Big Data na investigação criminal: "Imaginário Europeu" e orientações para o futuro

Laura Neiva

Doutoranda em Sociologia, Instituto de Ciências Sociais, Centro de Estudos em Comunicação e Sociedade (CECS), Universidade do Minho, Portugal

Helena Machado

Departamento de Sociologia, Instituto de Ciências Sociais da Universidade do Minho

Resumo

Por via de uma análise interpretativa e compreensiva do Regulamento Geral da Proteção de Dados 2016/679 e da Diretiva 2016/680, complementada por uma análise de discursos da Comissão Europeia que enquadram esta legislação, este texto reflete sobre o "Imaginário Europeu" em torno de *Big Data*, tecnologias e proteção de dados no contexto da investigação criminal. Analisamos o modo como são retratados os riscos e os benefícios das novas tecnologias nestes contextos e as controvérsias fluídas que surgem em torno de, por um lado, definir padrões de segurança e, por outro lado, gerir os impactos das tecnologias. Concluímos que as visões políticas expressam imaginários europeus de que a incorporação do *Big Data* e das tecnologias no combate ao crime auxiliará a investigação criminal. Esta análise permitiu mapear tendências europeias de "processos de governança" e identificar os imaginários sociotécnicos subjacentes que projetam e constroem simbolicamente "necessidades europeias" de riscos e benefícios em contextos de sociedades securitárias. Por fim, face aos dilemas ético-legais, sociais e políticos analisados, equacionamos pistas para o futuro da regulamentação de *Big Data* na investigação criminal.

Palavras-chave: *Big Data*, investigação criminal, imaginário europeu, enquadramento legal.

Introdução

Nos últimos anos constata-se um desenvolvimento das novas tecnologias ao serviço do policiamento e da investigação criminal, na procura de novas estratégias de combate ao crime. Neste contexto, a tecnologia de *Big Data*[4] tem assumido crescente visibilidade sobretudo em termos de projeção

[4] Neste texto o *Big Data* é concebido enquanto "tecnologia" ao invés de "técnica", na medida em que, tratando-se de uma reflexão inspirada nos Estudos Sociais da Ciência e Tecnologia perceciona o *Big Data* não apenas como uma técnica (um sistema objetivo, por exemplo, um software de informática que cumpre determinada finalidade num contexto particular), mas como uma tecnologia que reflete o conjunto de conhecimentos em torno das técnicas que engloba, as suas práticas de manuseamento e as interpretações, expectativas e sentidos que lhe são conferidos (Chan & Moses, 2017).

do futuro do policiamento (Babuta, 2017; Neiva, 2020). *Big Data* caracteriza-se como um conjunto de técnicas que, através do cruzamento de informações policiais e outras bases de dados, calcula indicadores numéricos, visando definir estratégias de prevenção e combate criminal (Brayne, 2017). Atualmente verifica-se a sua crescente proliferação em várias esferas do sistema de justiça criminal, dado que a sua utilidade tem vindo a ser socialmente construída e projetada enquanto ferramenta que pode apoiar decisões sobre rumos e estratégias de investigação criminal (Drewer & Miladinova, 2017). São prementes expetativas relativamente ao seu potencial para previsões criminais (Joh, 2014; Miró-Llinares, 2020; Moses & Chan, 2018; Shapiro, 2019), alocação eficiente de recursos policiais (Hu, 2019; Joh, 2016; Kubler, 2017; Ridgeway, 2018) e tomada de decisões de justiça mais céleres (Brayne, 2017; Hu, 2019; Joh, 2014, 2016). No entanto, constata-se o surgimento crescente de literatura académica que acentua que a tecnologia de *Big Data* pode potenciar a expansão da vigilância massiva (Coll, 2014; Lyon, 2014) e, deste modo, contribuir para ameaçar direitos civis, liberdades e garantias fundamentais (Babuta, 2017; Lei, 2019).

Partindo do conceito de "imaginários sociotécnicos" proposto por Jasanoff e Kim (2009) entendido como "formas coletivamente imaginadas da vida e ordem social que se refletem na conceção e na realização de projetos tecnológicos ou de inovação científica" (Jasanoff & Kim, 2009, p. 120), visamos explorar os valores, sentidos e expectativas em torno de *Big Data* na investigação criminal no contexto da regulação da União Europeia. Concretamente, procedemos a uma análise do Regulamento Geral da Proteção de Dados da União Europeia 2016/679 (RGPD) e da Diretiva Europeia 2016/680 sobre o tratamento de dados pessoais na prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções. Esta análise é enquadrada e complementada com uma abordagem de discursos da Comissão Europeia. A recolha dos documentos foi *online*, dado o seu acesso público nos *sites* do Conselho Europeu[5].

