© ***Cadernos de Dereito Actual*** nº 20. Núm. Extraordinario (2023), pp. 221-245
·ISSN 2340-860X - ·ISSNe 2386-5229

A PROTEÇÃO DE DADOS NO BRASIL EM FACE DAS DEMANDAS DE SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL: LIMITES E POSSIBILIDADES

Data protection in Brazil in the face of public safety demands and criminal persecution: limits and possibilities

Rogério Gesta Leal[1]
Universidade de Santa Cruz do Sul

Resumo: O objetivo geral deste trabalho é o de avaliar em que medida a proteção de dados no Brasil em face de demandas de segurança pública e persecução penal está adequadamente equalizada nos termos do projeto de Lei que tramita no Congresso Nacional sobre a matéria. A questão que queremos problematizar é a de que esta proposta de legislação contempla parcialmente a relação entre proteção de dados pessoais no âmbito da persecução penal e da segurança pública, pois está constituída de alguns elementos paradoxais que podem ir de encontro aos escopos que busca alcançar. Em face deste problema, nossa hipótese é a de que importa revisar alguns dos termos deste projeto de lei, sob pena de criarmos situações inexequíveis de persecução penal e tutela da segurança pública, como vamos detalhar.

Palavras-chaves: Proteção de Dados – Segurança Pública – Persecução Penal – Lei de Proteção de Dados Penal.

Abstract: The general objective of this work is to evaluate the extent to which data protection in Brazil, in the face of public security demands and criminal prosecution, is adequately equalized under the terms of the law project that is being discussed in the National Congress on the matter. The issue we want to discuss is that this proposed legislation partially addresses the relation between personal data protection in the context of criminal prosecution and public safety, as it is made up of some paradoxical elements that may go against the scopes it seeks to achieve. In view of this problem, our hypothesis is that it is important to revise some of the terms of this law project, under penalty of creating unenforceable situations of criminal prosecution and protection of public security, as we will detail.

Keywords: Data Protection – Public Safety – Criminal Prosecution – Criminal Data Protection Law

1. INTRODUÇÃO

[1] Desembargador do Tribunal de Justiça do Estado do Rio Grande do Sul, junto a Quarta Câmara Criminal, com competência exclusiva para julgamento de crimes praticados contra a Administração Pública e os praticados por Prefeitos e Vereadores. Doutor em Direito. Professor Titular da UNISC e da FMP.

Recibido: 06/03/2023
Aceptado: 03/05/2023
DOI: 10.5281/zenodo.7919269

O objetivo geral deste trabalho é o de avaliar em que medida a proteção de dados no Brasil em face de demandas de segurança pública e persecução penal está adequadamente equalizada nos termos do projeto de Lei que tramita no Congresso Nacional sobre a matéria.

A questão que queremos problematizar é a de que esta proposta de legislação contempla parcialmente a relação entre proteção de dados pessoais no âmbito da persecução penal e da segurança pública, pois está constituída de alguns elementos paradoxais que podem ir de encontro aos escopos que busca alcançar.

Em face deste problema, nossa hipótese é a de que importa revisar alguns dos termos deste projeto de lei, sob pena de criarmos situações inexequíveis de persecução penal e tutela da segurança pública, como vamos detalhar.

Para tanto, elegemos desenvolver o debate a partir dos seguintes objetivos específicos: (i) demarcar aspectos matriciais da tutela de dados pessoais; (ii) avaliar alguns marcos regulatórios da proteção de dados no Brasil; (iii) estabelecer análise crítica dos deveres de proteção estatal de dados pessoais em sede de persecução penal e segurança pública no âmbito do Projeto de Lei de proteção de dados na esfera penal.

Pretendemos nos valer na pesquisa do método de abordagem dedutivo, testando nossas hipóteses com os fundamentos gerais a serem declinados e em face dos fins que visa este novo projeto de lei, nos valendo de técnicas bibliográficas fundamentalmente.

2. ASPECTOS MATRICIAIS DA TUTELA DE DADOS PESSOAIS

Já algum tempo tem se dito que a privacidade configura conceito extremamente vago e evanescente[2], razão pela qual tal categoria não pode ser compreendida como fórmula unitária, mas como constelação de direitos, de modo que seu núcleo constitutivo de situações subjetivas tampouco pode ser restrito a estruturas simples, mas compostas e articuladas.

Assim é que tal direito não se resume somente a inviolabilidade da esfera privada, enquanto projeção de indiferenciado interesse de estar só, pois nele ocorre notável metamorfose qualitativa que o orienta irreversivelmente para os fins de caracterizar-se como *poder de controle sobre a circulação de informações pessoais*. Este poder de controle tem, como fim primário, o de proteger e tutelar a dignidade da pessoa humana, nomeadamente sob a perspectiva de sua identidade pessoal, o que contempla o modo como determinado sujeito é apresentado e percebido aos olhos dos demais sujeitos, através do complexo de informações que lhe dizem respeito[3].

Ao mesmo tempo, esta identidade pessoal tem sido tomada como a projeção social da personalidade, não difamatória e desviante, como o direito a própria imagem social, entretanto, como bem refere Rodotà, *la stessa costruzione dell'identità fosse insidiata dalle nuove tecnologie e dalla loro capacità di influenzare modi di essere e comportamenti*[4].

Ou seja, através da criação de perfis de pessoas enquanto consumidores, e mesmo pelo modelo de endereçamento da produção comercial em face de específicos estereótipos de usuários criado para saciar desejos induzidos, está se favorecendo, em verdade, processos de homogeneização em massa de comportamentos individuais e sociais, muitas vezes alienantes e facilmente manipuláveis, os quais, por sua vez, geram etiquetamentos que tendem a prejudicar a possibilidade de

[2]Como querem: MILLER, A.R. & BERKMAN, B.A. *The assault on privacy, computers, data banks and dossier*, University Michigan Press, Michigan, 1971.
[3]Em total concordância com a tese sustentada por: NIGER, S. *Le nuove dimensioni della privacy: dal diritto alla riservatezza, alla protezione dei dati personali*, CEDAM, Padova, 2016.
[4]RODOTÀ, S. *Il mondo nella rete – quali i diritti, quali i vincoli*, Laterza, Roma, 2014.

autodeterminação individual e de favorecer exclusões de quem não deseja reconhecer-se em tal modelo hegemônico de tendências[5].

Desta forma, também a proteção de dados pessoais configura instrumento importante à recomposição da pessoa tomada a partir de informações fragmentadas de si, representando, pois, garantia de sua representação de forma integral. Estamos nos referindo a algo para além da auto representação; mas a verdadeiro mecanismo de tutela diante do reducionismo/perigo às distorções que comportam processos de relações (físicas e virtuais), sociais e institucionais, e sua consequente pulverização de identidades, nomeadamente em ambientes virtuais. Por isto Bonfanti esclarece que:

> *"secondo la dottrina internazionalistica, la figura statunitense della privacy è stato assunta, fuori dalla dimensione regionale europea, in varie fonti di diritto internazionale come una sorta di concetto sintetico che consente la protezione di vari aspetti della vita dell'individuo (dalla integrità fisica e mentale, dalla sua identità ed intimità, dagli orientamenti sessuali, dalle informazioni personali, la vita familiare, la casa la corrispondenza, l'onore, la reputazione). Valga per tutti l'indicazione dell'art.12, della Dichiarazione Universale dei Diritti dell'uomo del 1948: "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni"*[6].

E por certo que tudo isto se complexifica a partir das décadas de 1960 e 1970, com o progressivo avanço da informática, das relações virtuais e dos dados e informações que transitam e são armazenados cada vez mais sem controles, eis que as possibilidades de acesso, coleta, armazenamento e uso deles ocorre em quantidades e qualidades sem precedentes, tudo a exigir adequações à tutela de dados pessoais[7]. Por tais razões, *la riservatezza diventa il forte diritto di non perdere mai il potere di mantenere il pieno controllo sul proprio "corpo elettronico", distribuito in molteplici banche dati nei luoghi più diversi. Un diritto che si caratterizza ormai come componente essenziale della nuova cittadinanza, da intendere come fascio di poteri e doveri che appartengono ad ogni persona, e non più come il segno di un legame territoriale o di sangue*[8] [9]*.*

Estabelecidos estes elementos, é importante precisar que estamos na presença de bem jurídico suscetível de modificação no tempo, em face das mutações

---

[5]Daí porque para Rodotà, com o que concordamos, é a dignidade, a igualdade e a liberdade, as pilastras sobre as quais devemos articular os percursos evolutivos do direito à privacidade.

[6]Segundo o autor, este direito seria contemplado por várias fontes, como a Declaração Universal dos Direitos do Homem, de 1948, o Pacto Internacional dos Direitos Civis e Políticos, de 1966 e, sobretudo, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais - CEDH, de 1948, ainda fazendo referência a várias outras fontes de direito internacional. *In*: BONFANTI, M.E. "Il diritto alla protezione dei dati persinali nel Patto Internazionale sui Diritti Civil e Politici e nella Convenzione Europea del Diritti Umani: similitudini e difformità di contenuti*", Rivista Diritti Umani e Diritto Internazionale*, f.3, Franco Angeli, Roma, 2011, p. 439.

[7]Lembremos que os próprios *cookies* podem ser considerados dados pessoais na medida em que identificam o *browser* ou o dispositivo digital pelo qual as pessoas navegam pela rede virtual, pois mesmo que uma informação isolada não tenha o condão de portar a identificação de um individuo, ela pode ser utilizada para viabilizar, por cruzamentos múltiplos com outros dados, o acesso a dados pessoais específicos.

[8]RODOTÀ, S. *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973, p. 31.

[9]Lorenzo Picotti lembra, e com ele concordamos, que: il diritto alla riservatezza non è solo il diritto ad essere lasciati in pace, ma è anche e soprattutto il diritto a che nessuno possa utilizzare, a nessun titolo e per nessuna ragione, senza il necessario consenso, qualunque informazione. *In*: PICOTTI, L. *Il diritto penale dell'informatica nell'epoca di internet*, Cedam, Roma, 2005, p. 61.

de contextos históricos e sociais; da exigência dos ambientes interativos (individuais, sociais e institucionais) que impõem o reconhecimento da ductilidade dos conteúdos da privacidade. Dai porque ser difícil podermos constituir definições rígidas e absolutas ao direito de privacidade *ex ante* todas as condutas concretas e potencialmente lesivas a ela, tampouco construir casos de incriminação tão genéricos que passem ilesos com a mudança do tempo e daqueles contextos referidos.

