UNIVERSIDADE DE BRASÍLIA

Faculdade de Direito

Ariadne Cristina de Souza

ENTRE A PRIVACIDADE E A VIGILÂNCIA:

Desafios ao direito fundamental à proteção de dados pessoais

Brasília

2019

Ariadne Cristina de Souza

ENTRE A PRIVACIDADE E A VIGILÂNCIA:

Desafios ao direito fundamental à proteção de dados pessoais

Trabalho de conclusão de curso apresentado à Faculdade de Direito da Universidade de Brasília como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. João Costa Neto

Brasília

2019

Ariadne Cristina de Souza

ENTRE A PRIVACIDADE E A VIGILÂNCIA:

Desafios ao direito fundamental à proteção de dados pessoais

Trabalho de conclusão de curso apresentado à Faculdade de Direito da Universidade de Brasília como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. João Costa Neto

Apresentado em 06 de julho de 2019

BANCA EXAMINADORA

_____

Professor Dr. João Costa Neto

_____

Professor Dr. Alexandre Kehrig Veronese

_____

Professor Dr. Paulo Cesar Villela Souto Lopes Rodrigues

Dedico este trabalho à minha turma da graduação, Direito 110, onde fiz muitos amigos que levarei para o resto da vida. Também dedico à minha família, por me proporcionarem tantos privilégios.

RESUMO

Este trabalho visa a analisar os conceitos e princípios relacionados à privacidade e à proteção de dados pessoais firmados no ordenamento jurídico pátrio, traçando um panorama evolutivo do tema no mundo. Expõe um breve histórico da jurisprudência do tema e revisa os principais conceitos da Lei Geral de Proteção de Dados relacionados aos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Verifica também as consequências de se manter no Estado Democrático de Direito práticas que perpetuam a admissibilidade automática das provas produzidas no inquérito policial, funcionando, assim, como instrumento de manipulação da verdade por detentores do poder e fugindo do escopo constitucional do processo. Por fim, faz uma breve discussão sobre o uso de novas tecnologias de reconhecimento biométrico com inteligência artificial por agentes de segurança pública e seus limites entre o que se espera da privacidade e o que se admite como interesse público.

Palavras-chave: privacidade; dados pessoais; lei geral de proteção de dados; direitos fundamentais; processo penal; gestão da prova.

ABSTRACT

This work aims at analyzing privacy's and personal data protection's concepts and principles set in this country's law system, drawing an international evolutionary landscape over the topic. It exposes a brief history of the precedents on the subject and revises the main concepts of Brazil's General Data Protection Regulation, relating to its principles of purpose limitation, lawfulness, data minimization, open access, accuracy, transparency, integrity, foresight and prevention, no discrimination and accountability. It also notes the consequences of keeping practices in a Democratic State of Law that maintain the automatic admission of evidence collected by police investigation, as it works as a means of manipulating the truth by the powerful actors involved and drifting away from the constitutional purpose of criminal prosecution. Lastly, it makes a brief discussion about the use of new biometric recognition technology assisted with artificial intelligence by public security agents and the limits between what is expected of privacy and what is expected to be of public interest.

Key words: privacy; personal data; general data protection regulation; fundamental rights; criminal prosecution; admissibility of evidence.

LISTA DE ABREVIATURAS E SIGLAS

ALPR - Sistema de Reconhecimento Automático de Placas de Carro
CDC - Código de Defesa do Consumidor, Lei nº 8.078/90
CF - Constituição Federal de 1988
CPP - Código de Processo Penal de 1941
FBI - Departamento Federal de Investigação da justiça dos Estados Unidos
GDPR - Regulamento Geral de Proteção de Dados da União Europeia
IDEC - Instituto Brasileiro de Defesa do Consumidor
LGPD - Lei Geral de Proteção de Dados, Lei nº 13.709/2018
PMERJ - Polícia Militar do estado do Rio de janeiro
RE - Recurso Extraordinário
REsp - Recurso Especial
SNI - Serviço Nacional de Informações
SPC - Serviço de Proteção ao Crédito
STF - Supremo Tribunal Federal
STJ - Superior Tribunal de Justiça

SUMÁRIO

INTRODUÇÃO

A Lei Geral de Proteção de Dados, sancionada em 2018, entra em vigor a partir de 2020, mas já está movendo não apenas o ordenamento jurídico, exigindo adaptações, mas também o poder legislativo, empresários, agentes reguladores, enfim, muitos setores da sociedade. A LGPD realiza um grande salto paradigmático quanto a proteção de dados pessoais, além de reacender o debate sobre os limites da privacidade ante o interesse público, e o faz trazendo uma estrutura de princípios[1]aplicados em qualquer atividade de tratamento de dados pessoais, os quais devem resguardar fundamentos elencados no artigo 2º. Desses fundamentos, muitos perpassam garantias constitucionais, tais como a privacidade, a liberdade de expressão, a inviolabilidade da intimidade, os direitos humanos e a dignidade humana. Mas dentre esses fundamentos, houve espaço para a inovação, elevando a autodeterminação informativa a este patamar.

Apesar de apresentar amplo campo de atuação, a novel legislação não é aplicada a algumas exceções, que estão no artigo 4º, como quando o tratamento de dados é realizado para fins de segurança pública. Ainda assim, a lei prevê expressamente a necessidade da atividade seguir os princípios gerais de proteção.

---

[1]"Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Ao mesmo tempo, ascende às políticas de segurança pública a tendência de “investir em inteligência”, muitas vezes traduzida como o emprego de equipamentos de alta tecnologia para o combate ostensivo e a prevenção da criminalidade.

O presente trabalho tenta trazer essas questões ao debate sobre a privacidade sob a perspectiva crítica de alguns autores quanto a não neutralidade inerentes à tecnologia e às políticas de vigilância, dado que tanto a tecnologia, quanto a vigilância, são temas cada vez mais tratados até com naturalidade pela população em geral, apoiada na crença de que a tecnologia não envolve fatores humanos e, portanto, é isenta de “vícios”, bem como na crença da necessidade de aprofundar a vigilância sobre os indivíduos em nome do “bem maior” promovido pela sensação de segurança.

1.INSTRUMENTALIDADE E GARANTIAS DO (PRÉ) PROCESSO PENAL

As garantias do processo penal carregam, em suas diretrizes constitucionais, a história da asserção dos direitos humanos no ordenamento jurídico, culminando em normas fundamentais adotadas pelas constituições democráticas modernas, versando sobre o direito à vida, à liberdade, à educação, entre muitos outros. Os direitos fundamentais podem ser lidos como garantias elevadas ao nível constitucional que determinam a postura do Estado quanto a suas ações (prestação de direitos sociais) e omissões (dever de não intervir) em relação aos indivíduos.

A evolução do processo penal pode ser observada como também a evolução das estruturas estatais. A imposição da pena como meio de controle social evoca a necessidade do Estado legitimar suas ações, adotando regras para o jogo que se supõem claras e de comum aceitação. Como bem resume Aury "Ao suprimir a vingança privada e avocar o poder de punir, nasce o processo penal como caminho necessário para que o Estado legitimamente imponha uma pena."[2].

O poder de perseguir e punir os indivíduos em busca da aplicação da pena definida pelo Direito Penal mostra-se portanto como a ação mais violenta que o Estado pode impor a estes. Para que seja legitimada essa violência, o Estado adota um procedimento peculiar às outras atividades jurisdicionais, dado que a apuração dos fatos nesse procedimento pode significar a privação da liberdade de alguém. Decorreria então o interesse do agente estatal em tornar o provimento jurisdicional mais aproximado da verdade processual quanto for possível, em busca de legitimidade, ao que chama Ferrajoli de "correspondência aproximativa":

> Diversamente de todas as outras normas e atos jurídicos, cuja condição única de validade é a observância das normas superiores, a legitimidade dos atos jurisdicionais penais, portanto, está condicionada também pela sua verdade processual no sentido já ilustrado de 'correspondência aproximativa'. Melhor dizendo, está condicionada pela verdade ou credibilidade, fática ou jurídica, dos discursos assertivos que formam sua motivação.[3]

---

[2] LOPES JR., Aury. Direito processual penal. 11ª ed. São Paulo: Saraiva, 2014. p. 26

[3] FERRAJOLI, Luigi. Direito e Razão: Teoria do garantismo penal. Tradução Ana Paula Zomer Sica, Fauzi Hassan Choukr, Juarez Tavares e Luiz Flávio Gomes. 1ª ed. Revista dos Tribunais. São Paulo. 2002. p. 436.

Importa destacar o sentido de “verdade” adotado por Ferrajoli, o qual se aproxima mais das inferências indutivas da verdade científica e da verdade histórica. Trata da abordagem da verdade processual tomada por duas proposições, a fática e a jurídica. A verdade processual fática, por trazer a percepção de fatos passados, aproxima-se dos princípios que guiam a formulação da verdade histórica. A verdade processual jurídica, no entanto, traz o caráter classificatório dos fatos passados interpretado pela linguagem jurídica.

Enquanto a investigação histórica constrói suas conclusões a partir de fontes pré-existentes, na investigação judicial é possível ir além das fontes de convicção pré-existentes e então produzir novas fontes de prova, em momento posterior ao fato. A inclusão de testemunhas, perícias, interrogatórios, entre outras fontes de prova, na formação da conclusão sobre a inferência judicial, contribui para a formação da verdade processual fática, na medida em que tentam compensar as limitações da impossibilidade da observação direta sobre o fato, ou seja, são inacessíveis à experiência.

Isso significa adotar a verdade processual menos como uma tentativa de recriar um acontecimento pretérito, com o fim de “encontrar” uma tese perfeita e incontestável, e mais como a formulação, a partir de fatos comprovados do passado e de peças probatórias produzidas no presente, da tese que melhor executa a conexão causal entre esses fatores empíricos. O resultado é a criação de hipóteses com maior probabilidade lógica de obter comprovação jurisdicional. Sobre a disputa de hipóteses, explica Juarez Tavares:

> Todas as controvérsias judiciais fáticas podem ser concebidas, de modo ademais não diverso das científicas, como disputas entre hipóteses explicativas contraditórias - uma que inclui a tese da culpabilidade e a outra a da inocência do acusado mas ambas concordantes com as provas recolhidas. E a tarefa da investigação judicial, igualmente à de qualquer outro tipo de investigação ou explicação, é eliminar o dilema em favor da hipótese mais simples, dotada de maior capacidade explicativa e, sobretudo, compatível com o maior número de provas e conhecimentos adquiridos com anterioridade.[4]

[4] Ibidem. p. 43-45

Ademais, o entendimento comum sobre o princípio da verdade real, como um dos objetivos do processo penal, presta maior serventia unicamente ao processo penal de raiz inquisitorial. A crença de que é essencial angariar todo tipo de prova que possa ser trazida ao processo para se chegar à verdade absoluta nos autos acaba por transformar não só a figura do juiz em parte atuante[5], mas a figura do acusado deixa de sustentar os direitos fundamentais válidos a qualquer cidadão, é objetificado, e passa a compor os meios de prova dos autos[6]. Ou seja, a prova é colocada em patamar superior ao dos próprios atores processuais, desconfigurando seus papéis no sistema acusatório e, portanto, aproximando o processo do modelo inquisitorial.