Concebemos os textos regulatórios e os discursos políticos como intrinsecamente implicados em visões coletivas reveladoras de interconexões entre tecnologia, cultura e política (Jasanoff & Kim, 2009). O objetivo é compreender como os dados e o *Big Data* são retratados nestes discursos e documentos, o modo como são projetados os compromissos políticos, sociais e éticos em relação ao *Big Data*, novas tecnologias e proteção de dados na legislação e discursos europeus sobre a investigação criminal, que noções de bem público e de cidadania emergem e como se conjugam princípios aparentemente contraditórios, como o da garantia da segurança e o da promoção da cidadania. Através da "análise dos argumentos" (Crawford,

[5] Os documentos podem ser acedidos por via dos *links* seguintes: http://data.europa.eu/eli/reg/2016/679/oj, http://data.europa.eu/eli/dir/2016/680/oj, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjBxMnD1bLvAhXKNcAKHQZBD-MQFjAAegQIARAD&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fjust%2Fdocument.cfm%3Fdoc_id%3D41689&usg=AOvVaw3I1vzt355KPbeP61JT9TLw, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjMuvOD1rLvAhXMiVwKHSONDysQFjAAegQIAxAD&url=http%3A%2F%2Fpublications.europa.eu%2Fresource%2Fgenpub%2FPUB_DS0216739PTN.1.1&usg=AOvVaw3nYjWxHv5eAWA9YsPFG9zK

2004, p. 23) almejou-se compreender o modo como a cultura política democrática na Diretiva 2016/680, no RGPD e nos discursos da Comissão Europeia enquadram os objetivos, riscos e benefícios da inovação tecnológica no contexto da investigação criminal. Esta escolha metodológica (Crawford, 2004) possibilitou compreender as crenças, os fatores políticos e o poder de persuasão dos argumentos legais. Esta análise debruçou-se sobre os conceitos (não) presentes nos documentos, os apelos feitos em torno do novo arsenal legal e as crenças normativas. Este método permitiu a análise do desenvolvimento e evolução de argumentos legais, do modo como se (re)configuram, como produzem efeitos sociais e o progresso dos recursos em torno do fenómeno-tema em estudo (Crawford, 2004).

Pretendemos responder às seguintes questões de investigação: i) De que modo os dados e o *Big Data* são retratados na legislação?; ii) Que compromissos políticos, sociais e éticos em relação ao *Big Data*, novas tecnologias e proteção de dados são revelados na legislação europeia sobre a investigação criminal? iii) Que noções de bem público e de cidadania emergem neste contexto? e iv) Como se conjugam, na legislação, princípios potencialmente contraditórios entre segurança (proteção contra o crime) e cidadania (respeito pela dignidade humana e privacidade)? Esta análise é o ponto de partida para mapear tendências europeias de "processos de governança" e de negociação de criação, e de fluxos de dados como procedimentos formalmente determinados em políticas e procedimentos que controlam como os dados são geridos e acedidos, por quem, como, e com que finalidades (Mourby *et al.*, 2018, p. 232). Por outro lado, a um nível interpretativo e compreensivo, identificamos os imaginários sociotécnicos subjacentes que projetam e constroem simbolicamente "necessidades europeias" de riscos e benefícios em contextos de sociedades securitárias (Jasanoff & Kim, 2009). Por fim, face a estes dilemas ético-legais, sociais e políticos, equacionamos pistas para o futuro da regulamentação de *Big Data* na investigação criminal.

Enquadramento do *Big Data* na investigação criminal

Com a crescente produção de dados digitais, o *Big Data* possibilita a extração de conhecimento destas informações. Caracteriza-se por ser uma tecnologia que, através da recolha, análise e processamento de informação diversas, calcula índices para aferir de relações entre variáveis, com o objetivo de auxiliar tomadas de decisão. O *Big Data* tem-se tornado parte integrante de um ecossistema de dados que oferece, cada vez mais, possibilidades para integrar novos e diferentes dados. Consequentemente, instiga novas questões acerca da forma como a sociedade, as instituições e cidadãos processam estes dados e estas informações (Cukier & Mayer-Schoenberger, 2013). Estas reflexões estendem-se ao campo da justiça criminal que, nos últimos anos, tem projetado a aplicação do *Big Data*, sustentando-se na construção social de que a tecnologia possibilita tomadas de decisões de justiça mais céleres, eficazes e eficientes. Discursos governamentais, a um nível global, enfatizam a utilidade da tecnologia, com argumentos centrados nas suas capacidades para desenvolver estratégias eficazes para garantir a segurança (Chan & Moses, 2017; Cukier & Mayer-Schoenberger, 2013).