A despeito disto, os debates internacionais sobre o tema conseguiram identificar um dúplice conteúdo mínimo ao direito de privacidade hoje: (i) enquanto liberdade negativa, que o enquadra como direito de manter reservados os próprios dados - direito ao segredo; (ii) enquanto liberdade positiva, como direito multifacetado de salvaguardar a identidade pessoal, de proteger dados pessoais - como direito de controle. Esta perspectiva dá vezo a nova definição de privacidade, passando-se de conceito estático, relativo ao mero segredo de informações referentes a esfera intima, e, portanto, atinente à proteção contra agressões a este patrimônio, para uma dimensão dinâmica, no sentido de ter sob controle todas as informações e dados que na moderna sociedade tecnológica em que vivemos circulam de modo sempre mais veloz[10]. Em outras palavras, esta dupla face da privacidade opera de modos concomitantes: pela reserva e pelo controle; a primeira, está associada ao silêncio; a segunda, à transparência.

Como a representação social do individuo passa muito também pela circulação de dados pela web, surge a necessidade de contarmos com certo tipo de *internet bill of rights*, pois cada vez mais impõem-se a necessidade de tutelarmos o que podemos chamar de corpo eletrônico, a identidade digital e a autodeterminação informativa. As pessoas cada vez mais são conhecidas através dos dados circulantes e virtuais que lhes são atribuídos por si próprias e por terceiros, criando verdadeira *existência relacional desencarnada*. Por conta disto as leis sobre tratamento de dados pessoais assumem hoje o papel de verdadeiros estatutos de proteção da pessoa em todas as suas dimensões, estendendo-se à tutela de qualquer informação referida ou referível a pessoa identificada ou identificável, seja qual for o seu conteúdo ou objeto.

Aliás, compreensão esta declinada pela Corte de Justiça da União Europeia, a partir do julgamento realizado pela Grande Sessão, no célebre caso *Maximilian Schrems v. Data Protection Commissioner*[11]*.* A Corte, entretanto, faz importante distinção envolvendo os bens jurídicos alcançados por sua legislação de dados, a saber: (i) enquadra o direito a privacidade como o relacionado aos espaços privados imunes a ingerências, (ii) enquanto que o direito a proteção de dados propriamente ditos como relacionados ao correto tratamento dos dados pessoais, independentemente do fato de serem dados privados. Neste ponto nos diz Lamanuzzi: *È lecito pertanto affermare che, il discrimen tra le due nozioni si rinviene nel bene oggetto di tutela, la sfera privata, che ha una portata esclusivamente individualistica, nel diritto alla privacy, e l'interesse generale alla correttezza e liceità del trattamento dei dati, nel diritto alla protezione dei dati personali, che ha la duplice natura di diritto dell'individuo e interesse della collettività*[12]*.*

E está correta a posição jurisprudencial sob enfoque, porque na sociedade hiper conectada como a nossa, com economia fundada sobre dados e alimentada por mecanismos de inteligência artificial, a confiabilidade e certeza de informações

[10]Sobre esta perspectiva ver as advertências que faz Taylor sobre os riscos de mantermos posturas estáticas diante da proteção de dados privados. *In*: TAYLOR, M. *Genetic data and the law – a critical perspective on privacy protection,* Cambridge University Press, New York, 2012.
[11]Ver o case *Maximilian Schrems v. Data Protection Commissioner*, realizado em 06/10/2015, C-362/14, *in*: EUR. *Maximilian Schrems v. Data Protection Commissioner,* disponível em*:* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362, acesso em 25/03/2023.
[12]LAMANUZZI, M. *Diritto penale e trattamento dei dati personali, Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*, disponível em: https://jus.vitaepensiero.it/news-papers-diritto-penale-e-trattamento-dei-dati-personali-codice-della-privacy-novita-introdotte-dal-regolamento-2016-679-ue-e-nuove-responsabilita-per-gli-en-4763.html, acesso em: 10/03/2023.

pessoais que se disponibilizam para fins de acesso são cruciais ao regular funcionamento de muitas outras relações – como as que se dão no mercado, por exemplo.

Nos Estados Unidos da América - EUA, por sua vez, desde o ensaio de Warren e Brandeis, em 1890, o tema da *privacy* sempre esteve na agenda de debates jurídicos daquele país[13] [14]. Neste texto os autores se utilizam de institutos do direito civil para configurar nova posição subjetiva correspondente às prerrogativas de posse ou propriedade que o individuo pode exercitar sobre seus bens materiais, mas agora sobre objeto diverso, de caráter imaterial, representado por certo tipo de esfera pessoal inviolável. Os fundamentos do direito privado utilizados aqui – e muito consolidados na experiência norte-americana – levam os autores a pressupor que a *common law* deve admitir a tutela desta dimensão personalíssima mais intima considerando o fato de que as prerrogativas dominiais reconhecidas pela legislação e jurisprudência ordinárias sobre os direitos dos autores e similares já apontavam para este caminho[15].

Certo que esta doutrina reclamou tempo de maturação para se ver refletida na casuística dos EUA, já que uma das primeiras Cortes Supremas Estaduais a lhe dar reconhecimento foi a da Georgia, 15 anos depois de sua elaboração[16] [17][18]. Mesmo assim, por longo tempo a jurisprudência em formação dava interpretação e aplicação diferenciada ao direito de privacidade, não oportunizando a constituição de diretrizes homogêneas às relações sociais e institucionais, isto praticamente até a segunda metade do século XX, concentrando-se os Tribunais a garantir a tutela de interesses privados genéricos reconhecidos de modo mais claro pela *common law* (como o *rigth to be let alone*), independentemente de questões relacionadas com a privacidade enquanto reserva propriamente dita[19] [20].

Hoje já podemos vislumbrar tratamento razoavelmente adequado e autônomo do tema da *privacy* (nos EUA) por parte dos Tribunais, tanto no que tange relações entre pessoas físicas e jurídicas com o setor público, como entre elas próprias, em face dos progressivos níveis de circulação de dados e informações diversos em ambientes físicos e virtuais.

---

[13]WARREN, S. & BRANDEIS, L.D. "The Right of Privacy", *Harvard Law Review*, vol.4, nº 5, December, 15, Boston, 1890, pp.193/220, disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf, acesso em: 08/03/2023.

[14]Ver também: LUGARESI, N. Internet, privacy e pubblici poteri negli Stati Uniti, Giuffrè, Bologna, 2000.

[15]E: AL-FEDAGHI, S.S. *The "right to be let alone" and private information*, *in*: CHEN CS., F. J; SERUCA I & CORDEIRO J. (eds), Enterprise Information Systems VII, Dordrecht, Springer, 2007, p. 157 e ss.

[16]Supreme Court of Georgia. *Pavesich V. New England Life Insurance Co*., 122 Ga. 190; 50 S.E., 68; 1905. Ga. Lexis 156. *In*: VLEX. *Pavesich V. New England Life Insurance Co*., disponível em: https://case-law.vlex.com/vid/pavesich-v-new-england-888103034, acesso em: 14/04/2023.

[17]Sobre a referencia acima, ver o excelente artigo de: ALLEN, A.L. "Natural Law, Slavery and the right to privacy tort", *Fordham Law Review*, vol.81, issue 3, 2013, p.1187 e ss, disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4854&context=flr, acesso em: 15/03/2023.

[18]A Corte de Apelo de New York, entretanto, em 1902, negou que o direito a privacidade tivesse colocação real na jurisprudência norte-americana, independente da doutrina de 1890, conforme se vê no caso *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902). *In:* Lexis News. *Roberson v. Rochester Folding Box Co, disponível em: https://www.lexisnexis.com/community/casebrief/p/casebrief-roberson-v-rochester-folding-box-co, acesso em: 13/04/2023*

[19]Ver o relato de Prosser fazendo este relato da jurisprudência. In: PROSSER, W.L. "Privacy", *California Law Review*, nº 3, vol. 48, august 1960, p.383 e ss.

[20]No mesmo sentido: PAGALLO, U. *La tutela della 'privacy' negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano, 2008.

Em tal perspectiva, também a Comunidade Europeia tem evoluído, eis que desde a primeira metade do século XX (1948), com a adoção da CEDH[21], houve o reconhecimento da necessidade de se ampliar o espectro de tutela da privacidade para além do seu significado negativo (*let to be alone*), basta vermos as disposições do art. 8º, deste documento, quando refere:

> *1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros[22].*

Veja-se que, na primeira disposição deste art. 8º, temos a imposição de *obrigação positiva* para todos – e à autoridade pública em especial – de reconhecer o direito ao respeito a vida privada e familiar da pessoa humana; na segunda, resta imposta à autoridade pública *obrigação negativa* de abster-se da violação da vida privada ou familiar desta mesma pessoa, *salvo* os casos previstos em lei envolvendo providência voltada a determinados escopos, dentre eles, o da segurança pública e prevenção de infrações penais. E estamos falando em quadra histórica na qual ainda inexistiam movimentos globais de violência e criminalidade – como o terrorismo – que fomentassem a revisão dos paradigmas de direito à privacidade (como o ocorrido no 11 de setembro de 2001, com os ataques as torres gemas em New York)[23].

Aqui temos já características particulares da proteção da privacidade na CEDH: a) a referência expressa à proteção da honra e da reputação presente na dimensão original dos EUA se vê ampliada para outros âmbitos; b) a interferência de autoridade pública é expressamente regulamentada; c) só são admitidas as intervenções públicas de âmbito pessoal que sejam exigidas por lei e que obedeçam a determinadas condições específicas. E tais avanços são importantes para dar caráter mais objetivo a proteção destes direitos e eventuais permissões excepcionais de ingerência nestes campos.