O modelo acusatório configura então separadamente os papéis das três partes no processo. Importa destacar a realocação do juízo à estrita função de julgar, ou melhor dizendo, de ser convencido pela verdade processual. O modelo brasileiro, regido pela Constituição Federal de 1988, institui o modelo acusatório[7], dada a série de regras características desse modelo trazidas em sua maioria pelo artigo 5º (contraditório e ampla defesa, o devido processo legal, presunção de inocência, entre outros)[8]. Porém, com o Código de Processo Penal de 1941 que traz características de um Estado autoritário, ainda há procedimentos típicos do modelo inquisitório e, não obstante tais procedimentos interpretados como exceções ao sistema acusatório ou como indícios de um sistema misto[9], adotando postura mais crítica tal qual a esposada pelo jurista Aury Lopes Jr, o resultado da aplicação dos princípios acusatórios constitucionais ao sistema vigente do CPP/41 é evidentemente inquisidor[10].

E como bem complementa essa crítica de forma empírica, o Doutorando Rafael de Deus Garcia, em sua dissertação de mestrado, mostra que os princípios acusatórios servem apenas a uma retórica vazia, mesmo na fase processual, partindo da gestão da prova no inquérito policial. Em ações penais abertas por via do inquérito (aqui ele pesquisa as ações sobre crimes de drogas) o juízo faz a recepção automática das provas produzidas por esse instrumento, sendo este um meio de se perpetuar opressões históricas típicas da nossa sociedade. Por fim, o que se tem é um sistema com aparente racionalidade (um sistema prévio inquisitório e um sistema judicial acusatório), mas que pelo “jogo de cartas marcadas” serve apenas para a legitimação

---

[5] Art. 156, II, do CPP.

[6] JUNIOR, Salah Hassan Khaled; HASSAN, Salah.A busca da verdade no processo penal: para além da ambição inquisitorial. São Paulo: Atlas, 2013. p. 168-170.

[7] PACELLI, Eugênio. Curso de processo penal. 22ª ed. rev., atual. eampl. São Paulo: Atlas, 2018. p. 10-11.

[8] Art. 5º, *caput* eincisos I, XXXV, LIV, LXXIV, XXXVII, LIII, LV, LVI, LXII e LVII.

[9] CAPEZ, Fernando. Curso de processo penal. 25ª ed. São Paulo: Saraiva Educação, 2018. p. 75-77, 85.

[10] LOPES JR., Aury. Op. cit., p. 141-142.

tácita do poder de violência do soberano, inicialmente executado pelo descontrole sobre ações policiais e posteriormente validado pelo judiciário[11].

É essencial tomar essa perspectiva crítica sobre os papéis a que se prestam as tão mencionadas fases do nosso processo penal, ou seja, a fase pré-processual e a processual em si, como vertente ético-política fundante dos princípios constitucionais acusatórios norteadores dos procedimentos penais. O professor Aury propõe como razão fundante do processo penal sua instrumentalidade constitucional[12]. A instrumentalidade do processo traz em si o princípio da nullapoenasine judicio. Essa máxima traz duas características que são a razão de ser do processo penal.

A primeira, que o processo não configura uma pena em si, já que é o requisito para que se chegue à pena de fato. Portanto, quando o caso mostra a total desnecessidade de aplicação de uma pena, deve-se evitar o sofrimento gerado pela propositura de uma ação penal inútil. Nesse sentido está o dispositivo do art. 397 do CPP, trazido pela reforma penal de 2008, o qual admite a absolvição sumária do acusado quando certas circunstâncias jurídicas mostram a inadequação do provimento de uma sentença.

A segunda, que a pena a ser aplicada tem conteúdo imperativo ou de conduta proibida, cuja sanção é voltada ao poder de aplicação da pena pelo Estado. Daí a necessidade de submissão ao processo, para que nem mesmo a ação voluntária em consentimento do acusado por si só provoque a aplicação da reprovação. O autor também destaca que a instrumentalidade do processo não é limitada à finalidade única da pena, mas trata de cumprir a realização do projeto democrático insculpido na Constituição Federal. A garantia dos direitos fundamentais e sua plena eficácia são o conteúdo principal da instrumentalidade do processo penal, pois ainda que acusado e submetido à violência do rito judicial, a dignidade da pessoa humana não pode ser suspensa.

---

[11]GARCIA, Rafael de Deus. O uso da tecnologia e a atualização do modelo inquisitorial: gestão da prova e violação de direitos fundamentais na investigação policial na política de drogas. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília. Brasília, 2015. p. 45-52.

[12] LOPES JR., Aury; GLOECKNER, Ricardo Jacobsen. Investigação preliminar no processo penal. 6ª ed. rev., atual. eampl. São Paulo: Saraiva, 2014. p. 38-45.

2. PRIVACIDADE

A discussão sobre o que é o direito à privacidade está ligada diretamente à evolução das tecnologias da informação, que passaram por rápidos avanços desde o século XX. A expansão do uso da fotografia, da publicidade, do telefone e de outros aparatos tecnológicos impulsionou tanto agentes privados quanto entes públicos a fomentar o debate quanto ao direito à privacidade.

Inicialmente, o direito à privacidade estava atrelado diretamente ao direito de propriedade, uma interpretação individualista traduzida na expressão do *righttobeletalone*, ou o direito a ser deixado só, cunhada pelo *common law*. Ou seja, a vida privada possuía delimitação espacial e geográfica. Não cabia ao governo exercer qualquer tipo de controle ou vigilância em território privado.

Essa perspectiva chegou à Suprema Corte com o caso *Olmstead v. United States*[13]. As novas tecnologias de captura de áudio, como as citadas anteriormente, proporcionaram aos agentes de segurança novos meios de aprofundar uma investigação. Em *Olmstead v. United States* questionou-se a constitucionalidade desse tipo de vigilância eletrônica e, à época, não foi constatada violação à Quarta Emenda pela justificativa de que o governo não invadiu fisicamente a propriedade do réu, não se tratando, portanto, de uma "busca". Não obstante, sucessivos casos de escutas "clandestinas" promovidas por agentes de segurança do governo continuaram a causar controvérsias.

Em 1967 a Suprema Corte admitiu os autos do caso *Katz v. United States*, um marco para a jurisprudência, dado que trata da rejeição (*overruling*) da tese anterior definida em *Olmstead*. Em *Katz*, a Suprema Corte definiu que a Quarta Emenda protege pessoas, e não lugares (*The FourthAmendmentprotectspeople, notplaces*)[14]. Estabeleceu também o teste da expectativa razoável de privacidade (*reasonableexpectationofprivacytest*), que é usado para averiguar quando uma investigação promovida por ente do governo caracteriza uma "busca" sem mandado e viola a Quarta Emenda[15].

O teste elaborado pelo advogado do recorrente, Harvey Schneider, traz dois aspectos que devem ser esclarecidos em um caso para que seja constatada a violação da quarta emenda pelo agente governamental, o subjetivo e o objetivo. Schneider, em sua sustentação oral, destaca especificamente o parâmetro objetivo do teste, em que é

[13]Olmstead v. United States, 277 U.S. 438 (1928).

[14]Katz v. United States, 389 U.S. 347 (1967).

[15] WINN, Peter. Katz and the Origins of the Reasonable Expectation of Privacy Test. McGeorge L. Rev., 2009, 40: 1.

questionado se a situação descrita no caso suscita na sociedade uma expectativa comum de privacidade.

Já o aspecto subjetivo foi elucidado pelo *Justice*Harlan da Suprema Corte, em opinião concorrente à opinião da maioria. Refere-se à necessidade da pessoa mostrar que subjetivamente ela espera existir razoável privacidade sobre suas atividades ou objetos pessoais. Portanto, o aspecto subjetivo procura complementar a análise do aspecto objetivo, como se em um caso, apesar da existência objetiva da expectativa de privacidade, sob o aspecto subjetivo não há razoabilidade a ser demonstrada (pode servir o exemplo de uma mala despachada que, submetida a vistoria de cães farejadores, tem revelado o seu conteúdo, ou a pessoa que dentro de sua casa fala tão alto que é possível ser ouvida e gravada da rua).

Tanto o aspecto objetivo, pautado nas expectativas da sociedade sobre o "homem médio", quanto o aspecto subjetivo, que evidentemente vai ser diverso de pessoa para pessoa, conferem ao teste um aspecto muito flexível, quase genérico demais à primeira vista. Porém, essa se torna a virtude do teste, como explica Peter Winn, que o descreve como uma estrutura em que o debate sobre a expectativa razoável de privacidade pode se desenvolver[16]. Sendo uma ferramenta típica do *common law*, o teste deixa espaço para capturar os diferentes contextos e suas complexidades do que a sociedade intui sobre a privacidade. Se o testeoferecesse uma resposta objetiva sobre as questões legais da privacidade, sob a Quarta Emenda, este logo se tornaria obsoleto dada a natureza das nossas intuições sobre o assunto.

É possível perceber que, apesar de Katz ser tratado como uma virada de paradigma na jurisprudência da Suprema Corte, a vinculação da privacidade à ideia de propriedade se manteve, ou ao menos não foi completamente superada. É como se expandisse a ideia de privacidade da propriedade privada para outros aspectos da dignidade humana e, dada a sua complexidade, fontes legais que estão além da Quarta Emenda passam a protagonizar o debate sobre as expectativas de privacidade. Por meio de novas legislações tratando casos específicos em suas especificidades, a Suprema Corte evita cair na tautologia de buscar exceções legais quanto à admissibilidade de certas provas (*exclusionaryrule*) em casos anteriores[17].

No âmbito legislativo, onde diversos atores da sociedade encamparam o debate sobre a privacidade e a proteção de dados pessoais, é possível observar a evolução das leis específicas em sucessivas gerações. A partir da década de 70, a primeira geração das leis de proteção de dados pessoais surgiu como reação imediata ao processamento de dados tanto pelo governo, quanto por empresas privadas, e a união

[16] Ibidem, p. 12.

[17] Ibidem, p. 9.

e manutenção desses dados em grandes bancos centralizados. Europa e Estados Unidos merecem destaque na produção legislativa nesse campo. As normas de primeira geração priorizavam a descrição de procedimentos que bancos de dados deveriam adotar em prol da segurança dos dados pessoais , mas não apontavam mecanismos legais que amparavam a dignidade individual e privada . São exemplos as Leis do Estado alemão de Hesse (1970), Lei de Dados da Sué cia (1973), Estatuto de Proteção de Dados do Estado alemão de Rheinland -Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Nos EUA, o Fair CreditReportingAct (1970) e o PrivacyAct (1974)[18].

A descentralização dos bancos de dados em unidades menores de órgãos públicos e de agentes privados rapidamente mostrou que as normas procedimentais da primeira geração não cobriam as novas demandas em termos de proteção desses dados pessoais. A regulamentação procedimental de bancos de dados centrais perdeu eficácia com o surgimento de muitos bancos de dados menores e controlados por diversos agentes, o que então resultou na necessidade de estabelecer direitos de privacidade mais fortes, para que o indivíduo tenha maior controle de seus dados. Priorizando direitos sobre procedimentos, na segunda geração de normas de proteção de dados pessoais foi desenvolvida a ideia de eficácia do consentimento e da liberdade de escolha do cidadão, uma vez que o fornecimento dos dados pessoais é imprescindível para a manutenção de programas do Estado de Bem Estar, ao mesmo tempo emque o não fornecimento dos dados pode privar o indivíduo do acesso a bens sociais e do mercado de consumo[19].

