

O direito à privacidade no tempo do big data: narrativas profissionais na União Europeia

RESUMO

Assiste-se hoje a um crescente debate em torno dos direitos humanos e do Big Data. Este artigo explora as expectativas de profissionais envolvidos na partilha transnacional de dados genéticos, geneticistas forenses e stakeholders de diferentes áreas relativamente à inclusão de Big Data na investigação criminal transnacional. Tendo por base uma metodologia qualitativa de análise de conteúdo de entrevistas, o objetivo é delinear os sentidos e aceder às significações que estes profissionais atribuem ao Big Data enquanto potencial técnica de investigação criminal, no âmbito das suas atividades profissionais. Apesar da promessa do potencial de Big Data em termos de eficácia e eficiência, a sua inclusão nos meios de investigação criminal impõe questões éticas e de direitos humanos que importam estudar. Conclui que os entrevistados referem a dificuldade de encontrar o equilíbrio entre a garantia dos direitos, liberdades e garantias dos indivíduos com a promoção da segurança pública; a ética da investigação criminal; e as violações ao direito à privacidade.

PALAVRAS-CHAVE: Big Data. Privacidade. Era digital. Direitos Humanos. Desafios.

Laura Neiva
b8214@ics.uminho.pt
Centro de Estudos de Comunicação
e Sociedade, Universidade do
Minho, Braga, Portugal.

INTRODUÇÃO

Os tempos contemporâneos caracterizam-se pela fluidez e mobilidade dos valores democráticos, que surgem com novas definições híbridas e maleáveis. Os direitos, liberdades e garantias individuais estão hoje no limbo do que é nosso e do que é de todos. A digitalização em massa dos aspetos sociais leva a que nos perguntemos: em que Era nos situamos? Quem somos nós neste palco digital? Que tipo de sociedade é que nós queremos? Conceitos como *data science*, *data mining* e *artificial intelligence* permeabilizam as nossas vidas e têm consequências no nosso cotidiano. Escândalos como o da *Cambridge Analytic*, as revelações de Edward Snowden, o surgimento da problematização e estudo das *fake news* revolucionaram o *modus operandi* dos nossos relacionamentos, abrindo leque para novos interesses técnico-científicos que redefinem as bases epistemológicas e deontológicas do conhecimento social.

Big Data se caracteriza pelo volume, variedade, formato e estrutura dos dados que manuseia e pela velocidade pela qual estes dados são processados e analisados (CHAN; MOSES, 2015; GANDY JR, 1989; KITCHIN, 2014; STEVENS; WEHRENS; DE BONT, 2018; YOUTIE; PORTER; HUANG, 2016; GONÇALVES, 2017). É uma técnica que coloca questões que obrigam as Ciências Sociais e Humanas a discutir e debater, para delinear ferramentas críticas que travem os efeitos do desenvolvimento tecnológico. É por isso que importa estudá-los, (re)pensá-los, debatê-los e colocá-los no epicentro do debate académico, social e político (NEIVA, 2019; BORGES; MACHADO, 2019). Existem estudos (SILVA; RODRIGUES, 2017; DIAS; VIEIRA, 2013; MEIRELES, 2016; FRANCO, 2018; YURI; REGINA, 2018; BRAYNE, 2017; CHAN; MOSES, 2017) que buscam avaliar a eficácia desta técnica em vários domínios e fazem revisões bibliográficas sobre o tema. Estes estudos, no Brasil, referem inúmeras controvérsias entre Big Data e o direito à privacidade, culminando num debate académico que reforça a necessidade de criar um novo arsenal legislativo que preveja o direito à privacidade na Era do Big Data. Contudo, não existem estudos que analisem discursos, carecendo este olhar prático sobre o fenómeno (SILVA; RODRIGUES, 2017; DIAS; VIEIRA, 2013; MEIRELES, 2016; FRANCO, 2018; YURI; REGINA, 2018).

Este artigo visa, além de combater esta lacuna científica, debater estas questões através da análise de entrevistas a 140 profissionais de cooperação transnacional europeia, geneticistas forenses, académicos, membros de companhias privadas, membros de organizações não governamentais e membros do corpo de investigação criminal, acerca do potencial de Big Data ao serviço da investigação criminal. É uma investigação inserida no Projeto EXCHANGE, que busca desmistificar, debatendo, algumas assimetrias provocadas por estes desequilíbrios. As questões que impulsionaram esta pesquisa foram: que expectativas em torno das potenciais aplicações de Big Data possuem os profissionais? Quais as suas percepções dos desafios ao direito à privacidade? O objetivo é aceder às visões que os profissionais possuem em torno do potencial de Big Data enquanto meio de investigação criminal transnacional, com foco nas questões de privacidade que apresentam. Estudar os diferentes olhares dos atores sociais sobre as tecnologias contribui para um entendimento da sua complexidade, potenciando reflexões éticas (LENZI, 2019). O artigo encontra-se dividido em cinco partes: na primeira apresenta uma contextualização teórica de Big Data, do direito à privacidade e dos desafios entre ambos. Posteriormente, apresenta o estudo empírico e as considerações metodológicas. Por fim, os resultados empíricos e as considerações finais.

BIG DATA - CONCETUALIZAÇÃO

Big Data pode ser perspectivado enquanto fenômeno cultural, tecnológico e acadêmico que funde tecnologia (exacerba o poder computacional e a precisão algorítmica), com análise (visa identificar regularidades entre conjuntos de dados) e mitologia (crença generalizada de que oferece maiores formas de inteligência e conhecimento) (CHAN; MOSES, 2015; BOYD; CRAWFORD, 2012). São conjuntos de dados recolhidos, analisados, substituídos por construções matemáticas, classificados numericamente e identificados por via de um índice para orientar decisões (GONÇALVES, 2017; CHAN; MOSES, 2017; LYON, 2014; DREWER; MILADINOVA, 2017; LEFÈVRE, 2017; MATZNER, 2016; WOOD; BALL, 2006). Esses dados vêm de diversas fontes: circuitos de câmeras de vigilância; localização geográfica; e/ou cedência de dados pessoais (LUPTON; MICHAEL, 2017; CHAN; MOSES, 2015; LYON, 2014). Big Data depende de *softwares* para coletar dados e informações pessoais que, em última instância, são estratégias de vigilância (LYON, 2014; HALFORD; SAVAGE, 2017). Isto significa que a vigilância automatizada se torna uma possibilidade crescente (GANDY JR, 1989; BOYD; CRAWFORD, 2012; FRADE, 2016; MATZNER, 2016). Potenciado pela sofisticação tecnológica, criou uma relação humano-algoritmo que modelou a forma como os cidadãos são abordados e identificados (LYON, 2014; WOOD; BALL, 2006). Por via de *softwares*, o comportamento humano é transformado em algoritmos e, sob um número, é reproduzido graficamente para ser codificado e analisado (MATZNER, 2016; WOOD; BALL, 2006; KUBLER, 2017; YURI; REGINA, 2018).