A mesma CEDH, nos anos vindouros, vai ampliando o âmbito do conceito de informação pessoal relevante a ser tutelada/alcançada pelas disposições do art. 8, da Convenção Europeia de Direitos Humanos - CEDU, a fins de alcançar a este titulo

---

[21]CEDH. *Declaración Universal de Derechos Humanos*, disponível em: https://www.derechoshumanos.net/normativa/normas/1948-DeclaracionUniversal.htm, acesso em: 13/04/2023

[22]Lembremos que o Conselho da Europa adota a Convenção nº 108 de 1981, como concretização deste art. 8º, em especial com foco na tutela de direitos relativos ao tratamento de dados pessoais. Mas mesmo este documento prevê em seu art. 9º, 2, que: *É possível derrogar as disposições dos artigos 5º, 6º e 8º da presente Convenção quando tal derrogação, prevista pela lei da Parte, constitua medida necessária numa sociedade democrática: a) Para proteccão da seguranca do Estado, da seguranca pública, para a proteccão dos interesses monetários do Estado ou para repressão das infrações penais; b) Para protecção do titular dos dados e dos direitos e liberdades de outrem*. *In*: COE. *Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal*, disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2,acesso em: 13/04/2023 (grifos nossos)

[23]Neste ponto ver a decisão da CEDH, no caso *Leander v. Sweden*, julgado em 1987, em que ratifica este entendimento de que o acesso e coleta de informações por parte dos órgãos de segurança pública, assim como a conservação destes, só é legitima se prevista por lei especifica precedente e desde que envolva interesse público superior de segurança nacional, o que se deu efetivamente neste caso. Com tal decisão a Corte estabelece critérios de permissibilidade de acesso e gestão de dados desta natureza conforme o art. 8, 2, da CEDU. *In*: OSCE. *Legislation Online*, disponível em: https://www.legislationline.org/download/id/3521/file/Case_of_Leander_v_Sweden_1987_en.pdf, acesso em: 29/03/2023.

imagens fotográficas, de vídeos, e mesmo dados acessados pela via de instrumentos de localização por satélite[24]. Inclusive tratando do direito de acesso a informação própria do postulante, a CEDH teve oportunidade de enfrentar, no caso *Gaskin v. United King*, no ano de 1989[25], o pedido de determinado cidadão, negado pelo Reino Unido com base na legislação nacional, de ter acesso a seus dados próprios relativos ao período em que esteve sob os cuidados do serviço social de infância, para os fins específicos de conhecer quais as informações que existiam nos registros públicos sobre as condições em que viveu e os eventuais abusos a que fora submetido. A Corte entendeu que as normativas domésticas de proteção de dados sensíveis como estes tem fundamento justificável, todavia, não podem impedir a pessoa própria a que estes dados se referem ter acesso a eles[26].

Em suma, as disposições da CEDH traçam as coordenadas fundamentais da proteção de dados pessoais na dimensão europeia, atribuindo novos caracteres à figura original da privacidade dos EUA, bem como demarca as linhas de desenvolvimento do futuro e, em parte, a produção contextual da legislação comunitária.

A jurisprudência CEDH indica que o tratamento de dados pessoais, nas suas diversas formas, representa dimensão em que se exerce o direito ao respeito pela vida pessoal. Correspondentemente e ao mesmo tempo, o tratamento de dados pode constituir caso de violação do mesmo direito. Em outras palavras, os dados pessoais e sua gestão não são mais, como no processamento original dos EUA, objeto de reclamação ou direito de *excludendi alios*, mas passam a constituir atividade que pode se tornar instrumento de prejuízo à pessoa humana, portanto, detecta a própria atividade de processamento e acesso, e não os dados pessoais, como objeto legal. Por isto a casuística tem formatado condições e possibilidades na presença dos quais o tratamento destes dados pode garantir o respeito pela vida pessoal do indivíduo, e o fazem bem.

Vejamos, a partir de agora, como o Brasil tem tratado destes temas, em especial no âmbito penal.

3. MARCOS REGULATÓRIOS DA PROTEÇÃO DE DADOS NO BRASIL – ASPECTOS GERAIS.

O tema da proteção de dados tem ingressado na agenda legislativa brasileira aos poucos – e antes tarde do que nunca –, implantando melhorias no tratamento de matéria tão sensível em todo o mundo, notadamente quando o vazamento e uso indevido de dados de pessoas físicas e jurídicas têm provocado tantos danos[27] [28], ao

[24]Conforme decisões da CEDH nos casos: (i) *PG.* e *J. H.* v. *United King*, de 25/09/2001, nº 44787/1998; (ii) *Peck* v. *United King*, de 08/07/2003, nº36022/1997; (iii) *Perry* v. *United King*, de 17/07/2003, nº63737/2000; (iv) *Uzun* v. *Germany*, de 02/09/2010, nº35623/2005. *In*: CEDH. *Case-law analysis*, disponível em: https://www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=, acesso em: 29/03/2023.

[25]ECHR. *Gaskin v. United King, disponível em:* https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695368%22],%22itemid%22:[%22001-57491%22]}, acesso em: 29/03/2023, *acesso em: 13/04/2023.*

[26]ECHR. *Case of Gaskin v. The United Kingdom*, *idem.*

[27]Basta vermos o vazamento de dados pessoais por conta da invasão da rede PSN da Sony, em 2011; o vazamento de dados do site de relacionamentos Ashley Madison; dados pessoais de 553 milhões de pessoas foram recentemente expostos em nova notícia de vazamento envolvendo o Facebook, dos quais 8 milhões de brasileiros teriam sido afetados conforme noticia em: UOL. *Vazamento do facebook*: descubra se seus dados foram expostos, disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/04/05/vazamento-do-facebook-descubra-se-seus-dados-foram-expostos.htm, acesso em: 08/04/2023.

[28]A revista Exame, em matéria publicada no dia 08/06/2021, dá conta de que: *o maior vazamento de senhas da história pode ter exposto 8,4 bilhões de senhas de serviços digitais. Um arquivo foi publicado em um fórum de hackers contendo os dados. Em referência ao vazamento de 32 milhões de senhas em 2009, o RockYou, o novo caso vem sendo chamado*

mesmo tempo que alimenta políticas agressivas de segmentos do mercado que acessam perfis de consumidores cujos dados, obtidos sem a devida autorização, servem de base para estratégias de criação de novos produtos, marketing, publicidade e propaganda.

Por conta disto foi editada a Lei nº 12.965/2014[29] no país, que trata sobre a proteção de dados pessoais (de pessoas físicas e jurídicas), nominada de Marco Civil da Internet, assim como as alterações necessárias que sofreu por parte da Lei nº13.709/2018 (Lei Geral de Proteção de Dados - LGPD)[30]. Esta normativa avançou na tutela destes bens jurídicos tão vulneráveis, demarcando de forma objetiva os que visa proteger (dado pessoal, dado pessoal sensível e dado anonimizado[31]), e as responsabilidades indenizatórias por prejuízos causados por acesso e manipulação destes bens (art.42, e ss, da LGPD[32]), bem como sanções administrativas pesadas

---

de "RockYou2021", de acordo com o site de segurança digital Cyber News*. As senhas contidas no arquivo de texto, que tem tamanho de 100 GB, têm entre seis e 20 caracteres*. *In*: EXAME. *Maior vazamento da história pode ter exposto 8 bilhões de senhas*, disponível em: https://exame.com/tecnologia/maior-vazamento-da-historia-pode-ter-exposto-8-bilhoes-de-senhas/, acesso em: 09/04/2023.

[29]BRASIL. *Lei nº 12.965 de 2014*, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acesso em: 12/04/2023.

[30]BRASIL. *Lei nº 13.709 de 2018*, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm, acesso em: 12/04/23.

[31]Artigo 5º - LGPD: "Para os fins desta Lei, considera-se: I – dado pessoal: informações relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre 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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (...)". *In*: BRASIL. *Lei nº 13.709 de 2018. Idem.*

[32]"Art 42 – LGPD: "O controle ou o operador que, e, razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. §4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso; Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro; Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano; Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente". *In*: BRASIL. *Lei nº 13.709 de 2018, Idem.*

aos agentes de tratamento de dados em face de infrações cometidas no particular (art.52, e seguintes, do mesmo diploma legal[33]).

Por certo que antes destes dispositivos contávamos com normas infraconstitucionais relacionadas à proteção de dados, inclusive penais, tais como a que trata do sigilo dos agentes do fisco no exercício de suas atividades, nos termos do art. 198, do Código Tributário Nacional[34]; a Lei nº 9.296/1996[35] e nº 10.217/2001[36], que versam sobre a interceptação telefônica e a gravação ambiental, bem como o Código de Defesa do Consumidor (Lei nº 8.078/1990[37]), quando fala sobre os bancos de dados nas relações de consumo. Mas não tínhamos regulação especifica sobre proteção de dados na esfera civil e penal.

O Brasil, todavia, optou, ao editar sua LGPD, por não tratar especificamente sobre questões associadas a aspectos penais; e o fez explicitamente, pelos termos do art. 4º, caput, inciso III, alíneas *a* e *d*, ao dizer que:

> *"O tratamento de dados pessoais previsto no inciso III [tratamento de dados realizado para fins de: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais] será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo*

---

[33]Art. 52 e ss – LGPD: "Artigo 52: Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); IX - (VETADO); X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção (...). In: *Lei nº 13.709 de 2018, Idem.*

[34]Art. 198 CTN: "Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades (...). *In*: BRASIL. *Código Tributário Nacional*, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm, acesso em: 13/04/2023.
[35]BRASIL. *Lei nº 9.296 de 1996*, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm, acesso em: 13/04/2023.
[36]BRASIL. *Lei nº 10.217 de 2001*, disponível em: https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10217.htm, acesso em: 13/04/2023.
[37]BRASIL. *Lei nº 8.078 de 1990*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm, acesso em: 13/04/2023.

> *legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei"*[38]

Por conta disto, foi constituída, pelo Congresso Nacional, comissão para elaborar proposta de regulamentação destes temas, coordenada pelo então ministro do Superior Tribunal de Justiça, Nefi Cordeiro, tendo sido entregue o projeto ao Parlamento no mês de novembro de 2020[39].

A aclaradora exposição de motivos deste projeto dá conta de que há grande lacuna legislativa existente no país sobre a matéria, destacando duas problemáticas centrais neste particular: (i) a que envolve a eficiência investigativa dos órgãos estatais nacionais, os quais, por não estarem adequados aos padrões internacionais de segurança quanto ao fluxo e tratamento de dados, inviabiliza, por vezes, a integração com órgãos de inteligência internacionais, obstando o próprio acesso a banco de dados e informações relevantes; (ii) a que diz respeito aos déficits de proteção dos cidadãos, visto que inexiste regulação geral sobre a ilicitude, a transparência, ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam grau de vigilância e monitoramento impensáveis há alguns anos[40].