Simultaneamente, Departamentos Policiais em contexto internacional (Brayne, 2017; Joh, 2014; Lei, 2019) e europeu (Drewer & Miladinova, 2017; Kubler, 2017; Pereira, 2019) têm aplicado o *Big Data* por via da agregação de sistemas e bases de dados policiais, pela possibilidade de combinação de dados diferentes (Brayne, 2018), da digitalização de informações criminais e a crescente partilha de informações entre Departamentos (Brayne, 2017; Joh, 2014). Paralelamente a esta expansão futurista do *Big Data* no policiamento (Babuta, 2017; Brayne, 2017; Joh, 2014) e das crenças políticas mitológicas generalizadas (Boyd & Crawford, 2012; Cukier & Mayer-Schoenberger, 2013) em torno da utilidade da técnica, assiste-se a uma consciencialização pública da proliferação crescente de bases de dados e informações pessoais disponíveis em várias plataformas como internet e dispositivos móveis, acoplada com a perceção de que estes desenvolvimentos possibilitam a utilização destas informações para fins não previstos ou não consentidos pelos seus dadores a um nível global (Gonçalves, 2017), desafiando os pressupostos democráticos europeus e dos Estados-nação. Esta conceção pública denota a necessidade de desenvolver modelos de governança responsáveis em torno da tecnologia (Mourby *et al.*, 2018), esclarecedores quanto ao modo como se processa, desde o acesso aos dados, aos resultados que produz e às interpretações que lhe são conferidas. A securitização crescente das sociedades contemporâneas e as atuais tendências abusivas de vigilância dos cidadãos (Coll, 2014; Lyon, 2014), através de, por exemplo, recentes possibilidades das autoridades policiais terem acesso a metadados telefónicos, têm suscitado receios de que o *Big Data* potencie a fragilização de princípios fundamentais das sociedades democráticas, como os de transparência e prestação pública de contas, que exigem a (re)formulação de regras éticas, legais e sociais.

Face a estas ansiedades públicas, constata-se a construção de um discurso político, a um nível geral, centrado na proteção de direitos, garantias e liberdades dos cidadãos (Cukier & Mayer-Schoenberger, 2013; Mann & Matzner, 2019; Mantelero, 2017; McDermott, 2017; Gonçalves, 2017), por via da criação de documentos legais que reforcem as garantias protetivas dos direitos humanos (Gonçalves, 2017; Mantelero, 2017), como o RGPD (2016/679) e a Diretiva (2016/680). Simultaneamente, verifica-se a proliferação de discursos (Comissão Europeia, 2016a, 2016b) que enquadram, sustentando, esta legislação como uma garantia que deve reforçar a confiança coletiva nas tecnologias e nas instituições de controlo. Estes documentos e discursos são concebidos como recursos culturais poderosos que moldam as respostas sociais à inovação, revelando os interesses políticos dos autores, concebidos como autoridades integrantes do governo com "monopólio efetivo sobre os regimes dos dados" (Ruppert *et al.*, 2017, p. 3). Como analisaremos, estas visões políticas expressam imaginários de que a incorporação do *Big Data* e das tecnologias no combate ao crime produzirá efeitos positivos na sua resolução, auxiliando a investigação criminal.

O *Big Data* não é uma realidade nova, o que é inovador e foco de análise neste texto é o modo como a sua expansão na investigação criminal se processa e é projetada do ponto de vista dos discursos

políticos e da legislação, bem como, os limites da sua aplicação. Pretendemos analisar estes dois últimos aspetos dado que, face às atuais controvérsias em torno das suas fragilidades na investigação criminal, nomeadamente, ao nível dos falsos positivos (Ferguson, 2015), correlações erradas (Hu, 2018; Joh, 2016) e má qualidade dos dados (Lei, 2019), é crucial compreender o modo como a política e os legisladores projetam o *Big Data* e regulamentam a sua utilização.

"Imaginário Europeu"

O modo como os imaginários europeus emergem na Diretiva 2016/680, no RGPD 2016/679 e nos discursos da Comissão Europeia (2016a, 2016b) em torno das novas tecnologias e da proteção de dados na investigação criminal, a forma como descrevem e anteveem os seus riscos, ajuda a compreender as perspetivas futuras da sua governança. Tendo como foco os riscos e benefícios apresentados nestes discursos políticos e o modo como estas tecnologias têm vindo a ser adotadas, é possível compreender a sua relevância política pública. Ambos os documentos e discursos foram enquadrados como uma resposta necessária face à inevitabilidade do progresso tecnológico, objetivando responder à necessidade de inovação dos meios securitários, para dar resposta às inseguranças, medos e riscos contemporâneos na Europa.

Os discursos da Comissão Europeia

A Comissão Europeia, aquando da publicação da Diretiva 2016/680 e do Regulamento Geral da Proteção de Dados 2016/679, pronunciou-se, esclarecendo o novo arsenal legislativo face à expansão da partilha de dados num contexto de desenvolvimento tecnológico sem precedentes nas diversas áreas. No âmbito da investigação criminal, visou-se reforçar a importância de assegurar as garantias protetivas dos direitos humanos, face à imersão do policiamento e repressão criminal num mundo tecnológico e mediado digitalmente. Consequentemente, face à publicação dos dois documentos legais, a Comissão Europeia (2016a, 2016b) referiu que dado o progresso das tecnologias digitais e considerando os seus benefícios na investigação criminal, elaborou recomendações que visam proteger as garantias fundamentais potencialmente lesadas nestes contextos.