Contudo, este método levanta questões. Estudos das Ciências Sociais e Humanas em geral, e sobre a vigilância em específico, enfatizam as questões sociais e éticas de Big Data. Quanto à credibilidade dos dados e das conclusões: os dados que coleta são representativos? A conversão de informações pessoais em algoritmos produz correlações significativas? As ações que estes resultados orientam são mais eficazes (MATZNER, 2016; YURI; REGINA, 2018)? Desde que Big Data começou a estar no centro da agenda pública, que se discutem as repercussões negativas desta tecnociência (SKINNER, 2018; ARAÚJO, 2013), que dada a sua faceta tecnológica sofisticada, pode converter-se numa prática que sofre de desvirtuamento da função (FRÓIS, 2015). Assim, pode cumprir fins não previstos inicialmente, nocivos para a sociedade e seus cidadãos. Desta forma, as disputas e controvérsias em torno do Big Data enquanto ferramenta de vigilância invisível são inúmeras. Urge debater as repercussões ligadas à submersão humana nesta sociedade tecnológica e digital (TAYLOR, 2017; BOYD; CRAWFORD, 2012; WOOD; BALL, 2006) e as consequências ligadas a esta realidade. Apesar de existirem estudos que buscaram desmistificar tendências legislativas, por via da análise de documentos legais e que buscam dar resposta aos desafios ao direito à privacidade levantados pelo Big Data (DREWER; MILADINOVA, 2017; GONÇALVES, 2017; KUBLER, 2017; MANTELERO, 2017), existe um vazio científico no que toca à análise de discursos de atores profissionais que trabalhem no meio da partilha de dados. O presente artigo apresenta dados inovadores que têm por base a análise de narrativas sobre o potencial de Big Data e as consequências sociais (im)previstas da sua expansão (NEIVA, 2019).

DIREITO À PRIVACIDADE – DEFINIÇÕES

O desenvolvimento do Big Data foi conjugado com a redefinição dos riscos e segurança, que trouxeram um novo paradigma no arsenal dos direitos humanos (BORGES; MACHADO, 2019). Edward Snowden, analista de sistemas e ex-contratado da Agência Nacional de Segurança (ANS) nos Estados Unidos da América (EUA) foi um dos principais responsáveis por inaugurar o debate público acerca das invasões de privacidade que a coleta massiva de dados acarreta para os cidadãos (VAN DIJCK, 2014; YOUNG, 2017; ALBUQUERQUE; PEDRO, 2013). Em junho de 2013 expôs o maior programa de vigilância da história dos EUA (OBSERVADOR, 2019), alegando que a ANS usava aparelhos eletrônicos como celulares e computadores para ativar a localização geográfica dos indivíduos, acesse aos *websites* visitados pelos cidadãos, inserindo, posteriormente, estas informações nas suas bases de dados (LYON, 2014; WRIGHT; KREISSL, 2015). A coleta massiva de cerca de cinco bilhões de registros de celulares por parte da ANS, por dia, convertia-a numa entidade que detinha volumosos dados classificados em categorias como escutas, codificação, exploração, ferramentas de análise e bases de dados (VAN DER VLIST, 2017). Este acontecimento sociopolítico despoletou indignações e ansiedades (GUZIK, 2009), colocando em causa a panóplia de direitos, liberdades e garantias dos cidadãos (OBSERVADOR, 2019).

Estudos observacionais das Ciências Sociais e Humanas referem que, a partir deste momento, os indivíduos adotaram comportamentos contraditórios: tentavam precaver os efeitos negativos da tecnologia, ao mesmo tempo que respondiam aos avanços tecnológicos, legitimando-os e expandindo-os (BORGES; MACHADO, 2019). Este tipo de comportamento é definido por Norberg, Horne e Horne (2007) como o paradoxo da privacidade: o espaço que reside na diferença entre a informação que é cedida e a intenção que o indivíduo tinha ao cedê-la. A cedência de dados pessoais não pressupunha que houvesse uma autorização para que os dados fossem utilizados para outros fins. A violação da privacidade individual matura-se quando os dados, embora sejam doados de forma voluntária, são partilhados e analisados para outros fins que não os previstos inicialmente. Este facto é consequência do que Fróis (2015) definiu como o fenómeno de desvirtuamento da função: desenrolar de consequências (im)previstas no desenvolvimento tecnológico, que não foram equacionadas aquando da sua criação.

Consequentemente, o direito à privacidade começa a ser visto como o lesado na equação da coleta massiva de dados. Este direito prevê a reserva de informações pessoais e da própria vida pessoal. Data de 1948, a sua primeira consagração na Declaração Universal dos Direitos do Homem. No artigo 12.º pode ler-se que “ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei” (também consagrado na Convenção Europeia dos Direitos do Homem de 1950 e no Pacto Internacional relativo aos direitos civis e políticos de 1966). Recentemente, o direito à privacidade foi ratificado pela Carta dos Direitos Fundamentais da União Europeia, em 2000, onde o artigo 7.º determina que “todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações”. É um direito reconhecido internacionalmente, na União Europeia (UE) e encontra consagração nacional em quase todas as constituições modernas, sendo um direito legal (WESTIN, 2003). Em termos práticos, este direito sustenta-se na dignidade da pessoa humana, tal como na autonomia privada e no livre desenvolvimento da sua personalidade (GONÇALVES, 2003; WARREN; BRANDEIS, 1890; BORGES;

MACHADO, 2019). O direito à reserva da intimidade da vida privada, sob a ótica de Gomes Canotilho e Vital Moreira (2005), perspectiva-se de dois primas menores: o direito a proibir o acesso de estranhos a informações sobre a vida privada e o direito a que ninguém propague informações que tenha sobre a vida privada de outrem. A concepção de vida privada inclui o respeito dos comportamentos, do anonimato, da vida em relação e da liberdade de consciência, tendo como objetivo último a proteção da liberdade das pessoas. Ou seja, existe uma proibição legal de aceder a informações pessoais, bem como, propriedades individuais. Todos os indivíduos possuem as suas informações e qualquer acesso que seja feito a essas informações é considerada uma violação à integridade pessoal do indivíduo (BORGES; MACHADO, 2019). Este é o nível político da privacidade, quando os governos instituem legalmente o direito à privacidade, na promoção de sociedades democráticas e assentes na valorização dos direitos humanos (WESTIN, 2003). Nesta linha de reflexão, a privacidade é a capacidade individual de o indivíduo controlar a forma como os outros utilizam suas informações (WESTIN, 2015). Clarke (1999) acrescenta que a privacidade engloba o interesse individual em ter um espaço pessoal, livre de entrada de outras pessoas ou organizações. Ou seja, pressupõe essa vontade autónoma e definida de restringir o acesso a áreas da vida privada (BORGES; MACHADO, 2019). É direito individual delimitar, mediante suas opções, de que forma suas informações devem e podem ser cedidas. E não se trata de um desejo peculiar humano (WESTIN, 2015, p. 102), sendo antes uma necessidade universal que pode, muitas vezes, se tratar apenas da procura por um isolamento temporário ou curtos tempos de intimidade. É neste momento que a privacidade desempenha um papel muito importante na autonomia individual. Além disso, é muito importante também quando os indivíduos se protegem contra exposições públicas. Nesses momentos é uma oportunidade individual para buscar tomar decisões por via da reflexão, processamento de informação, avaliação e consideração de alternativas ou consequências. É uma forma de limitar e proteger a comunicação sem que outros tenham conhecimento de nossas conversações (WESTIN, 2015). Este é o nível pessoal da privacidade, quando cada indivíduo afirma sua liberdade na vida cotidiana (WESTIN, 2003). Todos os seres demandam privacidade e ela é um pilar para a construção de sociedades democráticas (WESTIN, 2015, p. 34). A privacidade não é apenas um mero direito, é uma função social que cumpre fins individuais e coletivos. Não é apenas a vontade em estar sozinho, mas antes coexiste na relação que o individual tem com o coletivo exterior, porque apesar dos cidadãos limitarem os acessos públicos à sua vida privada, eles também querem ter relação com o mundo exterior (WESTIN, 2015).