As normas da terceira geração estabelecem o novo paradigma da proteção de dados com o entendimento do Tribunal Constitucional Alemão, que trouxe a ideia de "autodeterminação informativa"[20], no julgamento da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho", em 1982. Com base em normas que protegem o livre desenvolvimento da personalidade e a dignidade humana, o Tribunal chegou à conclusão que:

> o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo , na medida em que possibilita o armazenamento ilimitado de dados , bem como

[18] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. São Paulo: Saraiva, 2014. p. 38-39.

[19] Ibidem. p. 40-41.

[20] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 192-201.

> permite a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento.[21]

Há também a aproximação do indivíduo de todo o processamento dos dados, da coleta ao armazenamento.

A ampliação do acesso do cidadão a seus próprios dados, no entanto, exigia uma dedicação dispendiosa para que este conseguisse de fato controlar o fluxo e o uso de suas informações. A tecnologia evoluiu a ponto de ser quase impossível identificar o local onde estão armazenados os dados, já que os servidores são descentralizados. A eficácia da aquisição do consentimento do titular por vezes colocou em xeque a possibilidade de reparação por uma violação ao direito de privacidade.

A quarta geração das normas de privacidade tentaram fortalecer a política de compensação de danos causados por essas violações ("*no faultcompensation*"). Outra inovação das novas normas foi o reconhecimento de aspectos da subjetividade que não são disponíveis ao indivíduo e que devem ter proteção mais rígida, como é o caso dos dados pessoais sensíveis, os quais dizem respeito a características íntimas cujo tratamento informatizado pode acarretar a discriminação do cidadão, seja pela etnia, raça, religião e etc[22]. A partir da definição de alguns princípios, tais como a indisponibilidade de certos dados, o panorama das normas de proteção de dados pessoais passa a ser desenhado a partir de uma legislação geral que é complementada por normas setoriais[23]. A ampliação da proteção legal é traduzida na atenção diferenciada, dada a complexidade, para cada área específica de informatização.

Desde o célebre artigo de Warren e Brandeis que, muito a frente de seu tempo debate com profundidade os limites e soluções para a efetivação do direito à privacidade, a sociedade agoniza a dualidade tecnologia *versus* privacidade[24]. É certo que a privacidade carrega fluidez em sua definição, posto que atrelada a evoluções tecnológicas. Quando os autores definem que, dentro de um dos limites do direito à privacidade, o que é de interesse público não configura violação à privacidade, ainda assim há o receio sobre a difícil tarefa de determinar onde deve prevalecer o interesse comum e onde deve prevalecer a dignidade do indivíduo. Qualquer regra adotada deve,

---

[21] MENDES, Laura Schertel. Op. cit., p. 41-43.

[22] DONEDA, Danilo. Op.cit., p. 159-161.

[23] MENDES, Laura Schertel. Op. cit., p. 43 - 44.

[24] "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.", in: WARREN Samuel D.; BRANDEIS, Louis D. The Right to Privacy.Harvard Law Review, v. 4, n. 5, p. 193-220, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 20 mai. 2019, p. 195.

portanto, ter certa elasticidade para dar conta da variedade de circunstâncias apreciadas em cada caso[25].

Os autores concluem que a proteção da privacidade mostrou limitações a partir da ideia de proteção da propriedade. Com o uso de novas tecnologias, as violações acontecem sem o conhecimento ou a participação da parte lesada. Por essa razão, os direitos discutidos nos casos que suscitaram a proteção da privacidade não têm natureza contratual, mas são direitos oponíveis *erga omnes*. Dessa forma, a proteção do direito à privacidade deve ter fundamentos mais abrangentes, mas não no sentido de expandir o valor atribuído ao que épropriedade privada para, então, protegê-la. Trata da expansão da tutela pelo reconhecimento de um novo princípio, que consiste no direito à privacidade, para proteger as produções subjetivas da emoção e do intelecto humano[26].

No ordenamento brasileiro, a jurisprudência assimilou muito do entendimento internacional sobre o conceito de privacidade a partir da década de 90. A legislação mais antiga relacionada à proteção de dados pessoais é a Lei 9.507/97, que regula o habeas data. Com isso, um dos primeiros debates sobre privacidade na Suprema Corte Pátria deu-se em um recurso de habeas data, proposto em face do órgão de inteligência do governo da época, o SNI - Serviço Nacional de Informações. Apesar de resultar negado o pedido do impetrante, os Ministros trouxeram à luz conceitos importantes na elucidação do entendimento sobre a privacidade e a proteção de dados pessoais[27]. O Ministro Celso de Mello faz em seu voto a relação do direito ao acesso a informações do cidadão com o direito a autonomia individual e à preservação da intimidade. Já no voto do Ministro Sepúlveda Pertence é associado o habeas data ao acesso a uma ordem democrática transparente, a um direito material à privacidade[28].

Em 1995, o STJ encarou o debate sobre a privacidade sob a ótica do Código de Defesa do Consumidor, a Lei 8.078/90. O REsp 22.337-9/RS[29] discute o tema do prazo prescricional das ações de cobrança originando os registros no SPC, tratando especificamente do prazo para manutenção desse registro no banco de dados. Interpretando de forma inovadora o art 43, §1º do CDC, o Min Ruy Rosado vai além da comum relação da norma com vantagens econômicas para apontar o risco generalizado

[25]WARREN Samuel D.; BRANDEIS, Louis D.The Right to Privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890. p. 214-216.

[26] Ibidem. p. 211

[27] RHD 22, Relator(a): Min. Marco Aurélio, Tribunal Pleno, julgado em 19 de setembro de 1991, DJ 01-09-1995.

[28] MENDES, Laura Schertel. Op. cit., p. 130.

[29]REsp 22.337/RS, Rel. Ministro Ruy Rosado de Aguiar, Quarta Turma, julgado em 13 de fevereiro de 1995, DJ 20/03/1995.

aos cidadãos que a manutenção e processamento dessas bases de dados trazem, seja por agentes privados ou por agentes públicos. O julgado reconhece a vulnerabilidade do indivíduo frente ao grande volume de dados gerados por si e mantido por inúmeras entidades, o que significa um risco para a intimidade e a vida privada, valores com proteção constitucional no art. 5º, X, da CF/88. O acórdão também faz referência ao direito à autodeterminação informativa, conceito extraído do entendimento do Tribunal Constitucional Alemão em 1982.

Outro julgado que trouxe conceitos inovadores ao campo da privacidade de dados pessoais está no REsp 306.570/SP, de 2001. O Tribunal Superior reconheceu a necessidade de proteger os dados pessoais do réu, no caso, a informação sobre seu endereço atualizado, obtidos através de requisição ao Banco Central, com a justificativa de que esses dados não estavam resguardados pelo sigilo bancário. Ou seja, foi reconhecida a privacidade da informação detida pelo Banco Central de forma independente à proteção estabelecida pelo sigilo bancário, pois tais dados também não são públicos.

Em julgado mais recente, a 4ª Turma afirmou mais uma vez a mudança de paradigma no conceito de privacidade. O REsp 1.168.547/RJ[30] destacou como *"a evolução dos sistemas relacionados à informática"*, com a globalidade da distribuição de informações, dão ensejo a novas práticas que fogem da legalidade o que, no caso, trata do uso indevido de imagem em sítio eletrônico. Segue na ementa o novo conceito de privacidade (grifo nosso):

> 10. Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem.

É evidente a confirmação do novel entendimento do Tribunal pautado na autodeterminação informativa alemã, além do tratamento dado à tutela como direito fundamental à proteção dos dados pessoais, tomados da leitura dos incisos X e LXXII, da CF/88[31].

[30]REsp 1168547/RJ, Rel. Ministro Luis Felipe Salomão, Quarta Turma, julgado em 11 de maio de 2010, DJe 07/02/2011.

[31] MENDES, Laura Schertel.Op. cit., p. 133 - 140.

O direito fundamental à proteção de dados pessoais ganhou repercussão no âmbito legislativo, onde já se encontra tramitando a PEC 17/2019[32]. O projeto sugere a inclusão da proteção de dados pessoais entre os direitos fundamentais do cidadão e fixa a competência privativa da União para legislar sobre a matéria[33]. Seria adicionado o inciso XII-A ao art. 5º e o inciso XXX ao art. 22, respectivamente, da Constituição Federal.

De fato, o atual arcabouço legal para proteção da privacidade e de dados pessoais no Brasil é retirado de uma combinação de fundamentos constitucionais com normas ordinárias regulando relações especiais. A Constituição protege o acesso a dados por meio do direito à liberdade de expressão, do direito ao acesso à informação e à transparência, bem como viabiliza o instrumento do habeas data. Ademais, estabelece a inviolabilidade da vida privada, dos meios de comunicação telegráficos e telefônicos e da casa, ou propriedade privada, do indivíduo[34].

O habeas data foi instrumento de acesso a informação com função simbólica tão relevante quanto a prática. O habeas data surgiu não de uma necessidade de implementar um panorama legal para proteção da privacidade, mas da reação política da época com o fim da ditadura militar e a promulgação da constituição democrática de 88. Foi um meio de deixar claro que a população tinha direito ao acesso às informações que a ditadura militar havia acumulado[35].

Novos paradigmas sobre a proteção da privacidade e dos dados pessoais são adicionados ao ordenamento brasileiro com a edição de normas federais. O Código de Defesa do Consumidor, Lei 8.078/90, traz um arcabouço legal moderno para as demandas relacionadas a privacidade e proteção de dados pessoais, em um campo de atuação muito amplo, qual seja, das relações de consumo. É relevante a aplicação desse instrumento legal pela grande abrangência do conceito do que é o consumidor[36]. Com isto, o Código enseja a proteção de dados pessoais admitindo o direito do consumidor ao acesso a seus dados guardados em bancos de dados de prestadores de serviços, que os dados guardados sejam objetivos e claros, que o consumidor seja notificado sobre a guarda de dados pessoais negativos, que o consumidor tem o direito de corrigir ou exigir o cancelamento de dados imprecisos ou incorretos e que o prazo

[32] Disponível em <https://www.jb.com.br/pais/2019/05/1001112-ccj-do-senado-aprova-inclusao-da-protecao-de-dados-pessoais-como-direito-fundamental.html> Acesso em 27/05/2019.

[33] Parecer/relatório da CCJ. Disponível em <https://legis.senado.leg.br/sdleg-getter/documento?dm=7954439&ts=1558646438029&disposition=inline>.

[34] Artigo 5º, incisos IX, XIV, XXXIII, XXXIV, X, XII, LXXII; e artigo 220 da Constituição Federal de 1988.

[35] DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Springer Netherlands, p. 3-20, 2014. p. 5-6.

[36] Artigos 2º; 2º, §2º; 17 e 29, da Lei nº 8.078/90.

máximo para a manutenção de dados pessoais negativos é de 5 anos[37]. Na verdade, a aplicação do CDC é tão ampla que pode extrapolar as relações contratuais entre consumidor e fornecedor, sendo utilizado também para caracterizar as responsabilidades de proprietários de bases de dados que mantém dados de consumidores.