Relata a exposição de motivos, portanto, que o projeto de lei visa *harmonizar, de um lado, os deveres do Estado na prevenção e na repressão de ilícitos criminais, protegendo a ordem pública; de outro, assegurar a observância das garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins*[41]*.*

Constam como inspirações enunciadas pela exposição de motivos do anteprojeto tanto a LGPD brasileira, em especial as disposições dos seus arts. 4º, §1º, 6º, 17 a 22[42] (arts. 6º, 18 a 28, do anteprojeto[43]); como a Diretiva 680/2016[44], da União Europeia, que regulamenta especialmente o tratamento de dados para fins de segurança pública e persecução penal, marco suplementar ao Regulamento 679/2016[45], que trata dos dados como um todo.

Pelos termos desta Diretiva 680/2016, os dados recolhidos para finalidade de prevenção podem ser transmitidos aos demais países europeus e, eventualmente, ao estrangeiro, eis que a respectiva autoridade judiciária e de policia garantem, no tratamento dos dados de todas as pessoas físicas, adequado nível de tutela que não viola o direito a *privacy*. Ao mesmo tempo o marco normativo exige que as autoridades de segurança pública, no exercício dos seus misteres, respeitem os termos estabelecidos, sob pena de configurar abuso de autoridade[46].

---

[38]BRASIL. *Lei nº 13.709 de 2018, Idem.*

[39]Conforme noticia no site da Câmara dos Deputados, e ao que consta, até março de 2023, nenhum andamento teve o projeto nesta casa. *In:* BRASIL. *Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações*, disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/, acesso em 06/04/2023.

[40]Sobre a exposição de motivos do projeto de lei da LGPD Penal. *In*: BRASIL. *Anteprojeto de lei de proteção de dados para segurança pública e persecução penal*, disponível em: https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf, acesso em: 05/04/2023.

[41]BRASIL. *Anteprojeto (...), Ob. Cit*., p. 02.

[42]BRASIL. *Lei nº 13.709 de 2018, Idem.*

[43]BRASIL. *Anteprojeto de lei de proteção (...), Idem.*

[44]EUR. *Diretivas*, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU, acesso em: 13/04/2023.

[45]EUR. *Regulamentos*, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679, acesso em: 13/04/2023.

[46]Lembremos que a própria CEDH, em 2008, no caso *Marper vs. U.K*., envolvendo tema de conservação de dados pessoais (impressões digitais e DNA) para fins de investigação e de repressão criminal, teve oportunidade de dizer que há certa margem de discricionariedade da autoridade nacional no que toca a considerações afetas a natureza do direito garantido, a gravidade da ingerência e dos objetivos perseguidos pela norma diante do caso. *In*: ECHR.

E de tais fundamentos podemos deduzir que o foco do anteprojeto não é normatizar situações permissivas de violação de dados por parte do Estado em nome da *segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais*, mas proteger os titulares destes dados da má utilização e uso desenfreado pelas autoridades, mesmo quando estão agindo pretensamente em nome destes bens jurídicos.

A título de mera exemplificação, até em face de que estamos tratando de projeto de lei que ainda deve contar com alterações propostas pelo processo legislativo regulamentar, e mesmo sedimentações jurisprudenciais e doutrinárias a posteriori, gostaríamos de apontar alguns cuidados, riscos e perigos que desde já a normativa apresenta, inclusive para contribuir a sua maturação e realçar a necessidade de formatação do que chamamos de cadeia de custódia de dados privados enquanto espécie de dever de proteção suficiente.

4. DEVERES DE PROTEÇÃO ESTATAL DE DADOS PESSOAIS EM SEDE DE PERSECUÇÃO PENAL

Tenhamos presente desde logo que a LGPD brasileira, e o projeto de Lei que passamos a avaliar versando sobre a LGPD no âmbito da segurança pública e persecução penal, serão aplicadas ao *tratamento de dados*, ora compreendido como qualquer operação ou conjunto de operações realizadas sobre dados pessoais ou banco de dados, com ou sem o auxílio de meios automatizados, tais como coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio, cancelamento, anonimização, pseudonimização e fornecimento a terceiros, por meio de transferência, comunicação, interconexão ou difusão, ou seja, todo o ciclo de vida do dado pessoal.

O projeto de lei sob comento define, portanto, e de modo coerente, que seu objeto é o *tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*[47].

A regra deste art.1º já deixa clara a pretensão do legislador, qual seja, a de atuar no sentido de regulamentar os *dados tratados* pelas autoridades em suas atividades persecutórias em todos os âmbitos investigativos, sejam os *pessoais* (informação relacionada a pessoa natural, identificada ou identificável); *pessoal sensível*[48] (sobre origem facial 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 dado biométrico, quando vinculado à pessoa natural, situação sócio-econômica)[49]; pessoal sigiloso[50] (protegido por sigilo

---

Case of S. and Marper v. The United Kindon, disponível em: https://hudoc.echr.coe.int/eng#%7B%22dmdocnumber%22:%5B%22843941%22%5D,%22itemid%22:%5B%22001-90051%22%5D%7D, acesso em: 17/03/2023.

[47]Artigo 1º, do projeto de lei. *In*: BRASIL. *Anteprojeto (...), Idem.*

[48]Lembrando que, consoante disposição expressa no art.13, do projeto: *O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei, sendo que a autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais (que ainda precisa ser definido em termos de requisitos constitutivos, formais e materiais), informando ao Conselho Nacional de Justiça*. *In*: BRASIL. *Anteprojeto (...), Idem.*

[49]Para alguns autores inclusive os dados referentes à saúde e à vida sexual são considerados super-sensíveis, *in quanto sono gli unici per i quali non sussiste alcune esenzione che ne consente l'uso in assenza di un consenso*. *In:* ORLANDO, S. *I limiti della tutela penale del tratamento illecito dei dati personali nel mondo digitale.* In: Diritto Penale Contemporaneo, Tribunale de Milano, Milano, 2019, p.183.

[50]O art.14, do projeto, definiu que o tratamento destes dados sigilosos somente poderá ocorrer se estiver previsto em lei, e tão somente para atividades de persecução penal. E mais, no seu §2º, determinou que o acesso a dados desta natureza, controlados por pessoas jurídicas de

constitucional ou legal); *anonimizado* (relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento).

Mas quais as hipóteses de acesso e manejo de dados pessoais por estas autoridades? O projeto de lei somente esclarece isto no seu art. 9º, a saber: (i) quando necessário para o cumprimento de atribuição legal de autoridade competente, na persecução de *interesse público disposto em lei*, ou *regulamento*, observados os requisitos legais; (ii) *para execução de políticas públicas de segurança e persecução penal* previstas em lei; (iii) para a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente[51].

Sem sombra de dúvidas que a persecução de interesse público e a execução de políticas públicas envolvendo segurança e responsabilização penal configuram escopos de significados/sentidos muito abertos, justamente por se fundar em conceitos jurídicos passiveis de determinação (mesmo que complementar) demasiadamente discricionária por parte da autoridade na consecução material de suas operações/atividades, demandando atento controle por parte da Sociedade como um todo, e dos agentes de controle institucional interno e externo. Isto resta ainda mais delicado na medida que o projeto autoriza o acesso e manejo de dados para fins de persecução de interesse público disposto em regulamento, haja vista e em tese eventuais fragilidades estruturantes e normativas destes, exigindo atenção redobrada no particular.

Fazendo leitura simples do projeto, as premissas ali definidas revelam a preocupação do legislador em trazer às autoridades investigativas responsabilidades no tratamento de dados já existentes, abarcando desde de seus princípios e finalidades, passando pelo uso e acesso a dados desnecessários, *devendo ser descartados todos aqueles que surgirem durante o processo e forem inutilizáveis*, assim como autorização judicial para compartilhamento de dados, ainda que entre autoridades[52].

Só que, no exercício das atividades de segurança da comunidade e da persecução penal, o Estado deverá observar, dentre outros fundamentos, o respeito à vida privada e à intimidade, a presunção de inocência, a confidencialidade e integridade dos sistemas informáticos pessoais, a garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal[53], sob pena de operar em proteção insuficiente, ou em excesso, gerando consequências múltiplas de caráter indenizatório aos direitos violados, e mesmo de eventuais nulidades aos serviços públicos prestados indevidamente. Por certo que se associa a isto *o dever fundamental de prestação de informações* que os órgãos públicos devem respeitar

direito privado, será especifico a pessoas investigadas, dependendo sempre de ordem judicial prévia que esteja baseada em *indícios de envolvimento* dos titulares de dados afetados em infração penal, e na demonstração de necessidade destes dados à investigação. *In*: BRASIL. *Anteprojeto (...), Idem.*

[51]BRASIL. *Anteprojeto (...), Idem.*

[52]Como, aliás, faz o General Data Protection Europeu - GDPR, em seu art.10, determinando que: *Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority, in: GDPR. Processing of personal data relating to criminal convictions and offences,* disponível em: https://gdpr-info.eu/art-10-gdpr/, acesso em: 01/04/2023, (Grifos nossos).

[53]Como prevê o art. 2º, do mesmo documento. Na mesma linha vai o art. 39, do projeto, ao determinar que o tratamento de registros criminais deverá atender, para além dos princípios e fundamentos da lei, também a presunção da inocência e a finalidade de integração social do condenado. *In:* GDPR*. Processing of (…), Idem.*

em face das pessoas cujos dados são acessados e manejados, até por força do comando explícito do art. 40, do projeto de lei[54].

Estes elementos ganham ainda maior importância na medida em que o art. 3º do documento diz expressamente serem estas normas aplicadas a qualquer operação de tratamento realizada *por autoridades competentes em atividades de segurança pública e de persecução penal*. Ou seja, aqui estão albergadas operações/atividades envolvendo investigações policiais com suas inúmeras diligências; operações do Ministério Público instrumentais (prévias e concomitantes) as ações judiciais; cumprimento de medidas judiciais de processos já em andamento (ou preparatórias); e em todas estas fases/momentos em que a máquina estatal se encontra em movimento lidando com dados de pessoas. Por conta disto são muitas as possibilidades de exposição destes dados, a ponto de caracterizar violação de direitos assegurados, reclamando da autoridade competente cuidados, medidas objetivas/eficazes/capazes de suas preservações.