Assim, descreve ambos os documentos legais como soberanos quanto ao regime de proteção de dados pessoais que preveem, projetando-os como elementos cruciais para a construção de uma Europa com um panorama protetivo de direitos humanos sólido e coerente (Comissão Europeia, 2016b). Referindo que os dispositivos tecnológicos e o *Big Data* se afiguram como essenciais para a execução da investigação criminal, devem ser utilizados por garantirem a segurança transfronteiras, projetando uma imagem social das tecnologias como promotoras da segurança (Comissão Europeia, 2016a). Face aos riscos inerentes e emergentes destas tecnologias, a Comissão Europeia vem reforçar a conceção de que foram criadas regras explícitas e concretas que procuram administrar estes impactos, minimizando-os. Nomeadamente, refere

que o RGPD (2016/679) e a Diretiva (2016/680) "permitirão partilhar tais dados de forma mais eficaz tanto a nível da União Europeia como a nível internacional, (...) [e] reforçarão a confiança e garantirão a segurança jurídica transfronteiras" (Comissão Europeia, 2016b).

Desta forma, este enquadramento e sustentações discursivas face à implementação de um novo regime legal de proteção de dados no contexto da investigação criminal possibilita compreender o modo como a fluidez das controvérsias em torno da projeção das novas tecnologias como recursos úteis na manutenção da ordem social, mas, simultaneamente, como possivelmente impactantes na esfera dos direitos humanos, emergem e são comunicadas. Os discursos da Comissão Europeia (2016a, 2016b) salientam o modo como as entidades políticas concebem os riscos e os benefícios da tecnologia enquadrados no contexto securitário europeu, exacerbando a perceção política das vantagens do *Big Data* na investigação criminal, face à neutralização dos seus impactos, projetando expectativas promissoras quanto à sua aplicação.

De uma forma geral, esta previsão legal é enquadrada sob argumentos semelhantes de outras tecnologias de combate ao crime, projetando fundamentos da sua aplicação para a contribuição de um espaço europeu que promova e defenda a liberdade, segurança e justiça (Bigo, 2008). Consequentemente, é possível compreender o modo como as políticas europeias apoiam e preveem o desenvolvimento do *Big Data*, que exigirá a mobilização de recursos materiais e organizacionais estatais, mas também, recursos do imaginário que permitem relacionar este tipo de políticas ao bem comum dos cidadãos (Jasanoff & Kim, 2009, p. 141). Por exemplo, neste caso, garantir a segurança nacional e a redução das taxas de crime, socorrendo-se do progresso tecnológico para aprimorar a investigação criminal.

A Diretiva 2016/680 e o Regulamento Geral da Proteção de Dados 2016/679

Vários estudos têm apontado de que a Diretiva 2016/680 e o RGPD (2016/679) não dão respostas às atuais preocupações em torno do *Big Data* no geral (Gonçalves, 2017; Mann & Matzner, 2019; Mantelero, 2017; McDermott, 2017) e na investigação criminal (Babuta, 2017; Neiva, 2020), desde logo porque não se referem à técnica. Embora utilizem conceitos como "tratamento automatizado", "meios automatizados" e "decisões automatizadas" (a título de exemplo, artigo 2.º, n.º2, Diretiva 2016/680), não preveem especificamente o *Big Data*. No entanto, a definição de Big Data está implicitamente incluída na previsão de "tratamento" e "definição de perfis" do artigo 3.º, n.º2 e 4 da Diretiva 2016/680 e artigo 4.º, n.º2 e 4 do RGPD como "uma operação ou um conjunto de operações efetuadas sobre [conjuntos de] dados pessoais, por meios [não] automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão (...)" e "tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos

relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações". Os "dados pessoais" versam sobre a informação que é manuseada pelo *Big Data* (artigo 3.º, n. º1 Diretiva 2016/680 e artigo 4.º, n. º1 do RGPD): "(...) um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social (...)".

O *Big Data* deve ser entendido, para efeitos da Diretiva 2016/680 e do RGPD (2016/679), como um conjunto de técnicas que possibilita o cruzamento entre (conjuntos de) dados pessoais, por meios automatizados de recolha, acesso, manuseamento e partilha de informações. Dada a inexistência de outros documentos regulatórios em torno do tema, estes são considerados como norteadores da aplicação do *Big Data*. No entanto, o RGPD (2016/679) refere não se aplicar ao processamento de dados para fins de aplicação da lei[6], excluindo do seu âmbito de aplicação a proteção de dados nas atividades de segurança nacional (Samuel *et al.*, 2018, p. e20). Para esse fim, foi criada a Diretiva 2016/680 que prevê a proteção dos dados na investigação criminal.