A lei do cadastro positivo, Lei 12.414/2011, também traz ferramentas para a proteção de dados do consumidor. Elaborada para regular bases de dados com informações e histórico de crédito dos consumidores, a norma apresenta regras que os detentores dos dados devem seguir, estabelece responsabilidades em caso de danos no manuseio dos dados pessoais e os direitos do sujeito que concedeu os dados. Mais uma vez, a Lei reforça o princípio de que o indivíduo deve ter controle sobre seus dados pessoais, tanto na criação quanto no uso do seu histórico de crédito. Além disso, há previsão expressa do direito ao pedido de revisão, pelo consumidor, de qualquer decisão tomada por meio automatizado[38]. Outra inovação trazida pela norma é a proibição de armazenamento de dados pessoais sensíveis, ou seja, aqueles referentes a etnia, informação genética, orientação sexual, política, e etc. A proibição visa evitar situações discriminatórias[39].

A Lei de Acesso à Informação, nº 12.527/2011, inova ao trazer o arcabouço legal de proteção de dados pessoais manuseados por entes públicos. A principal proteção movida por esta norma é a limitação do acesso de terceiros aos dados de particulares, com a permissão em apenas algumas exceções, casos estes elencados na lei[40]. A norma não apenas associa a proteção de dados pessoais à proteção da privacidade, mas também é associada ao exercício da liberdade individual, agregando assim mais uma garantia aos princípios da proteção de dados. Importa grifar, no entanto, que, quanto ao tratamento de dados pessoais sensíveis, não é dado tratamento diferenciado, com uma proteção mais elevada, como é citado na lei do cadastro positivo.

---

[37] Artigo 43 da Lei nº 8.078/90.

[38] DONEDA, Danilo; MENDES, Laura Schertel. Op. cit., p. 8-9.

[39] Artigo 3º, §3º, da Lei nº 12.414/2011.

[40] "Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais."

3. LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/18, tutela a proteção de dados de pessoas naturais, incluindo os dados em meio digital, com o objetivo de proteger direitos relacionados à privacidade, a autodeterminação informativa, liberdade de expressão e comunicação, a honra, imagem e intimidade, a dignidade e os direitos humanos (art. 2º).

A lei alcança situações em que há operações com dados pessoais, sendo o tratamento referente "a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art 5º, inciso X).

Já os dados pessoais são divididos em duas categorias, as quais recebem tutelas diferenciadas, que são os dados pessoais e os dados pessoais sensíveis. Dado pessoal é o dado da pessoa natural que permite identificá-la ou torná-la identificável (artigo 5º, inciso I). A Lei Geral adota o conceito expansionista de dados pessoais, como explica Bruno Bioni, por proteger aspectos que denotam a personalidade do titular dos dados e, assim, podem interferir no livre desenvolvimento da personalidade (art 2º, VII) do indivíduo[41]. Um exemplo é o uso demetadados, ou seja, dados que não permitem a identificação direta da pessoa, mas que, se confrontados com outros dados, permitem sua identificação.

Os dados pessoais sensíveis são gerados a partir de descrições mais profundas de elementos da personalidade do titular. O artigo 5º, inciso II fala em " origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Tais dados recebem tratamento diferenciado pela lei visto que podem acarretar situações discriminatórias. Nesse sentido, Bruno Bioni aponta:

> a proteção dos dados pessoais perpassa a própria tutela do princípio da isonomia, na medida em que é um instrumento de contenção às práticas discriminatórias. (...) Tal tutela jurídica procura assegurar que o titular dos dados pessoais possa se

[41] BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019, p.66-81.

> relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto.[42]

Esse regime especial de tutela dos dados sensíveis esteve presente na história da legislação de dados nos países europeus desde a Diretiva de Proteção de Dados de 1995 (Diretiva Europeia 95/46/CE)[43]. Hoje, a LGPD toma como influência evidente o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), que estabelece tutela muito restrita ao tratamento de dados sensíveis, pois a regra prevê a proibição do tratamento desse tipo de dado, mas elenca dez circunstâncias excepcionais para que seja permitido o processamento[44].

Já a LGPD parte da necessidade do consentimento do titular para realizar o tratamento de seus dados (art 5º, inciso XII; artigo 11, inciso I). Nas hipóteses em que se dispensa o consentimento, a norma considera a situação de vulnerabilidade do titular dos dados sensíveis e elege um rol taxativo de situações cujo tratamento é permitido (artigo 11, inciso II). Daí extrai o caráter consequencialista[45] da lei, pois vincula esse mesmo tratamento mais rígido a qualquer dado pessoal "que possa causar dano ao titular" (artigo 11, §1º), bem como em casos de dados anonimizados, ou seja, que a princípio desvinculam a identidade do titular ao dado,mas que são revertidos, desanonimizados, por meios razoáveis. Esse último pode ser exemplificado por casos em que é feita a coleta de dados comportamentais de forma anônima, mas com o uso de um algoritmo agregado a outra base de dados os titulares são reidentificados. Por outro lado, Laura Schertel fala em um "tratamento sensível dos dados, que é capaz de transformar dados inofensivos em informações potencialmente discriminatórias."[46].

O que talvez seja o ponto mais relevante da lei geral está na construção dos princípios aplicados em qualquer atividade de tratamento de dados pessoais. O artigo 6º traz dez incisos que incluem os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

---

[42] Ibidem, p. 84.

[43] DIRECTIVA 95/46/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 24 de Outubro de 1995. Artigo 8º. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>.

[44] REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. Artigo 9º (1) e (2). Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:32016R0679>.

[45] BIONI, Bruno Ricardo. Op. cit. p. 77-80.

[46] MENDES, Laura Schertel. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Diss. Dissertação (Mestrado em Direito)–Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 63-64. Disponivel em <http://repositorio.unb.br/handle/10482/4782>, 2008.

Para o objetivo deste trabalho, importa explorar as aplicações dos princípios da finalidade e da não discriminação, pois o manuseio dos dados pessoais que não segue tais princípios pode significar a violação de fundamentos da norma que extrapolam o âmbito da legislação ordinária. Segundo alguns autores já explorados neste capítulo e em momentos anteriores, além do próprio tom das discussões acerca do novel instrumento normativo, bem como o fato de estar em tramitação a PEC 17/2019 para adicionar a proteção dos dados pessoais ao rol do artigo 5º da CF/88, é possível vislumbrar implicações constitucionais à resolução de demandas criadas pelo uso de novas tecnologias de captação de dados.

O princípio da finalidade exige que o tratamento de dados tenha um objetivo específico e legítimo, previamente informado ao titular dos dados. Dessa forma, o dado coletado é vinculado ao propósito informado, o que acaba por restringir seu uso por terceiros e impede abusos, como afirma Danilo Doneda, "este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade"[47].

O princípio da não discriminação impede o uso de dados pessoais para fins discriminatórios, abusivos ou ilícitos. Este princípio vem a tutelar principalmente os fundamentos defendidos no artigo 2º, inciso VII da Lei Geral. Laura Schertel apresenta o que hoje seria o princípio da não discriminação como um princípio da dimensão da igualdade e da liberdade. O grande avanço de tecnologias de processamento de dados em escala massiva, por organismos públicos e privados, colocaram o indivíduo em posição vulnerável quanto ao uso de seus dados. O que pode ser caracterizado como um estado de vigilância tem o potencial de discriminar e classificar os indivíduos. Segundo Laura, esse problema pode estar além da ótica da privacidade e requer seja estudado a partir da concepção de "vigilância"[48].

A vigilância na sociedade da informação é caracterizada pelo modo rotineiro em que ocorrem a coleta e manuseio de dados pessoais, catapultada pelo uso de tecnologias extremamente modernas capazes de perfilar o indivíduo com precisão. Daí que a partir desse ponto, "nota-se a necessidade de que a tutela jurídica dos dados pessoais abranja também a proteção da igualdade dos cidadãos e não apenas a sua liberdade, como ocorreu majoritariamente nas primeiras normas de proteção de dados. Para tanto, a proteção de dados pessoais deve ser apta a combater a discriminação passível de ocorrer em razão das informações extraídas dos bancos de dados,

---

[47] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 216-217.

[48] MENDES, Laura Schertel. Op. cit. p. 40-62.

buscando fornecer uma tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias."[49]

Desse modo, é possível extrair do ordenamento brasileiro o direito à proteção de dados pessoais como um direito fundamental autônomo. Tal interpretação não decorre apenas de uma análise dos riscos que o manuseio dos dados oferecem a garantias fundamentais da dignidade, liberdade e da intimidade, mas também importa considerar que há uma tendência a padronização normativa da proteção de dados pessoais em escala internacional[50]. Danilo Doneda sintetiza o "núcleo comum" de princípios que norteiam várias normas de proteção de dados pessoais. São eles o princípio da publicidade, da exatidão, da finalidade, do livre acesso e da segurança física e lógica. Suas nomenclaturas variam de ordenamento para ordenamento e suas interpretações podem ser adaptadas, mas "A aplicação de tais princípios, no entanto, é a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental em diversos ordenamentos."[51].

Ainda que não previsto na constituição, a proteção à intimidade (art 5º, inciso X), o direito à informação (art 5º, inciso XIV), o direito ao sigilo de comunicações telefônicas ou telemáticas (art 5º, inciso XII) e o habeas data (art 5º, inciso LXXII) formam uma estrutura de garantias fundamentais com as mesmas finalidades da proteção de dados pessoais. Na verdade é possível encontrar menção direta à proteção fundamental dos dados na Declaração de Santa Cruz de La Sierra, no item 45 do documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo Brasil em novembro de 2003[52].

Com esses instrumentos normativos, a leitura constitucional esteve estagnada em dicotomias rígidas sobre as informações: se são públicas ou particulares, se há sigilo ou não sobre a comunicação. Foi o entendimento emitido pelo Supremo no julgamento RE 418.416/2006, de relatoria do Ministro Sepúlveda Pertence, o qual estabeleceu que a proteção no artigo 5º, XII, é restrito à comunicação ("(...) é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das

[49] MENDES, Laura Schertel. Op. cit. p. 59.

[50] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journalof Law [EJJL], 2011, 12.2: 91-108. p. 98-102.

[51] Ibidem. p. 101.

[52] XIII CumbreIberoamericana de Jefes de Estado y de GobiernoDeclaración de Santa Cruz de laSierra. "45. Asimismo somos conscientes de que laprotección de datospersonales es underecho fundamental de las personas y destacamos laimportancia de las iniciativas regulatoriasiberoamericanas para proteger laprivacidad de losciudadanoscontenidasenlaDeclaración de La Antigua por la que se crealaRedIberoamericana de Protección de Datos, abierta a todos los países de nuestraComunidad.". Disponível em <https://www.oei.es/historico/xiiicumbredec.htm>.

comunicações telefônicas (...)") e, portanto, não se refere a proteção de dados armazenados. Nesse sentido, segue trecho da ementa:

> 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador.[53]

Esse entendimento relaciona a inviolabilidade do sigilo a uma liberdade negativa, a qual se limita a excluir a interferência de terceiros sobre a tutela. O caso tratava da apreensão de computadores que estariam sujeitos a alguma proteção constitucional atribuída aos dados, necessitando, assim, de mandado judicial para o acesso a estes, guardados em mídias físicas. Resultou consolidado que o maior risco para o cidadão é a comunicação dos dados, e não o mero armazenamento. A leitura binária de casos que suscitam a proteção da privacidade, constitucionalmente protegida, e da proteção dos dados pessoais ignora por completo a complexidade com que a tecnologia informacional tem alterado o tecido social, ou seja,

> apenas sob o paradigma da interceptação, da escuta, do grampo – situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias – não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.[54]

O Marco Civil da Internet, Lei nº 12.695/14, por exemplo, altera um pouco essa interpretação engessada sobre o meio digital, pois admite que não há exatamente uma separação entre o ambiente de armazenamento e de comunicação de dados[55].