No entanto, este direito torna-se árduo de obedecer devido à automação própria da mineração, análise e reutilização de conjuntos de dados (PÚBLICO, 2018; YURI; REGINA, 2018). Uma reflexão acerca da privacidade no meio de uma sociedade da informação tecnológica é crucial, num momento em que os governos e as empresas privadas possuem enormes quantidades de dados sobre as pessoas (WESTIN, 2015). Big Data inaugura uma ampliação da vigilância governamental em diferentes configurações do domínio privado. Este fenómeno exacerba questões acerca da privacidade individual e exposição à vigilância no que concerne ao livre fluxo de dados que o indivíduo não pode controlar (BALL DI DOMENICO; NUNAN, 2016; COLL, 2014; BARTLETT; LEWIS; REYES-GARLINDO; STEPHENS, 2018). A evidência científica no Brasil (SILVA; RODRIGUES, 2017; DIAS; VIEIRA, 2013; MEIRELES, 2016; FRANCO, 2018; YURI; REGINA, 2018) refere a emergência de um debate académico centrado na necessidade de um alvoroço legislativo que garanta o respeito pela privacidade dos indivíduos. Investigações jurídicas referem que o rápido desenvolvimento do mundo tecnológico, por vezes, ocorre de forma mais rápida que a reação do mundo jurídico a essa propagação digital (FRANCO, 2018). No entanto, inexistentes são os estudos sobre a análise das narrativas de profissionais que operam em partilha transnacional de dados, acerca de Big Data. Assim, este artigo afirma-se como uma inovação no campo científico da temática.

BIG DATA E PRIVACIDADE – DESAFIOS

O alarme social instaurou-se, desafiando a atenção pública e política para os riscos e incertezas que os sistemas de vigilância digitais baseados em dados causam. Os estudos do Direito surgem com uma noção crítica sobre a temática, caracterizando estes dilemas como um atraso direito-tecnologia (PÚBLICO, 2018). Esta percepção generalizada de que não existem respostas legislativas efetivas face ao rápido desenvolvimento tecnológico (FRANCO, 2018) cria uma necessidade de se operarem mudanças tectônicas (GONÇALVES, 2017) na legislação, no sentido de criar documentos que regulamentem a técnica e definam parâmetros legais a cumprir no seu manuseamento. Esta necessidade de operar a mudanças legislativas pode ser perspectivada sobre o conceito de tecnoética de Bunge (1980), pois se materializa na necessidade de instaurar um novo paradigma de regulamentos, ações e movimentos que preconizem normas sociais e legais para que a emergência destas tecnociências (SKINNER, 2018; ARAÚJO, 2013) não seja lesiva para os direitos humanos.

Consequentemente, os estudos da vigilância alertam para a emergência de um fenómeno de desvirtuamento de função (FRÓIS, 2015): o desdobramento dos fins que a tecnologia avança aquando da sua criação, em finalidades distintas que podem potenciar efeitos sociais negativos. Coloca-se em causa um fenómeno emergente, que ultrapassa a utilização legítima das novas tecnologias, que Orwell (2009) descrevera como a má utilização da tecnologia, ou seja, o manuseamento destas novas potencialidades de forma negativa. Estes conceitos balizaram a análise empírica deste artigo, sendo a lente conceptual adotada na interpretação dos dados.

Desde o momento em que se problematizaram todas estas questões, a Europa começou a debater as consequências da expansão da vigilância que recolhe e analisa volumes inimagináveis de dados. Face à sofisticação tecnológica foram adotadas medidas para acompanhar o progresso das tecnologias. O objetivo é minimizar os efeitos negativos nos cidadãos, na sociedade e no sistema democrático em geral. A Comissão Europeia concluiu que as práticas de vigilância vigentes se intensificaram devido ao avanço tecnológico e isso revela uma reconfiguração da inteligência tradicional. A evolução simultânea destes fenómenos facilita o acesso a uma escala maior de sistemas para extração de dados, quando comparada com a vigilância anterior (WRIGHT; KREISSL, 2015; GONÇALVES, 2017; MATOS, 2018). O contexto europeu permeabilizou-se a estas mudanças, buscando cumprir os princípios legislativos que defende, ao mesmo tempo que quer garantir a segurança e paz dos Estados-Membros.

Concretamente, em fevereiro de 2016, o Conselho da Europa procedeu a uma reconfiguração de orientações e normas específicas acerca da proteção de dados e informações pessoais, num contexto de Big Data (MANTELERO, 2017). O Regulamento Geral de Proteção de Dados (RGPD) de 2016/679 é um progresso legislativo que reflete a preocupação com as garantias dos direitos e liberdades dos indivíduos. Nele consta um arsenal de princípios relacionados com a proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação desses dados. Este Regulamento prevê que os cidadãos possuam um controlo maior sobre seus dados pessoais, garantindo condições igualitárias para empresas. Desta forma, enfatizou-se o direito à proteção dos dados pessoais, enquanto direito fundamental europeu. Além disso, contempla um conjunto de regras que visam a construção de um único mercado digital, ou seja, as mesmas regras, para todos os cidadãos e todas as empresas, assegurando uma aplicação uniforme e coerente entre os diferentes Estados-Membros. Há um reforço criado em torno de direitos como o da transparência, de informação, acesso e pagamento, e ao silêncio. Também o direito ao consentimento prevê que haja uma atitude positiva e clara de manifestação deste, para que se proceda à coleta dos

dados. Preconiza, também, um novo direito de portabilidade dos dados individuais, que permite aos cidadãos pedir às empresas que coletaram seus dados, a sua devolução. Definindo, também, os conceitos de violações de dados pessoais.