A "rápida evolução tecnológica" referida pela Diretiva (2016/680) como mola propulsora para a sua criação permite compreender o modo como a expansão das bases de dados e tecnologias no policiamento materializam a aplicação da ciência e da tecnologia nos objetivos securitários (Jasanoff & Kim, 2009), denotando a necessidade de modernização e adaptação aos novos desenvolvimentos que sustenta o apoio às novas tecnologias. Numa primeira fase, através da construção de instrumentos legais europeus, referindo que é necessário o seu desenvolvimento, sustentados em argumentos que enfatizam o bem público, a ordem social e a segurança (Levenda *et al.*, 2018). Neste contexto, a Diretiva 2016/680 vem facilitar a adoção do *Big Data* na Europa, na medida em que visa reforçar a confiança pública e cidadã nas tecnologias (Gonçalves, 2017), projetando o interesse em permeabilizar estas tecnologias à investigação criminal, reforçando a proteção e minimização dos seus riscos, através do estabelecimento de regras legais para a sua execução. Em segundo lugar, os objetivos da Diretiva 2016/680 projetam a conceção de uma "cultura política sociotécnica única" (Kim, 2018, p. 177), na medida em que promovem ideais de segurança e justiça no contexto atual inevitável de partilha de dados. Este tipo de discurso político constrói imaginários acerca do potencial das novas tecnologias, apresenta normas legais e regulatórias que as aprovam, tendo consequências na sua expansão (Ruppert *et al.*, 2017). Simultaneamente, tem repercussões ao nível das perceções sociais coletivas acerca das tecnologias, do seu investimento económico e da adesão comunitária (Jasanoff & Kim, 2009). Nas suas considerações introdutórias, a Diretiva 2016/680 refere que a utilização de tecnologias "permite o tratamento de dados pessoais para o

[6] "O presente Regulamento não se aplica ao tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" (RGPD, artigo 2.º, n.º2, alínea d).

exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais e execução de sanções penais", projetando a crença mitológica generalizada (Boyd & Crawford, 2012) em torno das tecnologias como ferramentas que agilizam a investigação criminal.

Outra característica da imaginação sociotécnica europeia em torno do *Big Data* é que as suas potencialidades são descritas como ilimitadas, enquanto que os seus riscos são retratados como limitados. Os seus benefícios são construídos como promotores da segurança e possibilitadores de tratamento de dados pessoais numa escala sem precedentes para a investigação criminal (Diretiva 2016/680). Por sua vez, os seus riscos são enquadrados como administráveis. Por exemplo, a referência na Diretiva (2016/680) da raça como um dado sensível, a proibição expressa da criação de perfis automatizados (artigo 11.º) que possam ser discriminatórios e a obrigatoriedade de proceder a uma avaliação de impacto sobre a proteção de dados (artigo 27.º) caso um tipo de tratamento se afigure de "(...) elevado risco para os direitos e liberdades (...)" com recurso a autoridades de controlo, são argumentos que procuram salvaguardar as já conhecidas fragilidades do sistema de justiça (Brayne, 2017; Lyon, 2014; Skinner, 2013, 2018a, 2018b), almejando reforçar a confiança coletiva nas instituições de controlo para responder a estas questões emergentes. A Diretiva (2016/680) refere que as suas normas legais contribuem "para a realização de um espaço de liberdade, segurança e justiça" regulamentando a proteção de dados no âmbito da partilha de informações através da tecnologia que "permite o tratamento [destes dados] numa escala sem precedentes para o exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais (...)". É possível analisar como é que estas controvérsias fluídas que surgem em torno de, por um lado, definir padrões de segurança e, por outro lado, gerir os riscos associados às tecnologias são temporariamente resolvidas. Além disso, o modo como são percecionados os riscos e os benefícios das novas tecnologias nestes contextos.

Portanto, ainda que se edifiquem pensamentos coletivos (Jasanoff & Kim, 2009, p. 123) que defendem que há uma ameaça aos direitos humanos e riscos para a ética nestes contextos (Babuta, 2017; Ferguson, 2015; Joh, 2014, 2016; Lei, 2019; Neiva, 2020), as respostas legais, na figura da Diretiva 2016/680, constroem uma paisagem argumentativa de que estes danos para os direitos humanos não foram ignorados. Mas foram interpretados e compreendidos através das lentes da aspiração europeia (Jasanoff *et al.,* 2007) em torno da perceção tecnológica como útil na investigação criminal e apoiado pela aplicação rigorosa das suas regras (Diretiva 2016/680). A Diretiva 2016/680 agrega modos de responder aos potenciais riscos que as tecnologias apresentam (Jasanoff & Kim, 2009), tornando-se uma forma de garantir o futuro técnico da segurança europeia. A análise do modo como os potenciais riscos da permeabilização das novas tecnologias no contexto da investigação criminal podem ser administráveis permite compreender como é que os imaginários sociotécnicos são um meio pelo qual o discurso legal antecipatório e as práticas são estruturados e, portanto, um mecanismo através do qual os futuros são projetados (Pickersgill, 2011). Estes imaginários sociotécnicos europeus em torno do *Big Data* na

investigação criminal estão a incorporar-se em práticas institucionais. Alguns Departamentos Policiais na Europa já começaram a adotar o *Big Data*, por exemplo em França (Kubler, 2017), em Portugal (Pereira, 2019) e a um nível macro, a Europol (Drewer & Miladinova, 2017).