---

[53] RE 418416, Relator(a): Min. Sepúlveda Pertence, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006.

[54] DONEDA, Danilo. Op. cit. p. 106.

[55]"Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma

E finalmente, no julgamento do RE 673.707/MG, com Relatoria do Ministro Luiz Fux, houve uma pequena mudança nesse entendimento. O Recurso é referente a um pedido de habeas data para que seja concedido acesso aos dados tributários do recorrente, que não estão sob sigilo, e cujo pedido foi feito por si próprio. Por unanimidade e nos termos do voto do relator, resultou entendimento com conceito mais amplo sobre os bancos e registros de dados associados aos dados pessoais e à autodeterminação informativa. Feita interpretação conforme da Lei nº 9.507/97, que regula o habeas data, foi assegurado ao titular dos dados, o contribuinte, o direito ao acesso a informações que lhe dizem respeito, em sistema informatizado público, ampliando o alcance desse acesso para outros ambientes informatizados dado que a finalidade do habeas data é o conhecimento das informações que se referem à personalidade do indivíduo[56]. Esse julgamento pode mostrar que o ordenamento está disposto a abraçar a estrutura principiológica e o debate propostos pela nova Lei Geral no âmbito constitucional.Nesse sentido, os seguintes trechos do voto do Relator (grifo nosso):

> A indigitada norma não tem por objetivo negar a seu próprio titular o conhecimento das informações que a seu respeito estejam cadastradas junto às entidades depositárias. Pretende, na verdade, restringir a divulgação a outros órgãos, que não o detentor das informações, ou a terceiros, que não o titular dos dados registrados, porquanto não tem o condão de restringir o direito postulado. Com efeito, a restrição que contém o parágrafo único do artigo 1º da Lei nº 9.507/97 deve ser interpretada em consonância com o supracitado artigo 5º, inciso LXXII da CRFB/88.
>
> (...)
>
> Encarta-se, assim, no conceito mais amplo de arquivos, bancos ou registro de dados, que devem ser entendidos em seu sentido mais lato, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto. (p. 4-5).

---

da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;" e "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.".

[56] RE 673707/MG, Relator(a): Min. Luiz Fux, Tribunal Pleno, julgado em 17 de junho de 2015.

O habeas data carrega em si o peso constitucional do direito ao acesso. Regulamentado pela Lei 9.507/97, *"A ação de habeas data visa a assegurar um direito presente em nosso ordenamento jurídico, ainda que não expresso literalmente."*[57], o cidadão tem acesso e poder de alterar seus dados em bancos de dados do governo ou com mero caráter público. Alvo de críticas pela falta de eficácia da ação, pela necessidade de ser interposta por advogado e por demandar prévio requerimento administrativo ao ente administrador dos dados, o voto do Ministro Relator no RE 673.707/MG traz inovações importantes para o futuro do habeas data. A expansão da sua eficácia para um direito positivo, não apenas negativo, torna material o direito à proteção de dados pessoais, além da dispensa de negativa de fornecimento dos dados pelo administrador[58]. Cabe ressaltar outro trecho do voto (grifo nosso):

> Por outro lado, o argumento da União no sentido de que existiria falta de interesse de agir, já que as informações solicitadas pela impetrante são as mesmas já repassadas pelo recorrente ao Fisco, não se sustenta.
>
> Na atual sociedade de risco, os contribuintes estão submetidos a uma imensa gama de obrigações tributárias principais e acessórias, que implicam no pagamento de diversos tributos e o preenchimento de diversas declarações, o que, por si só, já seria suficiente para permitir o acesso a todos os sistemas de apoio à arrecadação, de forma a permitir um melhor controle dos pagamentos e do cumprimento destas obrigações principais e acessórias (TORRES, Ricardo Lobo. Legalidade Tributária e Riscos Sociais. Revista de Direito da Procuradoria Geral do Estado do Rio de Janeiro, nº 53, pp. 178/198). (p. 12).

Daí que não faz sentido a garantia processual do habeas data não proporcionar o direito material, equivalente a tutela da proteção de dados, à autodeterminação informativa. Esse direito não pode mais ser concebido como direito negativo, posto que promove um dever de proteção do Estado, um direito positivo.

Importa ressaltar neste trabalho os princípios e fundamentos trazidos pela LGPD exatamente para proporcionar uma estrutura legal que proteja garantias fundamentais em qualquer ambiente de fluxo de dados que os avanços tecnológicos da sociedade da

[57] DONEDA, Danilo. Op. cit. p. 104.

[58] RE 673707/MG, Relator(a): Min. Luiz Fux, Tribunal Pleno, julgado em 17 de junho de 2015.

informação venham nos apresentar. Porém, a Lei Geral prevê exceções a sua aplicação, estabelecidas no artigo 4º. São elas quando o tratamento de dados é "realizado por pessoa natural para fins exclusivamente particulares e não econômicos;", "realizado para fins exclusivamente jornalísticos e artísticos, ou acadêmicos;", "realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;", ou "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei."[59].

Algumas remissões feitas pelos parágrafos do citado artigo merecem destaque. O §1º indica a necessidade de formulação de legislação específica para regulamentar o tratamento de dados previsto no inciso III, ou seja, os tratamento de dados feitos para a segurança pública, defesa e atividades de investigação e repressão de infrações penais. Não obstante a excepcionalidade, ainda é exigido que se observe o devido processo legal, os direitos do titular e os princípios elencados pela própria Lei Geral.

Dessa forma, é de se esperar ao menos o mesmo rigor na proteção de dados pessoais no contexto da gestão da segurança pública ou quando em sua devida admissão probatória ao processo penal. Soma-se a isso o mencionado tom de garantia constitucional que os princípios da proteção de dados pessoais tem tomado nos debates acadêmicos, na produção legislativa e na evolução da jurisprudência, a legislação hipotética deve "visar a um tratamento limitado desses dados, para evitar o seu eventual uso para propósitos que não atendam aos fundamentos republicanos do Estado Democrático de Direito."[60].

[59] Lei nº 13.709/2018. Artigo 4º, incisos I, II, III e IV.

[60] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, 2018, 19.3: 159-180. p. 163.

4.VIGILÂNCIA E DESAFIOS

O aparente conflito entre privacidade e tecnologia é outro ponto que merece esclarecimentos que vão além da simples binaridade. Como foi explanado em capítulo anterior, o termo “privacidade” sempre esteve em disputa e por muitas décadas foi atribuído a novos valores. Quanto a “tecnologia”, dada a velocidade com que se inova e a complexidade técnica à qual é atribuída, o termo também carrega nuances as quais faltam esclarecimentos. Muito do uso da tecnologia mudou com o advento de grandes avanços em um relativamente curto intervalo de tempo, levando de conexões feitas por internet discada à tecnologia 5G, de câmeras limitadas a rolos de filme a imagens em altíssima definição com armazenamento em nuvem, da busca manual entre arquivos em bases de dados ao uso de inteligência artificial para tal.

A sensação de estar em meio ao constante aprimoramento de nossas ferramentas nos faz acreditar quase sempre que, além de inevitável, o futuro servirá sempre ao bem da sociedade. Mas o que a história nos mostra é o contrário. A tecnologia sempre serviu, mais expressivamente, a uns indivíduos, ou entidades, ou governos, para estabelecer certo controle sobre outros indivíduos. E nessa guerra pelo controle, a privacidade sempre foi alvo crucial de investidas tecnológicas[61].

Garfinkel procura mostrar que por trás da tecnologia estão seres humanos que a criam e a projetam com o intuito de manter o controle sobre parcelas da sociedade, violando a privacidade desta. O autor ilustra como exemplo o argumento usado nas décadas de 50 e 60 em defesa de grandes corporações, justificando os enormes impactos ambientais que elas causavam como o preço a se pagar pela virtude do crescimento econômico. Hoje fala-se em crescimento econômico sustentável. Assim como o artigo publicado em 1890 por Warren e Brandeis[62], em que os autores se recusam a aceitar o fim da privacidade para que esta dê lugar à tecnologia, SimsonGarfinkel afirma que “a tecnologia não existe no vácuo” pois, na verdade, a tecnologia é regulada, ou deixa de ser regulamentada, conforme a sociedade entende suas prioridades sobre a ciência, o mercado, a política, entre outros aspectos[63].

O autor reforça a ideia de que a invasão da privacidade é uma escolha consciente dos operadores e desenvolvedores de tecnologias que agregam dados. Casos em que ocorreram violações da privacidade por empresas privadas e órgãos

[61] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. p. 31-62.

[62]WARREN, Samuel D.; BRANDEIS, Louis D.Right to privacy.Harv. Law Review, 1890, 4: 193.

[63] GARFINKEL, Simson. The Death of Privacy in the 21st Century. Cambridge: O’Riely, 2000. p. 15-16.

públicos mostram como a pressão pública pode ser um meio eficaz de forçar mudanças pelo processo político. E nesse sentido,Garfinkel destaca como, apesar de governos protagonizarem casos de grandes violações à privacidade dos cidadãos, é pela atuação do governo no processo de regulamentação que assim pode-se resultar em proteções mais robustas sobre a privacidade:

> Technology is not autonomous; it simply empowers choices made by government, business, and individuals. One of the big lessons of the environmental movement is that it's possible to shape these choices through the political process. This, I believe, justifies the involvement of government on the privacy question.[64]

Nos Estados Unidos, o poder bélico do governo com o uso de informações de civis é observado em momentos da história tais como os campos de concentração de japoneses, criados no início da Segunda Guerra Mundial, em território americano, onde foram mantidos 100.000 japoneses internados, a maioria sendo nativos dos Estados Unidos. Esse mapeamento de cidadãos japoneses só foi possível com o acesso aos dados do Departamento responsável pelo censo, sem mandado judicial, pois os tempos de guerra foram justificativa suficiente para a política discriminatória[65].

O FBI é outro exemplo emblemático de instituição que perpetrou abusos contra cidadãos usando seu robusto aparato tecnológico. A instituição justificou a necessidade de implementar devassas cada vez mais agressivas contra a privacidade dos indivíduos para combater o terrorismo e garantir a segurança do país. No entanto, nas décadas de 50, 60 e 70, movimentos sociais foram o grande alvo dessa tecnologia, o que resultou na perseguição a suspeitos de comunismo, homossexuais, integrantes de movimentos estudantis, movimentos feministas e negros. Dessa forma, a sociedade perdeu a confiança nas investidas tecnológicas da instituição, que utilizou da retórica do combate ao terrorismo para violar a privacidade dos cidadãos americanos e promover atos discriminatórios[66].