Estas transformações legislativas representam um progresso na regulação de Big Data (MANTELERO, 2017). No entanto, dada a extensão do debate público em torno do tema, as expectativas sociais culminam num apelo de um reforço legal em torno dos dados pessoais, existindo uma percepção generalizada de que são necessárias mais leis que visem garantir a proteção efetiva do direito à privacidade (PÚBLICO, 2018; NEIVA, 2019). Esta crença origina um movimento de tecnoética (BUNGE, 1980): a necessidade de criar meios suficientes que mitiguem consequências negativas da expansão destas tecnologias. Exige-se um controlo da tecnologia, por exemplo, através da criação de entidades que regularizem as ações tecnológicas e uma nova legislação (LENZI, 2019). Os profissionais entrevistados partilham desta demanda pela tecnoética (BUNGE, 1980), enfatizando a necessidade de criação de reforços legais e atualização renovada dos existentes, de forma a precaver as violações dos direitos humanos, dada a expansão de Big Data. Sob um olhar de atraso direito-tecnologia (PÚBLICO, 2018) os discursos denotam a questão que Franco (2018) descrevera como a noção generalizada de que, por vezes, as novas tecnologias ultrapassam a resposta jurídica ao seu desenvolvimento.

METODOLOGIA

Este artigo tem como base uma investigação desenvolvida no 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 sediado no Centro de Estudos de Comunicação e Sociedade, Instituto de Ciências Sociais da Universidade do Minho (Portugal) (Contrato N.º [648608]). Este Projeto, de forma geral, explora as dimensões sociais, éticas, políticas, culturais e regulatórias do uso de tecnologias de ADN para uso forense na UE. A metodologia do Projeto inclui a realização de entrevistas a 140 profissionais em 25 países da UE. Os dados recolhidos da realização das entrevistas são o eixo empírico do presente artigo. Estas entrevistas foram realizadas a profissionais diretamente envolvidos em redes policiais e judiciárias de partilha transnacional de dados genéticos na UE no âmbito da investigação criminal (n= 47), geneticistas forenses (n= 49), membros de organizações não governamentais (n= 11), entidades de supervisão/regulação (n= 11), legisladores (n= 5), profissionais de empresas privadas (n= 2), académicos (n= 9), investigadores criminais (n= 5) e membros de meios de comunicação social (n= 1). As questões de partida foram: que expectativas em torno das potenciais aplicações de Big Data possuem os diferentes profissionais? Quais as suas percepções de eventuais desafios ao direito à privacidade?

As questões colocadas aos participantes concentravam-se na opinião destes relativamente aos usos potenciais que o Big Data proporciona; e em relação aos potenciais riscos e benefícios associados ao uso de informações biométricas disponíveis e futuras como Big Data. Seguindo os pressupostos da *Grounded Theory* (STRAUSS; CORBIN, 1990), que possibilita a formação de teorias “fundamentadas” nos próprios dados (CHARMAZ, 2009), o trabalho de pesquisa pautou-se pela articulação e comparação sistemática e paralela entre coleta, e análise, dados empíricos e teoria (STRAUSS; CORBIN, 1990). As entrevistas foram alvo de uma análise de conteúdo qualitativo (MAYRING, 2004) e, posteriormente, integradas e interpretadas segundo o sentido atribuído pelos entrevistados às questões realizadas. No presente artigo

encontram-se apresentados os extratos das entrevistas, integrados com as Teorias (STRAUSS; CORBIN, 1990).

RESULTADOS EMPÍRICOS

Apesar das Ciências Sociais enfatizarem a importância do estudo das expectativas em torno dos fenômenos sociais (BORUP; BROWN; KONRAD; VAN LENTE, 2006; BROWN; KRAFT; MARTIN, 2006; HEDGE COE; MARTIN, 2003), estes são escassos. As expectativas dos profissionais entrevistados foram consideradas enquanto expectativas tecnológicas que tratam fenômenos fruto da tecnologia (BORUP et al., 2006). Caracterizam-se como sendo expectativas baseadas em incertezas, na medida em que o seu conteúdo narrativo e discursivo repousa sobre dilemas no que concerne a aspectos de direitos, liberdades e garantias. Os profissionais entrevistados exacerbam e compartilham a incerteza, tornando mais aparente a dualidade dos discursos em torno deste debate (BROWN; MICHAEL, 2003). Imbuídos sobre a crença de um atraso direito-tecnologia (GONÇALVES, 2017), referem frequentemente a necessidade de criar novas leis que regulamentem Big Data, para combater os efeitos negativos que provoca.

Narrativas profissionais: que desafios?

Os profissionais entrevistados referem que Big Data é uma técnica perigosa e arriscada por permitir o acesso a dados informativos por parte de entidades que podem usá-los com fins distintos dos previstos inicialmente, aquando da sua coleta. Ou seja, o acesso aos dados, que não está (ainda) bem definido, poderá ser cedido a entidades que podem lesar os titulares das informações coletadas, tal como expressa o seguinte entrevistado:

“Acho que é [Big Data] muito perigoso, nomeadamente para entidades que têm fins lucrativos (...), que têm acesso ou poderão ter acesso a uma série de informações que em conjunto lhes poderão dar informação que poderá prejudicar efetivamente as pessoas (...).” [Profissional diretamente envolvido em rede policial e judiciária de partilha transnacional de dados genéticos]

Tendo em conta a definição de Clarke (1999) de privacidade, a noção de que se materializa no espaço pessoal livre de acesso de outras pessoas e organizações, com estas técnicas, sob a ótica dos entrevistados, os indivíduos poderão ver a sua privacidade desrespeitada pelas empresas com fins lucrativos. Verifica-se uma preocupação unânime em garantir que o acesso às informações pessoais seja restrito a entidades definidas, para que a partilha, uso e cedência desses mesmos dados não sejam realizadas para outros fins, de forma a minimizar a lesão dos direitos, liberdades e garantias dos titulares dos dados. Estas expectativas são o reflexo da percepção de um fenómeno de desvirtuamento da função, ou seja, quando as novas tecnologias ao serviço da vigilância se concretizam em fins que não eram os previstos aquando da sua criação (FRÓIS, 2015). Este entrevistado refere que as informações pessoais cedidas por via destas técnicas podem prejudicar efetivamente as pessoas. Este tipo de acontecimentos, concretizam-se quando se procede a uma má utilização da tecnologia (ORWELL, 2009). Como forma de precaver estes efeitos negativos, os entrevistados referem que é crucial criar normas

legais que protejam os interesses dos indivíduos neste arsenal tecnológico, como se pode observar no seguinte extrato:

“(...) Para que essas situações [de cruzamento de um grande número de informações] possam passar a ser prática (...) terão de sair mais leis para proteção de determinados interesses dos indivíduos. (...) não pode ser qualquer pessoa que possa ter acesso a esse tipo de informações e ao cruzamento de essas informações, e não pode fazer o cruzamento assim aleatoriamente (...), tem de estar tudo muito bem regulado e muito bem definido (...).” [Geneticista Forense]

A definição legal das entidades com acesso aos dados é o primeiro passo identificado pelos entrevistados para que a expansão de Big Data seja menos lesiva. Encontra-se, frequentemente, nestas narrativas discursivas, o apelo à necessidade de se implementarem novas leis, regulamentos e definições legislativas para o Big Data. O que denota que os entrevistados partilham da expectativa de que existe um atraso direito-tecnologia (PÚBLICO, 2018): percepção de que o Direito, no sentido da legislação, ainda não respondeu aos desenvolvimentos tecnológicos. Esta ausência de resposta legal pode provocar o uso dos dados sem consentimento dos titulares. Desta forma, os entrevistados consideram que se trata de uma matéria a ser resolvida pelo Direito, como se lê nos seguintes extratos:

“(...) [Big Data é] uma questão de regulação pelo Direito (...).” [Membro de uma Comissão de Proteção de Dados]

“[Big Data] deve ser devidamente enquadrado segundo (...) juristas (...).” [Geneticista Forense]

Adotando a lente de Bunge (1980), estas expectativas revelam a necessidade de que os entrevistados expressam em criar-se uma tecnoética – um conjunto de regulamentos normativos que controlem e diminuam os efeitos nefastos que as tecnologias têm nos direitos humanos.