A amplitude de possibilidades é real em face do disposto no art. 7º, do projeto[55], que exige da autoridade competente a distinção, *na medida do possível*, entre diferentes categorias de titulares de dados, a saber: (i) pessoas em relação às quais existem indícios suficientes de que cometeram infração penal; (ii) pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer infrações penais; (iii) pessoas processadas; (iv) pessoas condenadas definitivamente; (v) vítimas ou potenciais vitimas; (v) testemunhas, ou ainda (vi) pessoas que possam fornecer informações sobre todos estes.

Em síntese, é possível que, em praticamente todas as ações de Estado voltadas à segurança pública e à persecução penal – nomeadamente as mencionadas acima –, existam dados pessoais passíveis de serem acessados e manejados licitamente pelas autoridades competentes, e quando isto ocorrer deverão ser observados necessariamente os requisitos a que estamos nos referindo.

Para além disto, quando a autoridade competente estiver acessando e manejando dados pessoais – a todo tempo -, e se deparar com dados irrelevantes ou excessivos à finalidade da operação/atividade licitamente procedida, *deverá descarta-los de modo seguro e formal*, e isto por força do disposto no art.15 e art.16, I, do projeto[56], sob pena de configuração de abuso de autoridade e desvio de poder, sujeitos as devidas responsabilidades cíveis, administrativas e criminais[57].

Destaca o art.4º, do projeto[58], que *esta lei não vai se aplicar ao tratamento de dados pessoais para fins exclusivos de defesa nacional e segurança do Estado*, e aí temos o problema das possibilidades de sentidos atribuídos a tais situações, nomeadamente quando temos assistido, em vários governos recentes do país, a utilização perigosa do instituto da *Garantia da Lei e da Ordem – GLO*, como instrumento de gestão pública para determinados eventos de natureza politica e social.

---

[54]Este dever não se confunde com o de transparência, pois há casos em que esta ocorre de forma parcial ou modulada no tempo, por conta mesmo de exigências das ações de segurança e persecução penal.

[55]BRASIL. *Anteprojeto (...), Idem.*

[56]BRASIL. *Anteprojeto (...), Idem.*

[57]Nos termos da Lei nº13.869/2019, que ampliou significativamente os casos de abuso de autoridade no país. O art.32, da norma, por exemplo, configura como crime negar ao interessado, seu defensor ou advogado, acesso aos autos de investigação preliminar, ao termo circunstanciado, ao inquérito, ou a qualquer outro procedimento investigatório de infração penal, civil ou administrativa, assim como impedir a obtenção de cópias, ressalvado o acesso a peças relativas a diligências em curso, ou que indiquem a realização de diligências futuras, cujo sigilo seja imprescindível, atribuindo a tais condutas detenção de seis meses a dois anos, mais multa. *In*: BRASIL. *Lei nº 13.869 de 2019*, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm, acesso em: 12/04/2023.

[58] BRASIL. *Anteprojeto (...), Idem.*

Este mecanismo da GLO, a despeito de legal[59] [60], pode ter legitimidade duvidosa em certos cenários de tensões políticas e sociais, haja vista a amplitude de possibilidades normativas autorizadoras do seu uso, em especial as que dizem com o *esgotamento dos instrumentos* destinados à preservação da ordem pública e da incolumidade das pessoas e do patrimônio, *assim formalmente reconhecidos pelo respectivo Chefe do Poder Executivo Federal ou Estadual como indisponíveis, inexistentes ou insuficientes ao desempenho regular de sua missão constitucional*[61]*.*

Não demarca esta legislação critérios, fundamentos e justificações claros para o reconhecimento referido acima, deixando ao livre arbítrio do Poder Executivo indicar isto, a despeito da tentativa modesta de regulamentar melhor a matéria através do Decreto Federal nº 3.897/2001[62]. E tal fato se torna ainda mais grave na medida em que, em regime de GLO, nos termos do §4º, do mesmo art.15, da Lei[63], os órgãos operacionais das Forças Armadas poderão desenvolver todas as ações de caráter preventivo e repressivo necessárias para assegurar o resultado da garantia da lei e da ordem, inclusive, pois, os que envolverem o manejo de dados privados de pessoas físicas e jurídicas – por óbvio que relacionadas ao escopo da GLO (que podem ser amplíssimos)[64].

Quiçá os princípios a que deve estar vinculado o tratamento de dados pessoais, instituídos pelo art.6º, do projeto, possam contribuir para o controle das ações de manejo dos dados na esfera penal e processual penal, notadamente os que envolvem:

> (i) A *finalidade* (inciso II), que obriga a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Por certo que a autoridade que acessar e manejar os dados deverá ponderar – de modo fundamentado – o tempo e modo oportunos para prestar tal informação, a fim de não comprometer as atividades de segurança pública e persecução penal, tomando cautelas formais e materiais no sentido de evidenciar, a todo tempo em que estiver tratando daqueles dados, os propósitos assinalados, sob pena de caracterizar desvios e abusos de autoridade, ou outras irregularidades e ilícitos.
> *(ii) adequação* (pertinência e relevância do tratamento diante dos objetivos pretendidos e em face do contexto do tratamento); *necessidade* (limitação do tratamento ao mínimo necessário às finalidades demarcadas, observados os critérios de abrangência, pertinência e não excessividade em face das finalidades informadas);

[59]Também está regulado pelo art. 15, da Lei Complementar nº 97, de 1999. *In*: BRASIL. *Lei nº 97 de 1999*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm, acesso em: 12/04/2023.

[60]E disciplinada no art. 142, da Constituição Federal de 1988, que as Forças Armadas se destinam à defesa da Pátria, à garantia dos poderes constitucionais e da lei e da ordem, e configura atribuição temporária destas, em períodos de normalidade constitucional, razão pela qual não se confunde com o Estado de Sítio e o Estado de Defesa, ou mesmo com a Intervenção Federal. *In*: BRASIL. *Constituição*, disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, acesso em: 12/04/2023.

[61]Termos utilizados pelo art.15, §§3º e 4º, da Lei Complementar nº 97/1999. *In*: BRASIL. *Lei nº 97 de 1999 (...), Idem.*

[62]BRASIL. *Decreto Federal nº 3.897 de 2001*, disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3897.htm, acesso em: 13/04/2023.

[63]BRASIL. *GLO*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm, acesso em: 13/04/2023.

[64]Importa o registro de que o Decreto Federal nº 3.897/2001, regulamentador da Lei Complementar nº 97/1999, em seu art. 3º, reconhece às Forças Armadas competência para desenvolver ações de polícia ostensiva, preventiva e repressiva que se incluem na competência das polícias militares. Não bastasse isto, a Lei Federal nº 13.491/2017, transferiu para a Justiça Militar o julgamento de crimes cometidos por profissionais das Forças Armadas em missões de garantia da lei e da ordem.

> e *proporcionalidade* (como compatibilidade do tratamento em face dos objetivos pretendidos) - incisos III, IV e V[65].

Este elemento de *adequação*, que também podemos associar a ideia de idoneidade, implica que toda a restrição aos direitos tutelados pelas leis de proteção de dados, em nome da segurança pública e da persecução penal, seja idônea tão somente para o atendimento do escopo autorizado pela norma, exigindo-se que os meios empregados no particular se apresentem instrumentalmente ajustados para alcançar o fim almejado.

Já o elemento da *necessidade* deve ser entendido como indispensabilidade do acesso e manejo de dados para os fins sob comento; remete que tais medidas se deem do modo menos restritivo possível aos direitos fundamentais consectários, evitando assim causar lesão dispensável a eles (certa proibição de excesso).

E o elemento *proporcionalidade* precisa ser tomado de modo estrito, no sentido de que qualquer restrição aos direitos fundamentais dos titulares dos dados envolvidos deve ser justificada pela relevância da satisfação dos escopos perseguidos– legais e legítimos[66] [67] [68].

Importante previsão é a estabelecida no art. 8º, parágrafo único, do anteprojeto, ao exigir que, caso o responsável verifique que tratou *dados pessoais inexatos*, ou que *tratou dados pessoais de forma ilícita*, o destinatário *deve ser informado tão logo seja possível*, e *os dados pessoais devem ser retificados ou apagados*, e se não o fizer, sua utilização para os fins de segurança pública ou persecução penal será considerada nula, podendo impactar inúmeros processos e procedimentos já realizados.

A despeito da regra ser o acesso do titular a seus dados pessoais que se encontram nas mãos de terceiros o projeto de lei sob comento previu, em seu art. 20, a possibilidade de que *a prestação de informações, e mesmo a concessão e acesso a dados, possa ser adiada, limitada, ou até recusada*, se e enquanto tal for necessário e proporcional para: (i) evitar prejuízo as investigações, inquéritos ou processos judiciais; (ii) evitar prejuízo à prevenção, detecção, investigação ou repressão de infrações penais, ou para a execução de sanções penais; (iii) proteger a segurança do Estado ou a defesa nacional; e ainda (iv) proteger direitos e garantias de terceiros[69]. E isto se justifica em face de delicados cenários de investigação e busca/coleta de provas envolvendo crimes por vezes complexos que reclamam cuidados especiais na persecução penal, sob pena de vazamento de informações e dados esvaziarem inúmeras medidas já levadas a cabo à delimitação da responsabilização.

Prevê adequadamente o projeto, em seu art.22, que a confirmação de existência, ou o acesso a dados pessoais, serão providenciados mediante requisição do titular em formato simplificado, *imediatamente*, ou por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a *finalidade do tratamento*, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. A nosso sentir esta disposição poderá ser flexibilizada, no que for adequado, necessário e proporcional, àquelas situações demarcadas pelos

---

[65]BRASIL. *Lei nº 13.709 de 2018, Idem.*

[66]Esta é uma reflexão que já tivemos oportunidade de explorar em nosso texto: LEAL. R.G. "Aspectos constitutivos da teoria da argumentação jurídica: a contribuição de Robert Alexy*", Revista de Investigações Constitucionais*, Vol.1, nº 2, Núcleo de Investigações Constitucionais da UFPR, Curitiba, 2014.

[67]Ver também: ALEXY, R. *Teoría de los Derechos Fundamentales*, Centros de Estudios Constitucionales, Madrid, 2000, p.112 e ss.

[68]Ainda: ALEXY, R. "The Construction of Constitutional Rights*"*, *Law & ethics of Human Rights*, Vol. 4, Issue 1, Article 2, Berkeley Electronic Press, Berkeley, 2010.