Esses exemplos deixam bem clara a posição do autor, pois há muitas referências na história que mostram o uso negativo da tecnologia, a qual tende sempre a violar a privacidade. Indica também como geralmente é mais complexo e mais caro produzir a tecnologia que proteja a privacidade dos indivíduos. Portanto não faz sentido acreditar em uma neutralidade inerente à tecnologia. Na verdade, o que é inerente à tecnologia é

[64] Ibidem. p. 21.

[65] Ibidem. p. 284.

[66] Ibidem. p. 285.

a capacidade de ser sempre mais intrusiva, pois está constantemente aprimorando técnicas de classificação e busca das informações[67].

De fato, um dos efeitos mais intrusivos permitidos pela tecnologia está na vigilância. E Garfinkel enquadra esse efeito em uma escolha, tanto social quanto no design, ou na técnica, desenvolvidos na tecnologia[68]. Ainda assim, é preciso esclarecer alguns aspectos sobre a vigilância, os quais são colocados em contraste no artigo de Christian Fuchs. Para o autor, de um lado está o conceito neutro de vigilância, de outro, o conceito negativo. O autor pretende destacar as diferenças entre as abordagens pelo bem da "controvérsia construtiva" do campo de estudo[69].

Partindo dos conceitos neutros de vigilância, é comum relacioná-la a uma categoria ontológica, como algo inerente às sociedades modernas. É fácil visualizar a naturalidade dessa vigilância quando a realização de censos periódicos da população se tornou ferramenta crucial para o regular funcionamento dos serviços públicos no Estado. Ou seja, um aspecto do conceito neutro de vigilância trata do mero acúmulo e processamento de dados sobre os cidadãos. Também partindo da ideia do censo, a vigilância funciona como um mal necessário para trazer benefícios às pessoas. Outro aspecto é pautado na sua universalidade, pois é fenômeno observável em todas as sociedades[70].

Já o conceito negativo de vigilância denuncia as estruturas de poder na sociedade. O acúmulo de dados sobre os cidadãos responde ao propósito de dominação, violência e coerção do dominador sobre a sociedade dominada. O autor explora principalmente a noção foucaultiana de vigilância, ou seja, "a vigilância é inerentemente coercitiva e dominadora - a negatividade é a pura imanência da vigilância."[71]. No centro do conceito está a ideia de vigilância do panóptico, onde o indivíduo vigiado está sempre visível, mas o poder controlador permanece invisível.

Apesar de algumas críticas quanto ao cabimento da perspectiva de Foucault para o estado da vigilância contemporânea, Fuchs salienta como o modelo do panóptico é relevante para a crítica da vigilância, já que de qualquer forma estabelece que a relação entre atores sociais é assimétrica quando temos os "atores poderosos", ou seja, os Estados e as empresas, os controladores da economia e da política, perante os indivíduos. É errônea a crença de que a descentralização das bases de dados, como consequência de evoluções tecnológicas, tenha democratizado o acesso à informação.

---

[67] Ibidem. p. 322-323.

[68] Ibidem. p. 141-143.

[69] FUCHS, Christian. Como podemos definir vigilância?.MATRIZes, 2011, 5.1: 109-136. p. 111.

[70] Ibidem. p. 112-114.

[71] Ibidem. p. 117.

Afirma: “Se entendermos que Foucault diz que os atores poderosos controlam o poder disciplinar, então a noção de uma vigilância centralizada e hierárquica ainda é válida.”[72]. De tal modo, o autor classifica a vigilância negativa como o acúmulo e processamento de dados de indivíduos para que o controlador esteja munido do poder de ameaça sobre comportamentos indesejados para discipliná-los[73].

Por fim, Christian Fuchs elege quatro razões para criticar os conceitos neutros sobre vigilância. Quanto ao valor etimológico da palavra, extrai-se a inerência da relação desta com a hierarquia, a dominação e a coerção. Quanto a confluência teórica dos conceitos neutros, o autor propõe a separação dos fenômenos que podem envolver desde o uso de tecnologias para o cuidado, muitas vezes ligado a serviços da medicina, dos relacionados à vigilância estatal, por exemplo. Para possibilitar a abordagem crítica sobre a vigilância, é preciso focar no entendimento das Ciências Sociais para que a crítica aos mecanismos poder faça sentido. Outro ponto eleito pelo autor é a necessidade de se diferenciar qualquer recuperação de informações, ou a sociedade da informação, dos padrões desiguais de poder inerentes à vigilância, ou a sociedade da vigilância. Sugere que a sociedade da vigilância seja uma disciplina diferente da sociedade da informação, esta, portanto, um conceito amplo, pois é fato que existem pontos positivos sobre as tecnologias da informação, mas os negativos se sobrepõem dadas as condições sociais heterônomas nas quais são inseridas. Por último, cogita negar a normatização do conceito de vigilância, porque se é normatizado é agregado um senso de neutralidade à violência perpetrada por sua forma repressiva. Se tudo é vigilância, a modalidade invasiva, coercitiva merece um campo apartado de estudo passível de críticas[74].

A partir destes conceitos desmistificados de tecnologia e vigilância, o direito é convocado a cumprir com seu papel máximo no ordenamento jurídico, ou seja, a proteção da pessoa humana. Novas tecnologias de vigilância estão sendo rapidamente inseridas no cotidiano das pessoas sem a devida avaliação dos seus efeitos em toda a complexidade das relações de poder que permeiam o tecido social. Uma das novas técnicas de vigilância ganhando popularidade nos últimos tempos é o reconhecimento facial, associado a procedimentos de inteligência, visando a segurança policial preventiva e preditiva, expandindo e interligando bases de dados[75].

No Brasil, tal tecnologia tem sido agregada a sistemas de vigilância com grande interesse por gestores públicos, testados principalmente em grandes eventos públicos.

---

[72] Ibidem. p. 121.

[73] Ibidem. p. 124.

[74] Ibidem. p. 125-128.

[75] SZABÓ, Ilona; RISSO, Melina. Segurança pública para virar o jogo. Zahar, 2018. Não paginado.

Os resultados dos projetos piloto de monitoramento, por enquanto, são resumidos a prisões de indivíduos reconhecidos pelo sistema de câmeras. Citando alguns exemplos nacionais, foi instalado um sistema de "videomonitoramento inteligente" para auxiliar o trabalho da polícia militar na festa de ano novo de Salvador, com um "recém-lançado software de reconhecimento facial", usando o banco de dados da Secretaria da Segurança Pública[76]. Em outro momento, as "câmeras inteligentes" chegaram a identificar um suspeito de homicídio com mandado de prisão em aberto frequentando bloco popular no carnaval de Salvador[77]. O sujeito foi abordado no meio da festa e preso. Já no carnaval do Rio de Janeiro, o sistema de monitoramento "cedido a custo zero" para a prefeitura identificou 8 mil pessoas na multidão de milhões de foliões, resultando em 10 prisões[78].

Comum aos sistemas testados em solo nacional é a sua origem. A tecnologia é chinesa, mas, no caso do Rio de Janeiro, o sistema foi cedido pela empresa de telecomunicações Oi. Como é possível observar nas reportagens, os agentes de segurança pública que estão implementando a tecnologia dizem, genericamente, que as bases de dados usadas para comparação dos perfis são da Polícia Civil e do Detran, e que buscam carros roubados e indivíduos foragidos da justiça. As imagens captadas são transmitidas em tempo real para o Centro Integrado de Comando e Controle (CICC) e então comparadas aos bancos de dados mencionados. Quando o sistema automatizado realiza uma correspondência, um alarme é soado no Centro e a imagem é congelada identificando o indivíduo suspeito. Daí é acionada a unidade mais próxima para realizar a abordagem e identificação.

A cidade de Curitiba merece destaque pelo ousado projeto de construção de uma "Muralha Digital"[79]. A ideia consiste em cercar a cidade com as "câmeras inteligentes", para reconhecimento facial e de placas de automóveis, adquiridas por meio de licitação internacional. O projeto também avança para sua segunda fase, cujo objetivo é integrar câmeras privadas no sistema unificado da Muralha, mediante

[76] Disponível em <http://www.ssp.ba.gov.br/2018/12/4933/Videomonitoramento-Inteligente-estreia-no-Reveillon-de-Salvador.html>. Acesso em 10 jun. 2019.

[77] Disponível em <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>. Acesso em 15 jun. 2019.

[78] Disponível em <https://tecnoblog.net/289696/rio-de-janeiro-identificou-8-mil-reconhecimento-facial/>. Acesso em 15 jun. 2019.

[79] Disponível em <https://www.gazetadopovo.com.br/politica/parana/de-olho-no-monitoramento-curitiba-muda-regras-para-a-instalacao-de-cameras-dqpfkx5asc5ugd2m49ysd8jni/>. Acesso em 16 jun. 2019.

permissão do proprietário do equipamento[80]. Tudo isso está regulado pela lei ordinária nº 15.405/2019, que cria a Política Municipal de Videomonitoramento de Curitiba[81].

Esses sistemas inteligentes de reconhecimento facial já são muito populares na China, sendo implementados em aeroportos como nova modalidade de check in e no metrô em algumas cidades para "facilitar" o pagamento das viagens[82]. O uso comercial do reconhecimento facial está associado ao sistema de crédito social, em que pessoas com boa pontuação sobre sua reputação recebem benefícios sociais e econômicos, enquanto aqueles que possuem baixa pontuação são penalizados e impedidos de acessar certos serviços, privados e públicos[83]. Integrado a este sistema estão milhões de câmeras segurança, espalhadas em grandes cidades e também em locais com algum interesse político ao governo chinês. Câmeras com reconhecimento facial em tempo real estão sendo implementadas ao equipamento de policiais, em proposta que parece ter saído de um filme futurista e distópico, possibilitando a identificação de qualquer pessoa na rua por meio de óculos inteligentes[84].

Todo o aparato tecnológico implementado com grande entusiasmo pelo governo chinês para expandir e aprofundar seu controle sobre a população tem sofrido críticas de ativistas pela proteção de dados pessoais, acadêmicos e jornalistas[85]. E pelo mundo, Estados democráticos que começam a implantar sistemas de vigilância por reconhecimento biométrico vivem notáveis dilemas sobre os limites do seu uso, a eficácia no combate a violência e os efeitos que a tecnologia gera sobre questões sociais complexas como a discriminação, o que é público ou privado, o papel da polícia, entre outras questões[86].

Nos Estados Unidos, alguns estados têm limitado o uso dessas tecnologias biométricas, ou estão até proibindo sua aplicação para as forças de segurança pública, dada a falta de regulamentação, bem como a falta de inclusão da sociedade no debate sobre a implantação ou não dessa forma de vigilância. A cidade de São Francisco, na Califórnia, foi a pioneira a banir o uso de softwares de reconhecimento facial pela polícia e outras agências de segurança. A Câmara de Supervisores de São Francisco

---

[80] Disponível em <https://www.gazetadopovo.com.br/politica/parana/cameras-que-reconhecem-rostos-e-veiculos-vigiarao-curitiba-em-seis-meses-8mvnjpamx62ffoo58si5b0p13/>. Acesso em 16 jun. 2019.