Orientações para o futuro

Embora estes imaginários sociotécnicos tenham estas repercussões práticas, há pontos específicos em que a Diretiva (2016/680) instiga debates e desafios atuais. Nomeadamente, quanto ao acesso aos dados por parte do titular, a Diretiva segue as regras dos processos judiciais, podendo este direito ser negado caso se afigure necessária a preservação confidencial dos dados (artigo 15.º), não havendo regras claras sobre a preservação deste direito. Também no que diz respeito à transferência de dados sobre infrações graves, é concedida uma maior flexibilidade de acesso aos dados por outros países, não sendo claras as restrições de acesso e tendo repercussões ao nível do princípio do consentimento e dos limites das bases de dados.

Relativamente ao consentimento, a Diretiva 2016/680 não prevê normas para o seu exercício, referindo que o "consentimento do titular dos dados (...) não deverá constituir a fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. Caso haja uma obrigação legal, o titular dos dados não tem verdadeira liberdade de escolha (...)", não prevendo a aplicação deste direito. Por sua vez, também não considera a possibilidade de acesso policial a outros tipos de informações como, por exemplo, dados de entidades comerciais, e isso levanta desafios éticos, ao nível da privacidade e da transparência que não estão enquadradas neste documento legal. Também no que diz respeito aos impactos negativos do *Big Data* ao nível da discriminação, por se basear em dados que podem estar sobre representados nas bases de dados[7] que pode perpetuar a criminalização de comunidades suspeitas sob escopo do sistema de justiça criminal (Brayne, 2017; Skinner, 2013, 2018a, 2018b), não são apresentadas respostas claras. As fragilidades técnicas do *Big Data* como a obtenção de correlações erradas fruto da análise de grandes volumes de dados diversos que podem perturbar as investigações criminais (Hu, 2018; Joh, 2016), por gerarem falsos positivos (Ferguson, 2015) e por se basear em dados potencialmente enviesados (Lei, 2019) também não estão previstas nestes documentos. Portanto, a Diretiva 2016/680 para a investigação criminal, à semelhança da reflexão de Gonçalves (2017, p. 107) sobre o RGPD (2016/679) a um nível geral, "não fornece os cuidados que seriam esperados de uma lei destinada a proteger um direito fundamental" (Gonçalves, 2017, pp. 114-115).

Atendendo a que habitualmente as Diretrizes têm um pendor geral e, posteriormente, são complementadas com outras orientações, concluímos que a Diretiva serve o propósito de construir um espaço legal que regulamente a proteção de dados no setor específico da investigação criminal. Esta

[7] Como minorias étnicas e grupos vulneráveis do ponto de vista social e económico.

previsão legal vem facilitar o desenvolvimento das tecnologias na investigação criminal na Europa, liberalizando situações impactantes nos direitos humanos, delegando competências para serem avaliadas e minimizadas. No entanto, não considera as instigações emergentes. O contexto atual requer uma análise peculiar que tome em consideração os diferentes desafios que o *Big Data* instiga neste campo. O Comité (artigo 51.º Diretiva 2016/680) responsável pela avaliação dos impactos das tecnologias na proteção de dados, deve identificar e prever valores éticos específicos a serem salvaguardados no uso e tratamento dos dados, fornecendo orientações que sejam claras e detalhadas a cada contexto, para minimização destes riscos. Estas entidades devem supervisionar as atividades de *Big Data* na investigação criminal de forma a assegurar de que se processam de acordo com limites legais.

Notas conclusivas

A presente abordagem compreensiva e interpretativa em torno da regulamentação legal do *Big Data* no contexto da partilha de dados para investigação criminal permitiu explorar de que forma foram projetadas as bases da cooperação e governança neste campo. Além disso, compreender os recursos concetuais utilizados na projeção destas tecnologias que podem melhorar a sua análise e implementação ao nível da avaliação dos seus riscos e benefícios.

O discurso europeu enquadrou o *Big Data* como desenvolvimento tecnológico inevitável no contexto da investigação criminal, caracterizando-o como útil na prevenção, investigação e repressão do crime. Consequentemente, projeta-o como ferramenta que melhora a segurança europeia. Um exemplo da ambição política europeia para o desenvolvimento deste projeto tecnocientífico (Jasanoff *et al.*, 2007) nestes contextos é a criação da Diretiva analisada no presente texto. A sua criação resulta da vontade política de garantir a proteção de dados pessoais na investigação criminal, face ao uso destas tecnologias neste setor. Esta vontade política reflete o poder que as entidades governamentais têm sobre os dados e a influência para definir o seu valor (Ruppert *et al.*, 2017). Por outras palavras, reforçando a proteção dos dados pessoais dos cidadãos e de outros direitos, liberdades e garantias, a Diretiva vem facilitar a expansão destas tecnologias na investigação criminal, assemelhando-se a uma salvaguarda geral que permite a sua aplicação, ao mesmo tempo que minimiza os potenciais danos da sua implementação, projetando as visões futuristas coletivamente partilhadas onde o poder da tecnologia se mobiliza para manter a segurança pública.