[69]A mesma norma exige que o responsável pelo tratamento dos dados deve informar o titular destes, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso, bem como indicar quando cessarão estes motivos.

incisos referidos no art. 20, sob pena de contradição em termos do próprio projeto, a ponto de colocar em risco escopos que está a perseguir[70].

Já o acesso da autoridade a dados pessoais controlados por pessoas jurídicas de direito privado (*google, facebook, whatsapp, instagran*) só pode ocorrer mediante previsão legal, sendo que a requisição – administrativa ou judicial – deverá indicar o fundamento legal de competência expressa para o acesso e a motivação concreta, demonstrando a adequação, necessidade e proporcionalidade da medida, sendo vedado pedidos genéricos ou inespecíficos[71].

Este tema já está sendo enfrentado, em parte, pelo Supremo Tribunal Federal, na perspectiva do controle de dados por provedores de internet no exterior, em sede de Ação Declaratória de Constitucionalidade-ADC nº 51, da relatoria do Min. Gilmar Mendes, tendo inclusive ocorrido audiência pública para debater o tema neste Tribunal (em 10/02/2020), oportunidade em que os interessados apresentaram vários argumentos a favor e contra o objeto da ação (Acordo de Assistência Judiciário-Penal entre os governos do Brasil e dos Estados Unidos referentes à obtenção de conteúdo de comunicação privada sob controle de provedores de aplicativos de internet sediados no exterior)[72].

A questão prática vertida nesta ação envolve ser constitucional, ou não, exigir-se o cumprimento de instrumentos de cooperação jurídica internacional à obtenção de dados e conteúdo armazenados no exterior por empresa com operação no Brasil, e isto porque tribunais brasileiros têm deixado de aplicar os ritos da carta rogatória ou do auxilio direto à obtenção destes dados, que estão sob o controle de empresas situadas em outros países, em nome da soberania nacional de suas jurisdições, pressionando com isto as empresas filiais localizadas no Brasil para a realização da entrega formal de dados sigilosos, atribuindo a elas multas diárias altíssimas, e até prisão de seus representantes legais.

A decisão final do STF nesta ADC veio a lume em 23/02/2023, no sentido de conhecer da ação, vencidos os Ministros André Mendonça e Nunes Marques, e, no mérito, por unanimidade, julgar parcialmente procedente o pedido formulado na inicial para declarar a constitucionalidade dos dispositivos indicados e da *possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia, nas específicas hipóteses do art. 11, do Marco Civil da Internet[73], e do art. 18, da Convenção de Budapeste[74]*; ou seja:

> *"nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no*

[70]O disposto no §1º, do art.20, parece contemplar, em parte, esta possibilidade ao prever que *o responsável pelo tratamento deve informar o titular dos dados, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso, bem como indicar quando cessarão os motivos da recusa ou da limitação de acesso*.

[71]Nos termos do art. 11, combinado com o art. 18 (ao afirmar que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, sendo que qualquer restrição a estes direitos deverá ser proporcional, limitada no tempo e necessária para finalidades de atividades de segurança pública e de persecução penal), do projeto de lei.

[72]A ação foi intentada pela Federação das Associações das Empresas de Tecnologia da Informação (Assespro Nacional), e foram aceitos como *amici curiae* as empresas Facebook - Serviços Online do Brasil Ltda., a Yahoo! do Brasil Internet Ltda., o Instituto de Referência em Internet e Sociedade-IRIS, e a Sociedade de Usuários de Tecnologia – Sucesu Nacional.

[73]Art. 11 – Marco Civil da Internet: "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros". *In:* BRASIL. *Lei 12.965 de 2014*, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acesso em: 12/04/2023.

[74]RM. *Convenção de Budapeste*, disponível em: https://rm.coe.int/16802fa428, acesso em: 13/04/2023.

> *Brasil e de crimes cometidos por indivíduos localizados em território nacional, com comunicação desta decisão ao Poder Legislativo e ao Poder Executivo, para que adotem as providências necessárias ao aperfeiçoamento do quadro legislativo, com a discussão e a aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais"*[75].

Ao largo deste debate tópico, contamos com decisões judiciais envolvendo, por exemplo, investigação de roubo e organização criminosa judicializada, em que o magistrado, acolhendo pedido da Polícia Civil, determinou que o Google identificasse todos os usuários ativos na data e horário do assalto, em um raio de 250 metros, assim como fornecesse outros dados dos usuários identificados na região do crime, tais como endereço de e-mail, locais salvos no Google Maps, e histórico de deslocamento e de buscas na plataforma nos últimos 30 dias[76].

Garante-se, de qualquer sorte e pelo projeto de lei sob análise, a eliminação dos dados pessoais após o *término do seu tratamento no âmbito e nos limites técnicos das atividades*, nos termos do art.17, do anteprojeto, sendo que o art.19 prevê que o titular dos dados pessoais tem direito de obter do controlador, mediante requisição: (i) confirmação da existência de tratamento destes dados; (ii) acesso aos seus dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; (v) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados[77].

Seguramente que aqui vamos ter diversos desafios a tratar, eis que determinados processos criminais, em face de suas complexidades e sofisticações (principalmente em delitos econômicos, de corrupção, lavagem de dinheiro, tráfico de drogas, dentre outros), reclamam tempos diferidos de instrução e julgamento (notadamente condizente a formatação das provas) não raro longos, eventualmente com múltiplas intercorrências e dificuldades[78]. Em tais contextos, seguro que o término de tratamento de dados poderá se prolongar, impondo-se, durante todo o período, aos que os acessam/manejam, que tenham protocolos e instrumentos aptos a garantir suas integridades, sigilos possíveis e informação a quem de direito – cadeia de custódia formatada e eficiente.

Outro problema surge em face da disposição do art. 23, do projeto, que está a exigir que as decisões tomadas com base no *tratamento automatizado de dados pessoais*, e que afetem os interesses do titular, sejam precedidas de autorização do CNJ e de publicação de relatório de impacto respectivo, comprovando a adoção de garantias adequadas aos direitos e liberdades do titular. Cumpre registrar que tal

---

[75]O STF levou em conta aqui também a morosidade excessiva – mesmo em tempos de comunicação virtual – do atendimento destas demandas pelas vias mais tradicionais – como a cooperação jurídica internacional -, o que tem implicado até o perecimento de direitos tutelados, ou ainda a total ineficácia da medida. *In*: STF. *ADC 51*, disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379, acesso em: 11/04/2023.

[76]Autos do Mandado de Segurança Criminal nº 2145603-41.2021.8.26.0000, da Comarca de Viradouro, em que são impetrantes Google Brasil Internet LTDA e Google LLC, e impetrado juízo de direito da vara única do foro de São Simão/SP. *In*: CONJUR. *Mandado de Segurança Criminal nº 2145603-41.2021.8.26.0000*, disponível em: https://www.conjur.com.br/dl/geolocalizacao-google.pdf, acesso em: 06/04/2023.

[77]Lembremos que o controlador, em caso de impossibilidade de adoção imediata das providências referidas, deverá enviar resposta ao titular dos dados que apresentou postulação especifica no sentido de: (i) comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou (ii) indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

[78]Pensemos nos casos de: (i) múltiplos autores, coautores, participes, terceiros; (ii) pessoas físicas e jurídicas envolvidas; (iii) naturezas distintas das provas reclamadas (periciais, técnicas, documentais, testemunhais), todos estes localizados em territórios distintos, nacional e, ou, estrangeiro.

dispositivo está relacionado com o art. 20, da Lei nº 13.709/2018, que já tratava da matéria determinando que *o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito, ou os aspectos de sua personalidade*.

Este tratamento automatizado oportuniza a construção do perfil do titular de dados obtendo, normalmente, informações através de várias bases de dados pessoais, e o faz a partir de procedimentos de classificação, aprovação ou rejeição destas informações com base em algumas regras, algoritmos e instruções. O problema é que esta decisão automatizada, feita com base em mapeamento de perfis pessoais construídos com aqueles meios de inteligência artificial, vão gerando, com baixos níveis de controle (ou nenhum), modelos que têm a finalidade de avaliar comportamentos e questões pessoais de determinados usuários, envolvendo informações relacionadas à situação econômica, vida profissional, interesses pessoais, comportamento e localização de indivíduos.

Agora, está este art.23, do projeto, determinando que decisões tomadas pelos órgãos públicos de segurança e persecução penal com base no tratamento automatizado de dados (quando afetem interesses do seu titular – e de hábito afetam), devem, sempre, ser *precedidas* de: (i) autorização do CNJ e (ii) publicação de relatório de impacto, comprovando a adoção das garantias já referidas[79]. Mas e quando estes órgãos, no exercício regular de seus ofícios, se depararem com situações de urgência que reclamam decisões imediatas, justamente em face dos dados pessoais automatizados acessados, deverão deixar de agir por não possuírem de pronto a autorização e relatório perquiridos? Entendemos que deverão agir, *em nome da proteção suficiente de direitos públicos indisponíveis* a que respondem, com a devida acuidade, adequação, necessidade e proporcionalidade, documentando tudo e reportando, assim que possível, ao CNJ, com o devido relatório de impacto, sob pena de inviabilizar processos e procedimentos relacionados à segurança pública[80].

O anteprojeto cria figura nova neste universo que é o chamado *relatório de impacto à proteção de dados pessoais* (art.23, combinado com o art.29), que reclama maior definição conceitual normativa, sendo atribuível ao CNJ a função de Autoridade Reguladora da matéria, até porque vem imposto como obrigatório para o tratamento de dados pessoais sensíveis, sigilosos, ou *em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados* (*caput* do art.29). Mas quem define, e com base em que critérios, quando se configuram estas operações? Por certo deverá ser a autoridade competente para o acesso e manejo destes dados, sujeita a eventual entendimento contrário da Autoridade Reguladora, mesmo que a posteriori[81]. O parágrafo terceiro, do art.29, demarca que este *relatório deverá conter*, no mínimo: *a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, e a análise*

[79]Somam-se a isto as exigências complementares do art.24, do projeto, à mesma matéria, nomeadamente os seus §2º, §3º, exigindo que o controlador elabore relatório do impacto de proteção do caso submetido, e que o CNJ deve, após examinar o relatório de impacto enviado, decidir sobre a decisão com base no tratamento automatizado de dados. O caput do dispositivo é confuso, vez que condiciona a imposição de sua disciplina *a hipótese de existência de elevado risco para os direitos fundamentais* do titular, não informando quem teria legitimidade para a valoração desta hipótese. Por outro lado, fez bem o artigo em prever ser vedada a adoção de qualquer medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada (§4º, do art.25).