[81] Disponível em <https://leismunicipais.com.br/a2/pr/c/curitiba/lei-ordinaria/2019/1541/15405/lei-ordinaria-n-15405-2019-cria-e-define-a-politica-municipal-de-videomonitoramento-de-curitiba-e-da-outras-providencias>. Acesso em 16 jun. 2019.

[82] Disponível em <http://en.people.cn/n3/2019/0612/c90000-9586904.html>. Acesso em 13 jun. 2019.

[83] Disponível em <http://en.people.cn/n3/2019/0613/c90000-9587328.html>. Acesso em 13 jun. 2019.

[84] Disponível em <https://www.scmp.com/news/china/society/article/2132395/chinese-police-scan-suspects-using-facial-recognition-glasses>. Acesso em 10 jun. 2019.

[85] Disponível em <https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html>. Acesso em 10 jun. 2019.

[86] Disponível em <https://theintercept.com/2019/02/27/carnaval-cameras-rio/>. Acesso em 25 mai. 2019.

(equivalente a uma câmara legislativa local) votou pela proibição da tecnologia dado o imenso poder que ela pode dar ao governo sobre a vida privada dos cidadãos e principalmente pela falta de elaboração de política apropriada que a regule[87].

Outro caso interessante vem do Condado de Fairfax, na Virgínia, onde um juiz do Condado determinou o fim da manutenção de base de dados contendo fotos de placas de automóveis, pois o uso do sistema automatizado de reconhecimento de placas pela polícia do condado de Fairfax viola a lei de proteção de dados da Virgínia[88]. A decisão versa sobre o "uso passivo" dos dados pela polícia. A lei de proteção de dados da Virgínia não é aplicável a sistemas relacionados a controles criminais, investigações ou inteligência, mas o sistema ALPR (*AutomatedLicense Plate Reader*) usa "câmeras inteligentes" para registrar e verificar placas de carros em bases de dados e, então, os dados das placas ficam armazenados e disponíveis ao acesso das autoridades por 364 dias. Essa guarda dos dados é o chamado "uso passivo". O juiz entendeu, portanto, que os dados da placa do carro guardados pelo ALPR funcionam como um *link* para a identificação de dados pessoais em outros sistemas, locais ou federais, aos quais as autoridades têm fácil acesso, sem mandado judicial, e, se o titular dos dados é identificável através deste link, então trata de efetivo dado pessoal, como descrito pela lei de proteção de dados do estado[89].

É evidente que há muito a se questionar sobre o uso dessas novas tecnologias, que lidam com dados sensíveis, por agentes de segurança do Estado. Andrew Guthrie explora em seu livro *The Riseof Big Data Policing* muitos dos desafios identificados até então pelo uso de tecnologias envolvendo big data e inteligência artificial em políticas de segurança pública. O autor elege cinco questões fundamentais que todo administrador que pretende implantar qualquer sistema de policiamento usando novas tecnologias e big data deve responder, como forma de preservar direitos fundamentais, comumente violados por esses sistemas de vigilância.

A primeira questão trata da gestão do risco que a implantação da tecnologia representa com o manuseio de dados sensíveis por agentes de segurança. O autor defende que é preciso verificar as necessidades da comunidade para se implantar o sistema adequado, seja este um sistema de policiamento preditivo, de mapeamento de

---

[87] Disponível em <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>. Acesso em 26 mai. 2019.

[88] Disponível em <https://www.washingtonpost.com/crime-law/2019/04/02/judge-orders-fairfax-police-stop-collecting-data-license-plate-readers/?noredirect=on&utm_term=.e3dee884ee66>. Acesso em 12 mai. 2019.

[89] Disponível em <https://pt.scribd.com/document/404043069/FxLPRruling0419#from_embed>. Acesso em 12 mai. 2019.

áreas de risco, de câmeras de vigilância ou de aplicativos de cruzamento de dados para investigações ou redes de inteligência. Trata de uma escolha política[90].

O segundo ponto questiona a origem dos dados captados e armazenados no sistema de big data. Por exemplo, quanto a sistemas de vigilância, pode significar o local em que é instalada a câmera, quais informações ela deve identificar ou quais situações devem motivar a ativação de um alarme automático. São muitos os exemplos citados em que os dados coletados são enviesados, errôneos ou incompletos. Quando se fala em reconhecimento facial com ferramentas de inteligência artificial que fazem a correspondência entre a imagem captada e um banco de dados, o dado inserido nas bases de suspeitos, ou procurados pela justiça, ou de sujeitos com passagens pela polícia, vêm de uma sociedade que produziu esse dado viciado por meio de séculos de história escravista e de marginalização de minorias sociais. Se o banco de dados ao qual será comparado dada imagem possui maioria de registros de pessoas negras, então é de se esperar que o sistema de busca associe mais pessoas negras aos resultados suspeitos, levando em consideração que esses sistemas, quando testados, apresentam alta taxa de falsos positivos especialmente para o reconhecimento de pessoas negras. Ora, o algoritmo não apresenta soluções “neutras” quando tem o potencial de colocar em risco minorias que, por alguma razão, “falham” o sistema[91].

A terceira resposta deve esclarecer quais resultados são esperados com o uso da tecnologia. Trata-se de expectativa de redução nos índices de violência, se o objetivo é reduzir gastos com segurança ou se o objetivo está em tocar na confiança que a sociedade tem sobre a justiça e agentes de segurança. O autor alerta que o policiamento com o auxílio dessas novas tecnologias altera a forma como agentes de segurança vão interagir com os cidadãos e que índices puros sobre a violência podem mascarar problemas graves de relacionamento entre uma comunidade e a força do estado[92].

A quarta questão vai exigir do sistema a possibilidade de ocorrer auditoria, se o sistema é testável e se há mecanismos de *accountability*. Os problemas com dados viciados e discriminatórios podem ser esclarecidos e amenizados se a tecnologia permite que a sociedade realize testes e encontre meios de ajustar constantemente o sistema. A possibilidade de testar a tecnologia é mais importante que explicar “como” a tecnologia funciona ou “porque” ela funciona[93].

---

[90] FERGUSON, Andrew Guthrie. The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press, 2017. p. 191-193.

[91] Ibidem. p. 194-197.

[92] Ibidem. p. 197-199.

[93] Ibidem. p. 200-201.

O último fundamento considera os riscos à autonomia dos indivíduos perante os sistemas de vigilância em massa. Acreditar que a tecnologia vá orientar a resolução de problemas humanos, nesse caso a sua relação com crimes, a partir da redução de todo tipo de complexidade humana a números e estatísticas, processados e classificados por algoritmos, reduz as pessoas a meros objetos. E dessa forma, se os agentes estatais de segurança são cobrados a apresentar números para a sociedade, de prisões por exemplo, para justificar seu trabalho, as pessoas por trás desses dados têm sua autonomia anulada em nome dos dados. No aspecto legal, esse tipo de policiamento expande a categoria do suspeito para a total generalização, ou seja, não se trata mais de recair a suspeição sobre uma pessoa, mas sobre um grupo de pessoas. A suspeição generalizada não é admitida no processo penal e, no mais, gera provas viciadas de nulidade. No direito norte americano, significa violação à Quarta Emenda, por falta de motivação idônea para a suspeição individualizada. Além do mais, a suspeição generalizada reforça a produção da culpa por estereotipagem, fruto das discriminações sistêmicas produzidas pela sociedade. O autorreforça: "*Big data policing should not be used to ignore this past. Believing that technological promise can avoid human problems offers a false hope, because no new technology can turn the page on systemic societal problems.*"[94].

Os sistemas de reconhecimento biométrico e busca de dados por inteligência artificial usados no Brasil devem se submeter aos questionamentos da comunidade interessada, que permeiam os pontos elaborados por Andrew Guthrie. As autoridades devem esclarecer à população como essas novas tecnologias não violam direitos fundamentais e, para isso, o mínimo de transparência é exigível. O IDEC - Instituto Brasileiro de Defesa do Consumidor - tomou parte nessa tarefa enviando uma carta à Polícia Militar do Rio de Janeiro, pedindo esclarecimentos sobre a tecnologia utilizada no Carnaval. O documento pede respostas sobre aspectos da parceria realizada com a empresa Oi, que desenvolveu o software de reconhecimento facial, sobre a segurança da ferramenta e quanto ao funcionamento da tecnologia. Até então a PMERJ não respondeu[95].

É de suma importância que os sistemas implantados no país sejam submetidos a testes, os quais podem revelar tendências discriminatórias geradas pelos próprios algoritmos. Ainda que os algoritmos para buscas e cruzamentos de dados não sejam elaborados para reproduzir comportamentos discriminatórios, os dados inseridos neles são enviesados, o que pode resultar, por exemplo, em uma tecnologia de reconhecimento facial racista e sexista. Exemplo da necessidade da submeter esses

[94] Ibidem. p. 204.

[95] Disponível em <https://idec.org.br/sites/default/files/carta_idec_coex.pdf>. Acesso em 19 jun. 2019.

sistemas a testes de reconhecimento de diversidade fenotípica e de gênero é o estudo realizado por JoyBuolamwini e TimnitGebru, que testaram três relevantes sistemas de reconhecimento facial no mercado: da Microsoft, IBM e Face++. O projeto *GenderShades* demonstrou que homens e mulheres de pele mais escura estão sujeitos a maiores taxas de erros e de falsos positivos nos algoritmos de reconhecimento facial nos três sistemas, do que homens e mulheres de pele clara. A diferença na taxa de erros entre esses grupos chega a 19,2%. Mulheres de pele escura estão sujeitas a taxas de erro de 20,8% a 34,7%, enquanto homens de pele clara chegam ao máximo de 0,3% de erros no reconhecimento facial. O estudo também separa os resultados para falsos e verdadeiros positivos, mostrando a enorme diferença que há entre sujeitos de pele escura, com taxa de falsos positivos que passam de 20%, e de pele mais clara, que nos três sistemas apresentam resultados quase nulos[96].

Outro exemplo interessante da imprecisão de alguns sistemas de reconhecimento facial trata da tecnologia usada na Inglaterra, testada inicialmente na final da UEFA *ChampionsLeague* e posteriormente nas ruas em condições normais[97]. A polícia forneceu relatório com resultados dos testes feitos na ocasião do evento de futebol citado e impressiona a baixa precisão do sistema. Foram 2.470 alertas de possíveis suspeitos identificados, sendo apenas 173 corretamente identificados, ou seja, 2.297 falsos positivos e uma taxa de erro de 92%[98].

O uso de reconhecimento facial com auxílio de inteligência artificial e grandes bancos de dados é tecnologia que coloca em risco princípios fundamentais da proteção de dados pessoais, além de anular um dos pilares que compõem o entendimento contemporâneo sobre privacidade, ou seja, a noção de autodeterminação informativa, o que por si só atropelam os princípios do livre desenvolvimento da personalidade e da dignidade da pessoa humana. Na verdade, a tecnologia coloca em xeque qualquer entendimento sobre a privacidade e seus limites, dado que, ao presumir a suspeição de toda a população, e não sua inocência[99], submetida de forma automática à devassa da categoria criminalizadora do suspeito, aspectos da privacidade protegidos legalmente são suspensos.

Como bem foi abordado na Dissertação do Rafael de Deus, o sistema inquisitório com a admissibilidade automática de provas formam um sistema de “cartas marcadas”

---

[96]BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: Conference on Fairness, Accountability and Transparency. 2018. p. 77-91.