Além destas considerações, os entrevistados tecem considerações, também, acerca da finalidade do uso dos dados. Referem que a utilização, partilha e cedência destas informações pessoais para outros fins que não os previstos inicialmente pode colocar em causa a privacidade dos dados cedidos. A percepção de que possa ocorrer o fenómeno de desvirtuamento da função (FRÓIS, 2015) inicialmente prevista para a técnica de Big Data, incontroável e que pode ter margem para lesar os direitos, liberdades e garantias. A consciencialização desta possibilidade encaminha os profissionais entrevistados num discurso que salienta a peculiaridade e sensibilidade dos dados (MACHADO; SILVA, 2015) que Big Data junta, enfatizando a necessidade de restringir o acesso apenas a autoridades e órgãos autorizados:

“(...) é o problema da limitação da finalidade, e o acesso a esses bancos de dados [de Big Data] deve ser restrito apenas a autoridades e órgãos autorizados.” [Membro de Comissão de Proteção de Dados]

Apesar desta ser uma das preocupações dos profissionais entrevistados, o Conselho Europeu, estabeleceu como um dos seus princípios a limitação da finalidade, que significa que os dados pessoais só podem ser recolhidos para fins específicos, explícitos e legítimos e não podem ser processados de forma incompatível com esses fins (GONÇALVES, 2017). No entanto, os profissionais

entrevistados consideram que existe o risco eminente dos dados pessoais serem usados para outros fins e lesar os titulares destes:

“(...) O risco é que a utilização desta informação [obtida por via de Big Data] extravase este âmbito. (...) É que se ultrapasse este foco (...) e se vá a outras áreas. (...) isso é que acho que pode ser perigoso.” [Geneticista Forense]

Estas expectativas materializam o que Orwell (2009) apresentou como sendo uma má utilização da tecnologia, ou seja, o seu uso para fins ilegítimos. Verifica-se uma antevisão dos riscos e dos perigos desta técnica, caso esta seja um meio para compilar e combinar dados, para fins não consentidos. A preocupação expressa que se prende com o acesso aos dados, a sua utilização e manuseio reflete a natureza privada destas informações pessoais. Estes recortes discursivos são consonantes com o que a literatura documenta sobre a temática. Boyd e Crawford (2012) enfatizam a importância de questionarmos: Quem tem acesso aos dados? Em que contextos? Com que restrições? Qual a finalidade? Tendo em conta que Big Data possibilita o acesso a um grande volume de informações geradas por e sobre pessoas, pode comprometer a privacidade dos indivíduos (HERSCHEL; MIORI, 2017). Ou seja, mais uma vez, a preocupação eminente dos entrevistados que a tecnologia cumpra fins distintos dos previstos inicialmente e use a coleta consentida dos dados para outras finalidades (FRÓIS, 2015). Consequentemente, esta natureza privada e pessoal dos dados informativos que estão armazenados nas bases de dados, exige que seja demarcada a margem de ação dos responsáveis pela sua manutenção e posterior partilha:

“(...) Tem de ser garantido que é privada [a informação contida nas grandes bases de dados], que só é acedida em determinados contextos. (...) eu acho que é essa linha que tem de ser traçada, [e] (...) se calhar, uniformizada em todos os países.” [Membro de Comissão de Proteção de Dados]

Os profissionais entrevistados enfatizam a natureza privada das informações e dos dados, salientando a necessidade de proteger o domínio sensível destes dados pessoais (MACHADO; SILVA, 2015). Na sua ótica, deve restringir-se o acesso a estas bases de dados, no sentido de minimizar as violações ao direito à privacidade.

Estes discursos são preocupações contemporâneas e alarmistas: nomeiam aspetos acerca das pessoas titulares dos dados que são alvo deste escrutínio, referindo os impactos, ao nível da privacidade, que este acesso pode ter nos cotidianos sociais, nas liberdades e garantias democráticas. Estes aspetos evidenciam a posição não concordante dos participantes (NEIVA, 2019):

“(...) Seria [utilizar Big Data como potencial meio de investigação criminal, genético e forense] uma invasão da privacidade das pessoas, (...). Ficar com essas informações quando são entidades que não estão acreditadas para o fazer ou... Não concordo muito. (...)” [Geneticista Forense]

Consequentemente, emerge uma visão generalizada acerca dos riscos e perigos que a expansão e o desenvolvimento de Big Data podem acarretar no direito à vida privada e na proteção de dados. Verifica-se uma representação socioprofissional que o uso de Big Data ao serviço da coleta de dados privados e pessoais, permitirá condicionar os cidadãos, na medida em que lhe restringe direitos e garantias. Estes

profissionais partilham da crença generalizada de uma má utilização de Big Data (ORWELL, 2009):

**“(...) As implicações que isso [Big Data] possa ter, nos direitos, nas liberdades, não se trata apenas de direito à vida privada e à proteção de dados, mas de uma maneira mais geral os condicionamentos das pessoas. (...)”
[Professor/Investigador]**

Não obstante, levantam-se dilemas morais e éticos: entre as garantias protegidas pelo Estado democrático europeu e a incontornável sofisticação tecnológica. Os profissionais nomeiam a dificuldade de se atingir uma harmonia política europeia entre a garantia da segurança dos cidadãos e a proteção de direitos (NEIVA, 2019). Neste debate contemporâneo, a par da percepção de que a tecnologia está em desenvolvimento, os participantes reconhecem que isso pode potenciar e aumentar a colisão com direitos, liberdades e garantias fundamentais dos cidadãos, como é ilustrativo no seguinte extrato:

“(...) Nós temos uma perspectiva na União Europeia [acerca do equilíbrio entre o direito à privacidade e o uso de dados pessoais] para assegurar o bem comum mais vocacionada para a proteção dos direitos fundamentais. (...) onde de facto se procura limitar, ou pelo menos garantir que o uso de dados pessoais não é feito de forma completamente livre e irrestrita, (...) mas é mesmo necessário limitar os direitos? O direito à privacidade e à proteção dos dados pessoais (...)? (...) vamos ter sempre esta tensão nos próximos anos. (...) Porque o desenvolvimento tecnológico vai-nos permitir novos mecanismos que vão ser utilizados também pelo Estado (...), e que vão colidir seguramente com direitos fundamentais dos cidadãos. (...)” [Professor/Investigador]

