasharing in the European Union", Policing & Society, 17(2), pp. 103–118.

JONES, R. & RAAB, C. (2015) "Effects of surveillance on civil liberties and fundamental rights in Europe – Good practice in privacy design: some examples" in WRIGHT D. & KREISSL R. (orgs.) Surveillance in Europe, London: Routledge, pp. 293-294.

KIERKEGAARD, S. (2008) "The Prüm decision - An uncontrolled fishing expedition in 'Big Brother' Europe", Computer Law and Security Report, 24(3), pp. 243–252.

KIETZ, D. & MAURER, A. (2006) "From Schengen to Prüm. Deeper integration through enhanced cooperation or signs of fragmentation in the EU?", SWP, pp. 1–5.

KREISSL, R., NORRIS, C., KRLIC, M., GROVES, L. & AMICELLE, A. (2015) "Surveillance - preventing and detecting crime and terrorism" in WRIGHT D. & KREISSL, R. (orgs.) Surveillance in Europe, London: Routledge, pp. 150-210.

KRIMSKY, S. & SIMONCELLI, T. (2011) Genetic justice: DNA Data Banks, criminal investigations, and civil liberties, New York: Columbia University Press.

LAMPLAND, M. & STAR, S. L. (orgs.) (2009) Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life, Ithaca: Cornell University Press.

LAW, J. (2008) "On sociology and STS", Sociological Review, 56(4), pp. 623–649.

LAZER, D. (org.) (2004) DNA and the criminal justice system: The technology of justice, Cambridge, MA: MIT Press.

LESSIG, L. (1999) Code and other laws of cyberspace, New York: Basic Books

LIU, N. (2013) Bio-privacy: Privacy regulations and the challenge of biometrics, Abingdon: Routledge.

LYNCH, M., COLE, S., MCNALLY, R. & JORDAN, K. (2008). Truth machine: The contentious history of DNA fingerprinting, Chicago: University of Chicago Press.

LYON, D. (2004) "Globalizing surveillance", International Sociology, Vol. 19, n. 2.

LYON, D. (2007) Surveillance studies: An overview, Cambridge: Polity Press.

MACHADO, H. & SILVA, S. (2008) "Confiança, voluntariedade e supressão dos riscos: Expectativas, incertezas e governação das aplicações forenses" in FROIS C. (org.) A sociedade vigilante: Ensaios sobre privacidade, identificação e anonimato, Lisboa: Imprensa de Ciências Sociais, pp. 151–174.

MACHADO, H. & SILVA, S. (2016) "Voluntary participation in forensic DNA databases: Altruism, resistance, and stigma", Science, Technology & Human Values, 41(2), pp. 322–343.

MACHADO, H. (2011) "Construtores da bio(in)segurança na base de dados de perfis de ADN", Etnográfica, 15(1), pp. 153–166.

MACHADO, H., & SILVA, S. (2010). Portuguese forensic DNA database: Political enthusiasm, public trust and probable issues in future practice. In HINDMARSH R. & PRAINSACK B. (orgs.), Genetic suspects: Global governance of DNA profiling and databasing (pp. 218–239). Cambridge: Cambridge University Press.

MACHADO, H., ALVES, B. & SILVA, S. (2015) "Proteção de dados pessoais em biobancos médicos e forenses: 'solidariedade' e reconfigurações da participação pública" in FONSECA C. & MACHADO H. (orgs.) Ciência, identificação e tecnologias de governo, Porto Alegre: Editora da UFRGS/CEGOV, pp. 56–74.

MACHADO, H., SILVA, S. & SANTOS, F. (2008) Justiça tecnológica: promessas e desafios, Ermesinde: Ecopy.

MACIEL, D. & MACHADO, H. (2014) "Biovigilância e governabilidade nas sociedades da informação" in MACHADO H. & MONIZ H. (orgs.) Bases de dados genéticos forenses: Tecnologias de controlo e ordem social, Coimbra: Coimbra Editora, pp. 141–166.

MARAS, M.-H. (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), pp. 65–81.

MARX, G. (2007) "Varieties of Personal Information as Influences on Attitudes towards Surveillance" in HAGGERTY K. & ERICSON R. (orgs.), The new politics of surveillance and visibility, Toronto: University of Toronto Press, pp. 79-110.

MCCARTNEY, C. (2006) Forensic identification and criminal justice: Forensic science, justice and risk, Cullompton: Willan Publishing.

MCCARTNEY, C. (2012) "Of weighty reasons and indiscriminate blankets: The retention of DNA for forensic purposes", The Howard Journal of Criminal Justice, 51(3), pp. 245–260.

MCCARTNEY, C. (2014a) "Forensic data exchange: Ensuring integrity", Australian Journal of Forensic Sciences, 47(May), pp. 36–48.

MCCARTNEY, C. (2014b) “Transnational exchange of forensic evidence” in BRUINSMA G. & WEISBURD D. (orgs.) Encyclopedia of criminology and criminal justice, New York: Springer, pp. 5302–5313.