[97] Disponível em <https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>. Acesso em 20 jun. 2019.

[98] Disponível em <https://pt.scribd.com/document/377980664/South-Wales-Police?campaign=SkimbitLtd&ad_group=100796X1589915Xb4ad6971b6d92f7c0fdd0439e61e3a08&keyword=660149026&source=hp_affiliate&medium=affiliate>. Acesso em 20 jun. 2019.

[99]art. 5º, LVII, da CF/88.

que aniquilam a instrumentalidade constitucional do processo penal. E já que a tecnologia em estudo não é submetida a regulação alguma, até então, é possível que ela seja usada pela autoridade estatal em momento pré-inquérito, como verificação da procedência das informações, se escusando de qualquer forma de registro. Ora, se não são esclarecidas questões como quem terá acesso a esses registros biométricos, por quanto tempo ficarão armazenados ou se os dados podem ser transferidos para outros sistemas, em se tratando de dados sensíveis não submetidos a qualquer manifestação de consentimento, nem ao menos é dada atenção à exceção do §2º do art. 11, inciso II, da LGPD[100].

O apelo à racionalização das políticas de segurança pública e das práticas de seus agentes é assunto em alta entre acadêmicos e gestores. No livro "Segurança pública para virar o jogo", com prefácio do Ministro Luís Roberto Barroso, IlonaSzabó explora muitos dos graves problemas que permeiam a agenda da segurança pública nacional, tratando de violência, educação, armas, drogas, entre outros temas. E a partir da descrição didática desses problemas, propõe soluções. Com relação à polícia, no capítulo 4, boa parte das sugestões feitas pela autora passam pela necessidade de investir em inteligência, incluindo:

> Lançar mão de recursos tecnológicos para melhorar a efetividade do trabalho policial, aproximar policiais da população e diminuir o tempo de resposta das ocorrências criminais. Isso inclui o investimento em sistemas de análise criminal por georreferenciamento, câmeras corporais, aplicativos que facilitem denúncias e contato entre cidadãos e policiais, entre outros.[101]

De fato, investir em melhores ferramentas para elucidação de crimes violentos, estes principalmente, é solução que tem grandes chances de promover resultados positivos para a redução da violência. Mas importa destacar o risco que há no discurso

---

[100]"Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

(...)

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

(...)

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei."

[101] SZABÓ, Ilona; RISSO, Melina. Segurança pública para virar o jogo. Zahar, 2018. Não paginado.

acrítico de promoção da tecnologia como solução para antigos e conhecidos problemas sociais. A crença na operação automática, na resposta neutra e no "legalismo" dos procedimentos, tanto o tecnológico, quanto o penal, como afirma Rafael de Deus, servem a "conservação das formas de poder", onde quem detém o poder dita a verdade, por mais racional que esta aparenta ser[102].

No mais, a inteligência artificial aplicada ao reconhecimento biométrico automatizado, se adotado sob condições duvidosas com falta de transparência, não passaria de um "tirocínio policial", nos moldes da falta de critérios objetivos para o reconhecimento da fundada suspeita, reproduzido por equipamentos eletrônicos de alcance massivo. Dessa forma, *"o erro do tirocínio policial é um ato inexistente judicialmente. O ato não acaba sendo judicializado, não podendo afinal sofrer do escrutínio legal e constitucional acerca de sua validade, valendo-se por fim como mero instrumento repressor das agências penais no subterrâneo jurídico."*. O acerto, portanto, é a validação *a posteriori* da suspeita[103].

[102] GARCIA, Rafael de Deus. O uso da tecnologia e a atualização do modelo inquisitorial: gestão da prova e violação de direitos fundamentais na investigação policial na política de drogas. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília. Brasília, 2015. p. 45-52.

[103] Ibidem. p. 152-158.

5.CONCLUSÃO

Por todo o exposto, é possível perceber que o uso desregulado de novas tecnologias de reconhecimento biométrico para fins de segurança pública pode trazer riscos concretos de violações a direitos fundamentais, e que essas violações perpassam, de forma ainda mais grave, a atividade investigativa policial. Como bem destacado por Rafael de Deus, o jogo de “cartas marcadas” no momento da admissibilidade das provas produzidas no inquérito serve ao propósito de manutenção do mesmo discurso de poder que mantém, além do sistema que oprime desproporcionalmente as minorias sociais, mas também a política pública de encarceramento em massa.

Os riscos apresentados são claros nos resultados dos poucos testes realizados com essa nova tecnologia. Nenhum teste nesse sentido foi realizado nos sistemas implantados no Brasil, que aliás, até então, mostrou que as autoridades não estão dispostas a realizar o que autores como Andrew Guthrie elegem como práticas ideais na implantação e operação dos novos sistemas de vigilância. Entidades da sociedade, como o IDEC, tentaram obter o mínimo de transparência sobre a atividade, questionando a falta de *accountability* das autoridades, mas sem sucesso até o momento. Portanto não se sabe a taxa de precisão dos sistemas de reconhecimento facial utilizados até então, se estes apresentam disparidades de raça e gênero como os demonstrados no projeto de JoyBuolamwini, se as imagens capturadas estão armazenadas em uma base de dados, ou se estão em várias bases, por quanto tempo ficarão armazenadas ou quem terá acesso aos dados coletados. São inúmeros questionamentos sem resposta.

Em uma época que o fundamento da autodeterminação informativa é um dos mais importantes pilares do debate e da legislação sobre proteção de dados e o direito à proteção de dados pessoais é elevado à categoria constitucional de direito fundamental, o pouco caso feito pelas autoridades nacionais quanto ao uso de sistemas de vigilância que partem da devassa de dados pessoais sensíveis é um cenário preocupante. O uso “ativo” desses dados pode servir a violação sistemática da instrumentalidade constitucional do processo penal, como explanado por Aury Lopes, bem como o seu uso “passivo” que pode implicar em total falta de segurança jurídica aos indivíduos identificados pelo sistema de reconhecimento automatizado.

Estudos sérios têm demonstrado que alguns sistemas de reconhecimento biométrico estão sujeitos a altas taxas de erro, ou, na forma mais preocupante, altas taxas de falsos positivos. Um erro de identificação nessa magnitude pode desencadear

ato de intervenção policial com consequências desastrosas. E ainda que a intervenção policial desnecessária por si só trate de violação à intimidade, Andrew Guthrie destaca a dificuldade que o indivíduo encontra para provar o dano sofrido pelo uso errôneo de seus dados pela autoridade policial, dada a falta de transparência das instituições sobre os seus sistemas de vigilância:

> Individuals targeted because of police error will find it difficult to challengethe mistake, because currently the law makes it extremely hard to correctnegligent record-keeping errors.119 Worse, because of the secrecy of policedatabases, no independent auditing system exists to challenge their accuracy.The lack of transparency directly hindersattemptsataccountability.[104]

A instituição adota como padrão de verdade a presumida objetividade racional da tecnologia, distanciando o humano da persecução penal, tornando mais cômoda a transformação deste em mero objeto para compor a prova. A falta de transparência apenas reforça a presunção de racionalidade sobre a tecnologia. A auditoria desses sistemas pode revelar um instrumento tão falho quanto o humano.

Portanto é problemático ainda assim admitir que esteja extinta qualquer expectativa de privacidade, seja em ambiente público ou privado, em nome da expectativa de maior segurança.Se o sistema de reconhecimento biométrico tem a capacidade de registrar local, dia, hora e imagem de uma pessoa, atrelada a uma profundidade de dados pessoais sensíveis ainda não esclarecida, deve-se convocar a sociedade, e aqui a referência pode estar no poder legislativo, para apontar que nível de privacidade é esperado de forma geral, principalmente em ambientes públicos, tal como elucidado pelo advogado Harvey Schneider, pelo parâmetro objetivo do teste de expectativa razoável de privacidade.

[104]FERGUSON, Andrew Guthrie.Op cit. p. 62.

REFERÊNCIAS

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais - A Função e os Limites do Consentimento*. Rio de Janeiro: Forense, 2019.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: Intersectional accuracy disparities in commercial gender classification. In: *Conference on Fairness, Accountability and Transparency*, 2018, 81: 1-15.

CAPEZ, Fernando. *Curso de processo penal*. 25ª ed. São Paulo: Saraiva Educação, 2018.

DECLARAÇÃO de Santa Cruz de laSierra = DECLARACIÓN de Santa Cruz de laSierra. 14 e 15 de novembro de 2003. Disponível em <https://www.oei.es/historico/xiiicumbredec.htm>. Acesso em: 7 jun. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL]*, 2011, 12.2: 91-108.

_____. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. In: *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*. Springer Netherlands, p. 3-20, 2014.

ESTADOS UNIDOS DA AMÉRICA. Katz v. United States, 389 U.S. 347 (1967). Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/>. Acesso em 9 mai. 2019.

_____. Olmstead v. United States, 277 U.S. 438 (1928).Disponível em: <https://supreme.justia.com/cases/federal/us/277/438/>.

FERGUSON, Andrew Guthrie. *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press, 2017.

FERRAJOLI, Luigi. Direito e Razão: Teoria do garantismo penal. Tradução Ana Paula Zomer Sica, Fauzi Hassan Choukr, Juarez Tavares e Luiz Flávio Gomes. 1ª ed. *Revista dos Tribunais*. São Paulo. 2002.

FUCHS, Christian. Como podemos definir vigilância?.*MATRIZes*, 2011, 5.1: 109-136.

GARCIA, Rafael de Deus. O uso da tecnologia e a atualização do modelo inquisitorial: gestão da prova e violação de direitos fundamentais na investigação policial na política de drogas. *Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília*. Brasília, 2015.

GARFINKEL, Simson. *The Death of Privacy in the 21st Century*. Cambridge: O'Riely, 2000.

JUNIOR, Salah Hassan Khaled; HASSAN, Salah. *A busca da verdade no processo penal: para além da ambição inquisitorial*. São Paulo: Atlas, 2013.

LOPES JR., Aury. *Direito processual penal*. 11ª ed. São Paulo: Saraiva, 2014.

LOPES JR., Aury; GLOECKNER, Ricardo Jacobsen. *Investigação preliminar no processo penal*. 6ª ed. rev., atual. eampl. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*. São Paulo: Saraiva, 2014.

_____. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Diss. *Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília*, DF, 2008.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, 2018, 19.3: 159-180.

PACELLI, Eugênio. *Curso de processo penal*. 22ª ed. rev., atual. e ampl. São Paulo: Atlas, 2018.

SZABÓ, Ilona; RISSO, Melina. *Segurança pública para virar o jogo*. Rio de Janeiro: Zahar, 2018.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial das Comunidades Europeias*, 1995, 23. Disponível em <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 6 jun. 2019.

_____. Regulamento (UE) 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). *Jornal Oficial da União Europeia*, 2016, 3: 1-88. Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:32016R0679>. Acessoem: 5 jun. 2019.

WARREN Samuel D.; BRANDEIS, Louis D.The Right to Privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acessoem: 20 mai. 2019.

WINN, Peter. Katz and the Origins of the Reasonable Expectation of Privacy Test. *McGeorge Law Review*, 2009, 40: 1.