O debate está instaurado e a necessidade de equilibrar os dois pratos da balança é cada vez mais sentida. Apesar dos estudos existentes evidenciarem as evoluções legislativas e as transformações legais que esta técnica desencadeou (DREWER; MILADINOVA, 2017; GONÇALVES, 2017; KUBLER, 2017; MANTELERO, 2017; PÚBLICO, 2018), este artigo indica que as representações profissionais de Big Data se direcionam no sentido oposto. Os profissionais entrevistados percebem esta realidade como um campo ainda por regulamentar. Apesar dos esforços legislativos no sentido de contrariar a percepção generalizada de um atraso direito-tecnologia (PÚBLICO, 2018), os discursos profissionais repousam nesse sentido. É expressa uma necessidade de legislar esta técnica, de operar no sentido de mudanças tectónicas (GONÇALVES, 2017) que possam responder aos dilemas que surgem. Por um lado, a garantia dos direitos e liberdades; em colisão com a coleta e armazenamento de dados pessoais e consequente violação à privacidade. Os profissionais entrevistados referem a necessidade de criar um novo paradigma que defina quem tem acesso aos dados, como é que esse acesso é feito e como é que os dados devem ser usados, *a posteriori* (NEIVA, 2019). Desta forma, os entrevistados ocupam uma posição de alta privacidade, na medida em que atribuem valor ao direito à privacidade e demonstram alta desconfiança organizacional, ao mesmo tempo que defendem intervenções de privacidade por via de regras legais (WESTIN, 2003).

CONSIDERAÇÕES FINAIS

É necessário (re)pensar as práticas atuais digitais usadas ao serviço da vigilância e refletir acerca de Big Data. As narrativas discursivas analisadas permitem tecer alguns recortes conclusivos acerca dos desafios que encontramos, no que toca à privacidade, na Era do Big Data. O arsenal teórico foi baseado em conceitos como desvirtuamento da função (FRÓIS, 2015), tecnociência (SKINNER, 2018; ARAÚJO, 2013), tecnoética (BUNGE, 1980), má utilização da tecnologia (ORWELL, 2009), atraso direito-tecnologia e mudanças tectónicas (GONÇALVES, 2017; PÚBLICO, 2018). Em geral, os profissionais entrevistados são atores sociais conectados laboralmente em setores onde, futuramente, Big Data poderá vir a constituir-se enquanto técnica de investigação criminal. E, em particular, meios de coleta, acesso e partilha de dados pessoais. As suas expectativas são veículos importantes para definição de rotas e caminhos futuros. Todos os profissionais entrevistados demonstraram preocupação com o direito à privacidade e possibilidade de Big Data lesar liberdades, direitos e garantias individuais. Em concreto, nomearam a necessidade de se identificar as entidades responsáveis pelo acesso aos dados recolhidos, de forma a diminuir as possibilidades do uso dos dados para outros fins que não os consentidos inicialmente, potenciando a proteção e promoção dos direitos humanos. Estes discursos evidenciam a preocupação dos entrevistados com o fenómeno de desvirtuamento de função (FRÓIS, 2015), no sentido em que o Big Data cumpra funções indesejadas. Para tal, referem frequentemente a necessidade de redefinir e criar, reforçando, a legislação no sentido de proteger e demarcar a natureza sensível e peculiar dos dados pessoais a serem coletados, analisados e partilhados (MACHADO; SILVA, 2015). Desta forma, apoiam e evidenciam a necessidade de operar em mudanças tectónicas (GONÇALVES, 2017) na legislação, no sentido de combater o atraso direito-tecnologia (PÚBLICO, 2018) que os profissionais entrevistados percebem. As suas expectativas expressam a necessidade de criar um novo paradigma em torno das novas tecnologias – uma tecnoética (BUNGE, 1980) – um movimento de ética em torno das potencialidades destas técnicas que balize a sua margem de ação, no sentido de promover a ética, ao mesmo tempo que protege os direitos humanos.

Apesar da concepção generalizada das narrativas dos entrevistados incidirem sobre a noção de um *atraso direito-tecnologia* (PÚBLICO, 2018), o regime legislativo tem-se permeabilizado à emergência das novas tecnologias (MANTELERO, 2017). O RGPD 2016/679 surge com a finalidade de criar um novo paradigma de regulação em matéria de proteção de dados, introduzindo mudanças na estrutura do sistema jurídico. Contudo, ainda continua por responder a questão sobre se o novo Regulamento abraçará o desenvolvimento de Big Data nos próximos anos (MANTELERO, 2017). Os entrevistados nomeiam a necessidade de criar soluções trazidas pelo Direito que não emergjam depois de estarem ultrapassadas pelos desenvolvimentos tecnológicos (FRANCO, 2018), apesar de se observarem mudanças tectónicas (GONÇALVES, 2017) que buscam dar respostas breves e eficazes a estes dilemas processuais. Estes resultados vão de encontro ao que é teorizado no Brasil sobre o tema. Os estudos indicam, de forma geral que Big Data apresenta características específicas que ultrapassam as proteções estabelecidas até ao momento. Estudos que se debruçam sobre a análise das tendências legislativas sobre a proteção de dados pessoais e privacidade indicam que é necessário reforçar a lei no sentido de garantir, com maior eficácia, o consentimento e o conhecimento dos titulares dos dados sobre o uso de seus dados (SILVA; RODRIGUES, 2017; DIAS; VIEIRA, 2013; MEIRELES, 2016; FRANCO, 2018; YURI;

REGINA, 2018). Apesar disso, estes resultados científicos indicam que a produção acadêmica sobre o tema é, ainda, escassa (CARLONI; COMNÈNE, 2013; YURI; REGINA, 2018). Espera-se, portanto, que este artigo alargue o debate e contribua para a produção de conhecimento social em torno da temática, combatendo a lacuna científica existente.

Concluindo, (re)pensar o Big Data simboliza promover a democracia e coesão social, numa sociedade tecnológica. Big Data é uma técnica que converte os deveres morais em deveres fluídos, dada o seu poder omnipresente. Assim, emerge um desafio moral social porque os cidadãos usam as novas tecnologias, mas também adotam uma postura crítica de controlo sobre a forma como estas os afetam. Os indivíduos desejam a privacidade, mas não de forma absoluta, porque também desejam integrar a sociedade. Desta forma, surgem dilemas pessoais entre o desejo da privacidade e o desejo de comunicar e expor-se a outros, cumprindo as normas sociais e integrando-as (WESTIN, 2015). Desta forma, é crucial pensar o fenómeno, buscando respostas aos dilemas éticos, mas também criar novas questões, sempre em busca do equilíbrio entre a garantia da segurança e a preservação dos direitos (NEIVA, 2019).