[80]Sobre este tema do dever de proteção estatal, ver o excelente texto de: LEAL, M.C.H. & MAAS, R.H. *Dever de proteção estatal, proibição de proteção insuficiente e controle jurisdicional de políticas públicas,* Lumes Juris, Rio de Janeiro, 2020.

[81]Lembrando ainda que Ministério Público e Defensoria Pública poderão requisitar este relatório quando estiverem atuando na defesa de direitos individuais coletivos (§2º, do art.29); mas por curioso que seja, a OAB não restou contemplada aqui.

do controlador com relação as medidas, salvaguardas e mecanismos de mitigação de risco adotados[82] [83]*.*

Andou bem o projeto de lei ao prever o que podemos nominar – analogicamente – de *cadeia de custódia das operações de tratamento de dados pessoais*, disciplinada nos art. 32 a art.34[84], garantindo, ao menos formalmente, procedimentos e protocolos uniformes destes registros a fim de dar segurança a todos os envolvidos no acesso e manejo de dados pessoais.

Já no que toca à segurança e sigilo dos dados pessoais versados pelo projeto, o art.36 estabelece que: *os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito*, impondo aos órgãos públicos políticas, protocolos e procedimentos adequados e eficientes para tal mister, sob pena de responsabilização pelos danos decorrentes daí. O problema é que estas medidas implicam disposição de recursos orçamentários, de logística, tecnologias, pessoal e infra-estrutural imensas, haja vista que os repositórios dos dados envolvidos igualmente são enormes, físicos e virtuais, e de distintas naturezas (origem facial 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 dado biométrico, situação sócio-econômica, dentre outros)[85].

O capítulo VII do projeto trata das tecnologias de monitoramento e tratamento de dados de elevado risco para direitos, liberdades e garantias dos titulares dos dados, a partir do seu art.42, *exigindo para que isto ocorra prévia exigência de lei específica* que estabeleça garantias aos direitos dos titulares *e seja precedida de relatório de impacto de vigilância*. Não bastasse isto, o §2º, do mesmo artigo, ainda determina que o processo legislativo consectário – submetido a consulta pública com ampla participação social (§4º) - deverá ser instruído por análise de impacto regulatório com vários requisitos demarcados pelos incisos de I a VI, assim como estabelecer política de uso destes dados (§3º).

Mas enquanto esta regulamentação não ocorre não se sabe quem deverá constituir previamente o juízo de valor, e objetivo, sobre ser, ou não, elevado o risco de que trata o dispositivo! Então resta a pergunta: até a edição da norma postulada faz-se o quê com as investigações em andamento e as necessárias à tutela da segurança pública e persecução penal[86]?

---

[82]Podemos pensar no polêmico *Perfil de Gerenciamento de Infratores Correcional para Sanções Alternativas* – COMPAS, norte americano, cujo escopo é o de demarcar riscos envolvendo pessoas que reincidem em crimes e auxiliar magistrados na tomada de decisões em tais casos. Este programa, a partir de várias perguntas pré-definidas, formata um score do réu e do risco que ele representa em termos de recalcitrância criminal. Ocorre que análises realizadas pela organização de jornalismo investigativo ProPublica diagnosticaram que o algoritmo formatado pelo programa indica que pessoas negras possuem alto risco de reincidência, revelando/denunciado elemento discriminatório desta ferramenta. *In*: COMPAS CORE. *Risk assessment*, disponível em: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html , acesso em 13/04/2023.

[83]Para conhecer melhor a Pro pública, ver o site: PROPUBLICA. *Investigative Journalism in the Public Interest*, *In*: https://www.propublica.org, acesso em 14/04/2023.

[84]Complementada esta cadeia pelas medidas de segurança, técnicas e administrativas de proteção dos dados pessoais descritas no §3º, do art.36, deste projeto. *In*: BRASIL. *Anteprojeto (...), Idem.*

[85]Mesmo que o §1º, deste art. 36, preveja que o CNJ poderá dispor de padrões técnicos mínimos para tornar aplicáveis tais disposições, ainda assim talvez nem todos os órgãos públicos que respondam por competências de segurança e persecução penal tenham condições de constituí-los.

[86]A despeito disto, esta exigência, ao menos em face dos termos ali colocados, vai exigir do processo legislativo de origem e do próprio texto final ampla e detalhada capacidade regulatória.

Seguramente a máquina estatal não poderá ficar paralisada neste interregno e nestes setores, sob pena de colapso dos bens jurídicos que visa alcançar, razão pela qual a atribuição de sentido melhor que se pode dar, no caso, é o de que tal disposição do projeto opera com *efeitos demarcatórios supervenientes* a sua existência, pois inexistem neste momento comandos normativos proibitivos de utilização daquelas tecnologias e tratamentos já regulamentos e indispensáveis aos desideratos perseguidos. É no exercício, pois, de suas competências que os órgãos de segurança e persecução penal responsáveis levarão a cabo a valoração material fundamentada dos riscos elevados a serem evitados em cada caso.

Para fins de segurança pública, todavia, o projeto está vedando a utilização de tecnologias de vigilância[87], diretamente acrescida de técnicas de investigação de pessoas determinadas e em tempo real, de forma continua, exceto quando houver conexão com atividade de persecução penal individualizada e autorizada por lei e decisão judicial (art.43), e isto é importante porque não permite, de modo aberto e indiscriminado, que politicas ou ações genéricas de segurança pública se valham de mecanismos invasivos como estes relacionados as tecnologias de vigilância para acessar e manipular dados e informações de quaisquer pessoas, exigindo, pois, cuidados de políticas e ações viralizadas por todas as partes de videomonitoramento de cidades por câmeras distribuídas em vias e espaços públicos e privados[88].

Neste ponto, tivemos o reconhecimento jurisprudencial da ilegalidade de procedimento investigatório de SIM SWAP (transferência de linha telefônica para outro chip em poder da autoridade policial) autorizado por ordem judicial de primeiro grau para que a autoridade policial habilitasse o chip do agente investigador com o fim de ter pleno acesso e em tempo real de chamadas e mensagens transmitidas pela linha originária dos investigados. O problema é que este procedimento coloca a autoridade policial como participante das comunicações de todas as pessoas que se valham da linha transferida, podendo interagir e gerenciar estas informações a seu livre arbítrio[89].

Já o uso compartilhado de dados pessoais entre as autoridades competentes só é possível, de acordo com o projeto, com autorização legal e judicial, ou no contexto de atuações conjuntas autorizadas legalmente (art.45), desautorizando o compartilhamento direto e contínuo de banco de dados pessoais, exceto os referentes a dados públicos, e os que se destinam a investigação ou processo criminal específico. O §2º, deste mesmo artigo, determina que requisições de acesso a dados entre autoridades competentes para uso compartilhado devem ocorrer devidamente motivadas quanto (i) ao contexto específico do pedido, (ii) à base legal, (iii) finalidade, (iv) necessidade e (v) proporcionalidade, devendo ainda o registro destes acessos e usos serem mantidos por no mínimo 5 anos[90].

---

[87]Estamos falando de medidas como: (i) o uso de equipamentos de validação biométrica, para os fins de reconhecimento facial ou de digitais de pessoas; (ii) circuitos de câmeras de vigilância; (iii) uso de drones para filmagens e retenção de imagens e sons; (iv) rastreadores eletrônicos, dentre outros.

[88]Citemos os casos das cidades de: (i) Taiyuan, China, com 465.255 câmeras para 3.975.985 pessoas, perfazendo um total de 117,02 câmeras por 1.000 pessoas; (ii) Wuxi, China, com 300.000 câmeras para 3.315.113 pessoas, perfazendo um total de 90,49 câmeras por 1.000 pessoas; (iii) Londres, Inglaterra (Reino Unido), com 691.000 câmeras para 9.425.622 pessoas, perfazendo um total de 73,31 câmeras por 1.000 pessoas. Estas cidades – e tantas outras, inclusive no Brasil – tem sustentado tais medidas em face dos argumentos de: redução de crimes, análise inteligente, preventiva e curativa, de riscos e perigos sociais; identificação de objetos abandonados; aprimoramento de investigações criminais. Mas pergunta-se: a que custo para direitos e garantias fundamentais individuais? *In*: DGT. *Conheçam as cidades que mais investem em vídeo monitoramento no mundo*, disponível em: https://dgt.com.br/conheca-as-cidades-que-mais-investem-em-videomonitoramento-no-mundo/, acesso em: 11/04/2023.

[89]STJ. REsp nº 1806792/SP, disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp, acesso em 14/04/2023.

[90]Importantes previsões normativas se encontram nos arts. 47 e 48, na medida em que vedam, como regra geral, autoridades competentes praticar compartilhamento de dados

O que temos de entender aqui é a necessidade de adequar estas disposições a processos criminais envolvendo delitos complexos e sofisticados, com múltiplos protagonistas (pessoas físicas e jurídicas), de inúmeros lugares/países, haja vista que, nestes casos, os modos, tempos e espaços de atuações delinquentes não são lineares, mas multidirecionais e transversais, reclamando modulações controladas e documentadas dos acessos e manejos da dados pelas investigações, sob pena de esvaziamento ou inviabilização da segurança pública e da persecução penal. Por óbvio que mesmo em situações como estas inexiste impedimento de que se observem os requisitos estabelecidos, justamente para garantir mais segurança a eventuais violações de privacidade e intimidade que impliquem aquelas medidas.

No que tange as sanções estabelecidas pelo projeto, destacamos o disposto no §1º, do art.63, ao determinar que o agente público que facilitar ou der causa à infração das suas normas, responderá seja disciplinarmente, seja por improbidade administrativa, seja por crime eventualmente configurado, e por todos estes âmbitos cumulativamente, se for o caso.

Cria também o projeto de lei, em seu art.66, novo artigo para o Código Penal brasileiro[91], caracterizado como art.154-C, tipificando a seguinte conduta: *Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiro a ele relacionados*, atribuindo pena de reclusão de 1 a 4 anos e multa, assim como aumentando-a de um a dois terços quando os dados pessoais forem sensíveis ou sigilosos, e quando o crime for praticado por funcionário público em razão do exercício de suas funções.