Neste texto foi possível compreender de que forma é que estes discursos legais antecipatórios são estruturados por imaginários sociotécnicos. No entanto, o empreendimento em torno do *Big Data* envolve-se em discussões controversas de importância social que precisam de ser informadas pelas visões de *stakeholders*[8] mas também dos sujeitos, para abordar os possíveis impactos negativos do *Big Data* (Micheli

[8] Consideramos a definição de Micheli *et al.* (2020, p. 5) de *stakeholders* como "indivíduos, instituições, organizações ou grupos que são afetados, ou têm efeito no modo como os dados são governados e no valor que lhes é conferido".

et al., 2020). Os documentos e discursos legais concentram-se na segurança e na qualidade dos dados, não se focando diretamente nas questões sociais e éticas do uso desses dados. Ou seja, não existe um modelo que avalie os resultados negativos desses processos que afetam os cidadãos e a sociedade.

Os potenciais danos do uso do *Big Data* não se limitam apenas à privacidade, ao consentimento e à proteção de dados, mas estendem-se a outros preconceitos sociais, como a discriminação, o viés algorítmico e a vigilância total (Brayne, 2017; Ferguson, 2015; Joh, 2016; Lyon, 2014). Portanto, os riscos abrangidos pelos documentos legais devem estender-se a uma avaliação mais complexa do processamento dos dados que abarque estes impactos. A ausência desta perspetiva ética no RGPD 2016/679 e na Diretiva 2016/680 levanta questões sobre que valores norteiam a futura sociedade algorítmica. Seria importante que, com foco numa dimensão coletiva, a formulação de documentos legais englobasse diferentes atores sociais que podem desempenhar um papel importante na avaliação destes impactos. Este conjunto de atores pode auxiliar a democratização da governança dos dados do *Big Data* e reavaliar o valor que é produzido em torno das informações que agrega (Micheli *et al.*, 2020). Sugerimos, portanto, que haja um maior envolvimento público no debate acerca da temática, que definam controlos externos para a supervisão da sua aplicação, que permitam que os riscos do *Big Data* sejam compreendidos e se produzam métodos e práticas transparentes para os minimizar. Consideramos que estes impactos negativos podem ser minimizados através da elaboração de recomendações que resultem de deliberações com diferentes *stakeholders* e que se orientem por princípios de transparência e envolvimento dos cidadãos (Chan & Moses, 2017; Gonçalves, 2017; Mantelero, 2017).

A rápida evolução tecnológica exige novas formas de refletir as instituições, a sociedade, a democracia e os seus valores fundamentais. Por mais sedutora que possa ser a imagem social e política do *Big Data* na previsão e repressão do crime, esta mitologia não deve cegar as políticas quanto às suas imperfeições inerentes, os seus riscos e viés. Portanto, estas últimas, nas suas formulações devem incluir não só considerações acerca das suas potencialidades, mas também das suas limitações, ameaças e novos desafios éticos que emergem para construir modelos de governança de minimização dos seus erros e imprecisões. Além disso, a Diretiva 2016/680 prevê recomendações para que os Estados-Membros elaborem garantias de proteção de direitos e liberdades. É um encorajamento para que, por exemplo, na investigação criminal se criem regulamentos com normas internas e institucionais que assegurem uma maior proteção dos dados pessoais recolhidos.

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]); e da Fundação para a Ciência e Tecnologia [referência de bolsa 2020.04764.BD].

Bibliografia

Babuta, A. (2017). *Big data and policing: an assessment of law enforcement requirements, expectations and priorities*. Royal United Services Institute for Defence and Security Studies, 1-41.

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). Ashgate.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662-679. https://doi.org/10.1080/1369118X.2012.678878

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977-1008. https://doi.org/10.1177%2F0003122417725865

Brayne, S. (2018). The criminal law and law enforcement implications of big data. *Annual Review of Law and Social Science*, *14*, 293-308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839

Chan, J., & Moses, L. (2017). Making sense of big data for security. *The British Journal of Criminology*, *57*(2), 299-319. https://doi.org/10.1093/bjc/azw059

Comissão Europeia (janeiro, 2016a). A Reforma da UE sobre a Proteção de Dados e os Megadados. Ficha informativa. Direção-Geral da Justiça e dos Consumidores.

Comissão Europeia (janeiro, 2016b). De que modo a reforma da proteção de dados ajudará a combater a criminalidade internacional? Ficha informativa. Direção-Geral da Justiça e dos Consumidores.