The right to privacy in big data era: professionals narratives in the European Union

ABSTRACT

There is a growing debate today about human rights and Big Data. This paper explores the expectations of professionals involved in the transnational exchange of data, forensic geneticists, and stakeholders from different fields about the inclusion of Big Data in the transnational criminal investigation. Based on a qualitative methodology of content analysis of interviews, the objective is to access the meanings that these professionals attribute to Big Data as a potential criminal investigation technique, within the scope of their professional activities. Despite the promise of the potential of Big Data in terms of effectiveness and efficiency, their inclusion in criminal investigations imposes ethical and human rights issues that need to be addressed. I conclude that the interviewees refer to the difficulty of finding the balance between guaranteeing the rights, freedoms, and guarantees with the promotion of public safety; the ethics of criminal investigation; and violations of the right to privacy.

KEYWORDS: Big Data. Privacy. Digital era. Human Rights. Challenges.

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 sedado no Centro de Estudos de Comunicação e Sociedade, Instituto de Ciências Sociais da Universidade do Minho (Portugal).

REFERÊNCIAS

ALBUQUERQUE, G.; PEDRO, R. (2013). Facebook como dispositivo de vigilância e visibilidade: algumas controvérsias em questão. **Revista Tecnologia e Sociedade**, v. 9, n. 18, 2013.

ARAÚJO, E. (2013). A espera e os estudos sociais do tempo e sociedade. In: ARAÚJO, E.; DUQUE (Eds.). **Os tempos sociais e o mundo contemporâneo. Um debate para as ciências sociais e humanas**. Universidade do Minho: Centro de Estudos de Comunicação e Sociedade / Centro de Investigação em Ciências Sociais, 2013, pp. 9-27.

BALL, K.; DI DOMENICO, M.; NUNAN, D. Big data surveillance and the body subject. **Body & Society**, v. 22, n. 2, pp. 58-81, 2016.

BARTLETT, A.; LEWIS, J.; REYES-GALINDO, L.; STEPHENS, N. The locus of legitimate interpretation in Big Data sciences: Lessons for computational social science fromomic biology and high-energy physics. **Big Data & Society**, v. 5, n. 1, pp. 1-15, 2018.

BOYD, D.; CRAWFORD, K. Critical questions for big data. **Information, Communication & Society**, v. 15, n. 5, pp. 662-679, 2012.

BORGES, L. C.; MACHADO, D. Q. O Círculo: um estudo observacional dos conflitos entre o desenvolvimento tecnológico e os limites da privacidade. **Revista Tecnologia e Sociedade, Curitiba**, v. 15, n.38, p. 242-258, out/dez. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/8500> . Acesso em: 02/12/2019.

BORUP, M.; BROWN, N.; KONRAD, K.; VAN LENTE, H. The sociology of expectations in science and technology. **Technology analysis & strategic management**, v. 18, n. 3-4, pp. 285-298, 2006.

BRAYNE, S. Big data surveillance: The case of policing. **American Sociological Review**, v. 82, n. 5, pp. 977-1008, 2017.

BROWN, N.; KRAFT, A.; MARTIN, P. The promissory pasts of blood stem cells. **BioSocieties**, v. 1, n. 3, pp. 329-348, 2006.

BROWN, N.; MICHAEL, M. A Sociology of Expectations: Retrospecting Prospects and Prospecting Retrospects. **Technology Analysis and Strategic Management**, v. 15, n. 1, pp. 3-18, 2003.

BUNGE, M. **Ciência em Desenvolvimento**. Belo Horizonte: Itatiaia, 1980.

CANOTILHO, G.; MOREIRA, V. **Constituição da República Portuguesa. Lei do Tribunal Constitucional**. Coimbra: Coimbra Editora, 2005.

CARLONI, G. L. B. D. S.; COMNÈNE, A. **Privacidade e inovação na era do Big Data**. Graduação (Direito) - Fundação Getulio Vargas. Escola de Direito da FGV Direito. Rio de Janeiro, 2013.

CHAN, J.; MOSES, L. Is Big Data challenging criminology? **Theoretical Criminology**, v. 20, n. 1, pp. 21-39, 2015.

CHAN, J.; MOSES, L. Making sense of Big Data for security. **British Journal of Criminology**, v. 57, n. 2, pp. 299-319, 2017.

CHARMAZ, K. **A construção da teoria fundamentada: Guia prático para análise qualitativa**. Porto Alegre: Artmed, 2009.

CLARKE, R. Internet privacy concerns confirm the case for intervention. **Communications of The Acm**, v. 42, n. 2, p. 60-67, 1999.

COLL, S. Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance. **Information, Communication & Society**, v. 17, n. 10, pp. 1250-1263, 2014.

DIAS, A.; VIEIRA, N. Big Data: questões éticas e legais emergentes. **Ciência da Informação**, v. 42, n. 2, 2013.

DREWER, D.; MILADINOVA, V. The BIG DATA challenge: Impact and opportunity of large quantities of information under the Europol Regulation. **Computer Law & Security Review**, v. 33, n. 3, PP. 298-308, 2017.

UNIÃO EUROPEIA. Lei n.º 2016.679 de 27 de abril de 2016. Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia, v. 3, pp. 1-88.

FRADE, C. Social theory and the politics of Big Data and method. **Sociology**, v. 50, n. 5, pp. 863-877, 2016.

FRANCO, M. Big Data e Open Data vs. Privacidade: constituiria a ferramenta tecnológica em uma invasão à privacidade? **Revista de Estudos Jurídicos UNESP, Franca**, v. 20, n. 32, pp. 295-308, 2018. Disponível em: <http://seer>.

franca.unesp.br/index.php/estudosjuridicosunesp/index>. Acesso em: 12/12/2019.

FRÓIS, C. Dos estudos de vigilância, videovigilância e tecnologia. Reflexão sobre o estado da arte. In: CUNHA, M. (Ed.). **Do crime e do castigo: temas e debates contemporâneos**. Editora Mundos Sociais, 2015, pp. 147-157.

GANDY JR, H. The surveillance society: information technology and bureaucratic social control. **Journal of Communication**, v. 39, n. 3, pp. 61-76, 1989.

GONÇALVES, M. (2003). **Direito de Informação: Novos Direitos e Formas de Regulação na Sociedade de Informação**. Coimbra: Almedina, 2003.

GONÇALVES, M. The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. **Information & Communications Technology Law**, v. 26, n. 2, pp. 90-115, 2017.

KITCHIN, R. Big Data, new epistemologies and paradigm shifts. **Big Data & Society**, v. 1, n. 1, pp. 1-12, 2014.

PÚBLICO. **Quem controla os nossos dados?** Disponível em: <https://www.publico.pt/2018/03/20/tecnologia/opiniao/quem-controla-os-nossos-dados-1807206> . Acesso em: 28 març. 2019.

GUZIK, K. Discrimination by Design: predictive data mining as security practice in the United States 'war on terrorism'. **Surveillance & Society**, v. 7, n. 1, pp. 3-20, 2009.