MCCARTNEY, C., WILLIAMS, R. & WILSON, T. (2010) “The future of forensic bioinformation. Leeds”. Disponível em: http://www.law.leeds.ac.uk/assets/files/research/ccjs/forensic-bioinformation-report.pdf

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), pp. 305–322.

METCALF, J. & CRAWFORD, K. (2016) “Where are human subjects in Big Data research? The emerging ethics divide”, Big Data & Society, (June), pp. 1–14.

MIRANDA, D. (2015) “Criminal investigation through the eye of the detective: Technological innovation and tradition”, Surveillance & Society, 13(3), pp. 422–436.

MONAHAN, T. (2010) Surveillance in the time of insecurity, New Brunswick, NJ: Rutgers University Press.

NISSENBAUM, H. (2010) Privacy in context: technology, policy, and the integrity of social life, Stanford: Stanford Law Books.

NUFFIELD COUNCIL ON BIOETHICS. (2007) The forensic use of bioinformation: Ethical issues, London. Disponível em: http://nuffieldbioethics.org/wp-content/uploads/The-forensic-use-of-bioinformation-ethical-issues.pdf

NUGER, K. P. & WAYMAN, J. L. (2004) “Biometrics and the US Constitution”, in WAYMAN J., ANIL J., DAVIDE M. & DARIO M. (orgs.) Biometric Systems: Technology, Design and Performance Evaluation, Nottingham: Springer, pp. 311-33.

O’NEILL, M. (2010) “The issue of data protection and data security in the (Pre-Lisbon) EU Third Pillar”, Journal of Contemporary European Research.

POST, R. (2001) “Three concepts of privacy”, Georgetown Law Review, Vol. 89.

PRAINSACK, B. & ARONSON, J. (2015) “Forensic genetic databases: Ethical and social dimensions”, International Encyclopedia of the Social & Behavioral Sciences, 9, pp. 339–345.

PRAINSACK, B. & TOOM, V. (2010) “The Prüm regime. Situated dis/empowerment in transnational DNA profile exchange”, British Journal of Criminology, 50(6), pp. 1117–1135.

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), pp. 71–79.

PRAINSACK, B. (2010) “Key issues in DNA profiling and databasing: Implications for governance”, in HINDMARSH R. & PRAINSACK B. (orgs.) Genetic suspects: Global governance of forensic DNA profiling and databasing, Cambridge: Cambridge University Press, pp. 153–174.

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), pp. 32–47.

PUGLIESE, J. (2012) Bodies, technologies, biopolitics, New York and London: Routledge.

RAAB, C. (2015) “Effects of surveillance on civil liberties and fundamental rights in Europe – surveillance: Effects on privacy, autonomy and dignity”, in WRIGHT D. & KREISSL R. (orgs.), Surveillance in Europe, London: Routledge.

REGAN, P. (1995) Legislating privacy, Chapel Hill: University of North Carolina Press.

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), pp. 1–13.

SCHAAR, P. (2010) “Privacy by design”, Identity in the Information Society - Special Issue, 3(2), pp. 267–274.

SCHOEMAN, F. (1992) Privacy and social freedom, Cambridge University: Press, Cambridge.

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), pp. 319–342.

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), pp. 886–906.

SOLOVE, D. & ROTENBERG, M. (2003) Information Privacy Law, New York: Aspen publishers.

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), pp. 477-564.

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), pp. 690–702.

TOOM, V. (2012) “Bodies of science and law: Forensic DNA profiling, biological bodies, and biopower”, Journal of Law and Society, 39(1), pp. 150–166.

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, pp. e1–e4.

TSEKERIS, C. (2007) “Performativity”, in RITZER J. (org.) Blackwell Encyclopedia of Sociology.

TSELONI, A. & PEASE, K. (2010) “DNA retention after arrest: Balancing privacy interests and public protection”, European Journal of Criminology, 8(1), pp. 32–47.

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), pp. 606–610.

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), pp. 57–63.

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.

WILLIAMS, R. & JOHNSON, P. (2004a) “Circuits of surveillance”, Surveillance & Society, 2(1), pp. 1–14.

WILLIAMS, R. & JOHNSON, P. (2004b) “‘Wonderment and dread’: Representations of DNA in ethical disputes about forensic DNA databases”, New Genetics and Society, 23(2), pp. 205–223.

WILLIAMS, R. & WIENROTH, M. (2014) Ethical, social and policy aspects of forensic genetics: A systematic review, Newcastle upon Tyne, UK.

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.

WOODWARD, J. (1997) Biometrics: Identifying law & Policy concerns. Disponível em: http://www.cse.msu.edu/~cse891/Sect601/textbook/19.pdf

WRIGHT, D. & KREISSL, R. (2015) “European responses to the Snowden revelations”, in Reinhard K. (org.) Surveillance in Europe, London: Routledge, pp. 6-50.