Coll, S. (2014). Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance. *Information, Communication & Society, 17*(10), 1250-1263. https://doi.org/10.1080/1369118X.2014.918636

Crawford, N. C. (2004). Understanding discourse: a method of ethical argument analysis. *Qualitative Methods*, *2*(1), 22-25.

Cukier, K., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, *92*, 28-40.

Diretiva da União Europeia de 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680

Drewer, D., & Miladinova, V. (2017). The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation. *Computer Law & Security Review*, *33*(3), 298-308. https://doi.org/10.1016/j.clsr.2017.03.006

Ferguson, A. (2015). Big data and predictive reasonable suspicion. University of Pennsylvania Law Review, 163(2), 327-410.

Gonçalves, M. E. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. *Information & Communications Technology Law*, *26*(2), 90-115. https://doi.org/10.1080/13600834.2017.1295838

Hu, J. (2018, November). Big data analysis of criminal investigations. In *2018 5th International Conference on Systems and Informatics (ICSAI)* (pp. 649-654). IEEE. https://doi.org/10.1109/ICSAI.2018.8599305

Hu, Y. (2019, April). Intelligent Procuratorate Depends on Big Data Investigation Technology. In *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 20-23). IEEE. https://doi.org/10.1109/ICCCBDA.2019.8725723

Jasanoff, S., & Kim, S. H. (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., Kim, S. H., & Sperling, S. (2007). Sociotechnical imaginaries and science and technology policy: a cross-national comparison. *NSF Research Project, Harvard University*.

Joh, E. E. (2014). Policing by numbers: big data and the Fourth Amendment. *Washington Law Review*, *89*, 35-68.

Joh, E. E. (2016). The new surveillance discretion: automated suspicion, big data, and policing. *Harvard Law & Policy Review*, *10*, 15-42.

Kim, E.-S. (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

Kubler, K. (2017). State of urgency: Surveillance, power, and algorithms in France's state of emergency. *Big Data & Society*, *4*(2), 1-10. https://doi.org/10.1177%2F2053951717736338

Levenda, A. M., Richter, J., Miller, T., & Fisher, E. (2018). Regional sociotechnical imaginaries and the governance of energy innovations. *Futures, 109,* 181-191. https://doi.org/10.1016/j.futures.2018.03.001

Lei, C. (2019). Legal control over Big Data criminal investigation. *Social Sciences in China*, *40*(3), 189-204. https://doi.org/10.1080/02529203.2019.1639963

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1-13. https://doi.org/10.1177%2F2053951714541861

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, *6*(2), 1-11. https://doi.org/10.1177%2F2053951719895805

Mantelero, A. (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer law & security review*, *33*(5), 584-602. https://doi.org/10.1016/j.clsr.2017.05.011

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, *4*(1), 1-7. https://doi.org/10.1177%2F2053951716686994

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 1-15. https://doi.org/10.1177%2F2053951720948087

Miró-Llinares, F. (2020). Predictive policing: Utopia or dystopia? On attitudes towards the use of big data algorithms for law enforcement. *SocArXiv.* 1-28.

Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and society*, *28*(7), 806-822. https://doi.org/10.1080/10439463.2016.1253695

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, *34*(2), 222-233. https://doi.org/10.1016/j.clsr.2018.01.002

Neiva, L. (2020). *Big Data na investigação criminal: desafios e expectativas na União Europeia.* Editora Húmus.

Pereira, M. (2019). *Big Data: o caso do sistema estratégico de informação, gestão e controlo operacional da Polícia de Segurança Pública* [Dissertação de Mestrado Integrado em Ciências Policiais, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa]. Repositório Comum. http://hdl.handle.net/10400.26/30342

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

Regulamento da União Europeia 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à 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 (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Ridgeway, G. (2018). Policing in the era of big data. *Annual Review of Criminology*, *1*, 401-419. https://doi.org/10.1146/annurev-criminol-062217-114209

Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. *Big data & Society*, *4*(2), 1-7. https://doi.org/10.1177%2F2053951717717749

Samuel, G., Howard, H. C., Cornel, M., van El, C., Hall, A., Forzano, F., & Prainsack, B. (2018). A response to the forensic genetics policy initiative's report "Establishing Best Practice for Forensic DNA Databases". *Forensic Science International: Genetics*, *36*, e19-e21. https://doi.org/10.1016/j.fsigen.2018.07.002

Shapiro, A. (2019). Predictive policing for reform? Indeterminacy and intervention in Big Data policing. *Surveillance & Society,* 17 (3/4), 456-472. https://doi.org/10.24908/ss.v17i3/4.10410

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%2F0038038513493539

Skinner, D. (2018a). Race, racism and identification in the era of technosecurity. *Science as Culture*, *29*(1), 77-99. https://doi.org/10.1080/09505431.2018.1523887

Skinner, D. (2018b). Forensic genetics and the prediction of race: what is the problem?. *BioSocieties*, *15,* 329-349. https://doi.org/10.1057/s41292-018-0141-0