HALFORD, S.; SAVAGE, M. Speaking sociologically with big data: symphonic social science and the future for big data research. **Sociology**, v. 51, n. 6, pp. 1132-1148, 2017.

HEDGECOE, A.; MARTIN, P. The drugs don't work: expectations and the shaping of pharmacogenetics. **Social studies of science**, v. 33, n. 3, pp. 327-364, 2003.

HERSCHEL, R.; MIORI, V. Ethics & Big Data. **Technology in Society**, v. 49, pp. 31-36, 2017.

KUBLER, K. State of urgency: Surveillance, power, and algorithms in France's state of emergency. **Big Data & Society**, v. 4, n. 2, pp. 1-10, 2017.

LEFÈVRE, T. Big data in forensic science and medicine. **Journal of Forensic and Legal Medicine**, v. 57, pp. 1-6, 2017.

LENZI, L. Reflexões sobre o caráter ambíguo e controverso da tecnologia. **R. Technol. Soc.**, Curitiba, v. 15, n. 36, p. 151-164, abr./jun. 2019.

LYON, D. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, v. 1, n. 2, pp. 1-13, 2014.

LUPTON, D.; MICHAEL, M. 'Depends on Who's Got the Data': Public Understandings of Personal Digital Dataveillance. **Surveillance & Society**, v. 15, n. 2, 2017.

MACHADO, H.; SILVA, S. Public perspectives on risks and benefits of forensic DNA databases: an approach to the influence of professional group, education, and age. **Bulletin of Science, Technology & Society**, v. 35, n. 1-2, pp. 16-24, 2015.

MANTELERO, A. Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. **Computer Law & Security Review**, v. 33, n. 5, pp. 584-602, 2017.

MATOS, S. Biometria e privacidade: desafios bioéticos na cooperação policial e judicial na União Europeia. In: SOL, A.; GOUVEIA, S. (Eds.). **Bioética no Século XXI**. Charleston: CreateSpace Independent Publishing, 2018, pp. 255-286.

MATZNER, T. Beyond data as representation: The performativity of Big Data in surveillance. **Surveillance & Society**, v. 14, n. 2, pp. 197-210, 2016.

MARYING, P. "Qualitative Content Analysis". In: FLICK, U.; VON KARDORFF E.; STEINKE, I. (Eds.). **A Companion to Qualitative Research**. London: Sage, 2004, pp. 266-269.

MEIRELES, V. Autonomia e privacidade no ambiente digital. **Revista Eletrônica de Ciência Política**, v. 7, n. 2, 2016.

NEIVA, L. **Big Data na investigação criminal: previsão do risco, vigilância e expectativas sociais na União Europeia**. Tese (Mestrado) – Mestrado em Crime, Diferença e Desigualdade, Universidade do Minho, Braga, Portugal, 2019.

NORBERG, P. A.; HORNE, D. R.; HORNE, D. A. The privacy paradox: personal information disclosure intentions versus behaviors. **The Journal of Consumer Affairs**, v. 41, n. 1, p. 100-126, 2007.

ORWELL, G. **1984**. Editora Companhia das Letras, 2009.

OBSERVADOR. **Edward Snowden: a privacidade dos dados e uma geração "que já não é dona de nada"**. Disponível em: <https://observador.pt/2019/11/04/edward-snowden-a-privacidade-dos-dados-e-uma-geracao-que-ja-nao-e-dona-de-nada/> . Acesso em: 4 nov. 2019.

OBSERVADOR. **Termómetro da Web Summit: se não fosse Edward Snowden, tínhamos passado frio**. Disponível em:

<https://observador.pt/2019/11/04/termometro-da-web-summit-se-nao-fosse-edward-snowden-tinhamos-passado-frio/>. Acesso em: 4 nov. 2019.

SILVA, C. R.; RODRIGUES, E. M. T. (2017). Privacidade em Big Data: panorama e agenda de pesquisa. **Sistemas & Gestão**, v. 12, n. 4, pp. 491-505.

SKINNER, D. Race, Racism and Identification in the Era of Technosecurity. **Science as Culture**, v. 29, n. 1, pp. 1-23, 2018.

SOUZA, L. Dilemas e hesitações da modernidade tardia e a emergência da sociedade de controle. **Revista Mediações**, v. 15, n. 2, pp. 78-99, 2010.

STEVENS, M.; WEHRENS, R.; DE BONT A. Conceptualizations of Big Data and their epistemological claims in healthcare: A discourse analysis. **Big Data & Society**, v. 5, n.2, pp. 1-21, 2018.

STRAUSS, A.; CORBIN, J. **Basis of qualitative research: Grounded theory procedures and techniques for developing grounded theory**. Newbury Park: SAGE Publications, 1990.

TAYLOR, L. What is data justice? The case for connecting digital rights and freedoms globally. **Big Data & Society**, v. 4, n. 2, pp. 1-14, 2017.

VAN DER VLIST, F. N. Counter-Mapping Surveillance. **Surveillance & Society**, v. 15, n. 1, pp. 137-157, 2017.

VAN DIJCK, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, pp. 197-201, 2014.

VAN LENTE, H. Navigating foresight in a sea of expectations: lessons from the sociology of expectations. **Technology Analysis & Strategic Management**, v. 24, n. 8, pp. 769-782, 2012.

WARREN, S.; BRANDEIS, L. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, pp. 193-220, 1890.

WESTIN, A. **Privacy and Freedom**. New York: IG Publishing, 2015.

WESTIN, A. Social and political dimensions of privacy. **Journal of Social Issues**, v. 59, n. 2, pp. 431-453.

WOOD M.; BALL, K. (Eds). A report on the surveillance society. Disponível em: <https://ico.org.uk/media/about-the-ico/documents/1042388/surveillance-society-public-discussion-document-06.pdf> , 2006. Acesso em jan. 2018.

WRIGHT, D.; KREISSL, R. **Surveillance in Europe**. Oxon and New York: Routledge, 2015.

YOUNG, S. Slipping Through the Cracks: Background Investigations after Snowden. **Surveillance & Society**, v. 15, n. 1, pp. 123-136, 2017.

YOUTIE, J.; PORTER, A.; HUANG, Y. Early social science research about Big Data. **Science and Public Policy**, v. 44, n. 1, pp. 65-74, 2016.

YURI, L.; REGINA, C. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da ciência da informação no Brasil. **Perspetivas em Ciência da Informação**, v. 23, n. 4, pp. 117-132, 2018.

Recebido: 22/12/2019

Aprovado: 09/05/2020

DOI: 10.3895/rts.v16n45.11439

Como citar: NEIVA, L. O direito à privacidade no tempo do big data: narrativas profissionais na União Europeia. **Rev. Technol. Soc.**, Curitiba, v. 16, n. 45, p. 1-20, out/dez. 2020. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/11439> . Acesso em: XXX.

Correspondência:

Direito autoral: Este artigo está licenciado sob os termos da Licença Creative Commons-Atribuição 4.0 Internacional.