Por fim, traçando paralelo entre os conceitos da cadeia de custódia no Processo Penal, em especial a partir da Lei Anticrime (Lei nº13.964/2019[92]), e a inserção de artigos específicos nesta matéria, a partir do art.158-A e seguintes, do Código de Processo Penal- CPP brasileiro[93], podemos sustentar que este projeto da LGPD Penal vem realçar à importância da integridade da prova penal constituída de dados, informações e registros pessoais, e os cuidados que as autoridades de segurança pública e de persecução penal devem ter com o acesso, tratamento e gestão do ciclo de vida destes elementos, vez que constituem a trilha auditável de juízos absolutórios ou condenatórios na esfera criminal[94].

---

pessoais com pessoas jurídicas de direito privado, excetuando algumas situações; e vice e versa (pessoas jurídicas de direito privado ->autoridades competentes).

[91]BRASIL. *Código Penal*, disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em: 14/04/2023.

[92]BRASIL. *Lei nº 13.964 de 2019*, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm, acesso em, 14/04/2023.

[93]Artigo 158-A – CPP: "Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte. §1º O início da cadeia de custódia dá-se com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio; §2º O agente público que reconhecer um elemento como de potencial interesse para a produção da prova pericial fica responsável por sua preservação; §3º Vestígio é todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal (...)". *In*: BRASIL. *Código de Processo Penal*, disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm

[94]Outro exemplo é o artigo 37, da LGPD, que estabelece que: *o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem*; na mesma direção o art.158-E, do CPP, está prevendo que: *todas as pessoas que tiverem acesso ao vestígio armazenado deverão ser identificadas e deverão ser registradas a data e a hora do acesso*. *In*: BRASIL. *Lei nº 13.709 de 2018, Idem.*

5. CONSIDERAÇÕES FINAIS

Como temos sustentado neste trabalho, o direito a proteção de dados tem sido desenvolvido a partir do direito ao respeito a vida privada, sendo que este conceito se refere ao ser humano em geral, sem qualquer discriminação, e mesmo suas dimensões eventualmente institucionais – como as pessoas jurídicas.

Isto significa que, em primeiro lugar, afastando-nos da dimensão exclusiva do delito que historicamente marcou a violação da privacidade no final do século XIX, temos que a proteção da privacidade envolve o reconhecimento da titularidade de sujeitos de direito a terem sua vida privada preservada, enquanto verdadeiro direito subjetivo, o que implica possuir posição plena de proteção.

Em segundo lugar, a noção de proteção de dados que adotamos tem como centro neural o objeto do direito, que deixa de ser uma noção sintética que garante a proteção de vários momentos da vida privada, e passa a ser a exigência de tratamento de realidade jurídica específica atinente à informação pessoal, de acordo com obrigações regulamentares específicas.

Em terceiro lugar, o direito a privacidade e à proteção de dados pessoais, na sua qualidade de direito humano ou liberdade fundamental, enraizado na identidade pessoal do homem, recebe âmbito de exercício mais amplo dirigido diretamente às autoridades públicas (incluindo as legislativas).

Ou seja, o sistema normativo de garantias do direito à integridade da vida privada na dimensão do tratamento de dados pessoais é a elaboração de disciplina de atividades públicas e privadas que devem ser realizadas de forma a serem compatíveis com os direitos dos indivíduos. Isto abre caminho a uma atividade reguladora pública, que garanta a aplicação dos princípios fundamentais do tratamento de dados pessoais.

Assim, o direito a tutela de dados pessoais pode ser considerado, em perspectiva afirmativa, como direito do sujeito a que seus próprios dados sejam registrados, gestados, custodiados, acessados, transmitidos a terceiros e divulgados de modo correto; e em perspectiva negativa, como direito de que não ocorra qualquer tipo de aquisição, utilização ou manipulação de informações relativas a estes dados pessoais contrárias as possibilidades restritas que a norma autoriza.

Em suma, a *ratio* principal de tal direito é atribuir ao sujeito a possibilidade de autogovernar-se e autodeterminar-se a partir de sua própria consciência. Ganha força aqui o argumento de: *se il diritto in generale svolge oggi, sempre più, una funzione di umanizzazione della tecnica, soprattutto quando il soggetto di diritto rischia di divenire mero oggetto di calcoli predittivi e tecniche manipolative, il diritto alla protezione dei dati personali rappresenta una straordinaria risorsa per mantenere la persona, nella sua libertà e nella sua responsabilità, al centro della società digitale*[95]*.*

Políticas (legislativas, administrativas, cíveis, criminais, dentre outras) de *data protection*, portanto, não tratam de criar – fundamentalmente - mundos privados isolados e inexpugnáveis, resguardado de intenções e comportamentos indiscretos e invasivos, mas também visam proporcionar condições claras e seguras de projeção livre da existência de cada qual, inclusive através de dados e informações pessoais, garantindo ao mesmo tempo o controle sobre o modo pelo qual tais elementos venham a circular e sejam por outrem utilizados.

6. REFERÊNCIAS

AL-FEDAGHI, S.S. *The "right to be let alone" and private information*, in: Chen CS., Filipe J., Seruca I., Cordeiro J. (eds), Enterprise Information Systems VII, Springer, Dordrecht, 2007.

[95]ORLANDO, S. *I limiti della tutela penale del tratamento illecito dei dati personali nel mondo digitale, Ob.cit., p.172.*

ALEXY, R. *Teoría de los Derechos Fundamentales*, Centros de Estudios Constitucionales, Madrid, 2000.

_____. *The Construction of Constitutional Rights*. In Law & ethics of Human Rights, Volume 4, Issue 1. Article 2. Berkeley: Berkeley Electronic Press, 2010.

ALLEN, A.L. "Natural Law, Slavery and the right to privacy tort*", Fordham Law Review*, vol.81, issue 3, 2013, p. 1187 e ss, disponível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4854&context=flr, acesso em: 15/03/2023.

BONFANTI, M.E. "Il diritto alla protezione dei dati persinali nel Patto Internazionale sui Diritti Civil e Politici e nella Convenzione Europea del Diritti Umani: similitudini e difformità di contenuti*", Rivista Diritti Umani e Diritto Internazionale*, f.3, Franco Angeli, Roma, 2011.

BRASIL. *Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações*, disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/, acesso em 06/04/2023.

_____. *Anteprojeto de lei de proteção de dados para segurança pública e persecução penal*, disponível em: https://www.justica.gov.br/news/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf, acesso em: 05/04/2023.

_____. *Lei 12.965 de 2014*, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acesso em: 12/04/2023.

_____. *GLO*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm, acesso em: 13/04/2023.

_____. *Código Tributário Nacional*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/l5172compilado.htm, acesso em: 13/04/2023.

_____. *Decreto Federal nº 3.897 de 2001*, disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3897.htm, acesso em: 13/04/2023.

_____. *Constituição*, disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, acesso em: 12/04/2023.

_____. *Lei nº 97 de 1999*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm, acesso em: 12/04/2023.

_____. *Lei nº 13.869 de 2019*, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm, acesso em: 12/04/2023.

_____. *Lei nº 9.296 de 1996*, Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm, acesso em: 13/04/2023.

_____. *Lei nº 10.217 de 2001*, disponível em: https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10217.htm, acesso em: 13/04/2023.

_____. *Lei nº 8.078 de 1990*, disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm, acesso em: 13/04/2023.

_____. *Lei nº 12.965 de 2014*, disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, acesso em: 12/04/2023.

_____. *Lei nº 13.709 de 2018*, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm, acesso em: 12/04/23.

_____. *Lei nº 13.964 de 2019*, disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm, acesso em, 14/04/2023.

_____. *Código de Processo Penal*, disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm, acesso em 14/04/2023.

_____. *Código Penal*, disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em: 14/04/2023.

CEDH. *Declaración Universal de Derechos Humanos*, disponível em: https://www.derechoshumanos.net/normativa/normas/1948-DeclaracionUniversal.htm, acesso em: 13/04/2023.

_____. *Case-law analysis*, disponível em: https://www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=, acesso em: 29/03/2023.

COE. *Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal*, disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2, acesso em: 13/04/2023.

CONJUR. *Mandado de Segurança Criminal nº 2145603-41.2021.8.26.0000*, disponível em: https://www.conjur.com.br/dl/geolocalizacao-google.pdf, acesso em: 06/04/2023.

COMPAS CORE. *Risk assessment*, disponível em: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html , acesso em 13/04/2023.

DGT. *Conheçam as cidades que mais investem em vídeo monitoramento no mundo*, disponível em: https://dgt.com.br/conheca-as-cidades-que-mais-investem-em-videomonitoramento-no-mundo/, acesso em: 11/04/2023.

ECHR. *Gaskin v. United King, disponível em:* https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695368%22],%22itemid%22:[%22001-57491%22]}, acesso em: 29/03/2023, *acesso em: 13/04/2023.*

ECHR. *Case of S. and Marper v. The United Kindon*, disponível em: https://hudoc.echr.coe.int/eng#%7B%22dmdocnumber%22:%5B%22843941%22%5D,%22itemid%22:%5B%22001-90051%22%5D%7D, acesso em: 17/03/2023.

EUR. *Maximillian Schrems v Data Protection Commissioner*, disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362, acesso em 25/03/2023.

_____. *Diretivas*, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU, acesso em: 13/04/2023.

_____. *Regulamentos*, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679, acesso em: 13/04/2023.

EXAME. *Maior vazamento da história pode ter exposto 8 bilhões de senhas*, disponível em: https://exame.com/tecnologia/maior-vazamento-da-historia-pode-ter-exposto-8-bilhoes-de-senhas/, acesso em 09/04/2023.

GDPR. Processing of personal data relating to criminal convictions and offences, disponível em: https://gdpr-info.eu/art-10-gdpr/, acesso em: 01/04/2023.

LAMANUZZI, M. *Diritto penale e trattamento dei dati personali - Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti*, disponível em: https://jus.vitaepensiero.it/news-papers-diritto-penale-e-trattamento-dei-dati-personali-codice-della-privacy-novita-

introdotte-dal-regolamento-2016-679-ue-e-nuove-responsabilita-per-gli-en-4763.html, acesso em: 10/03/2023.

LEAL, M.C.H. & MAAS, R.H. *Dever de proteção estatal, proibição de proteção insuficiente e controle jurisdicional de políticas públicas*, Lumes Juris, Rio de Janeiro, 2020.

LEAL. R.G. "Aspectos constitutivos da teoria da argumentação jurídica: a contribuição de Robert Alexy*", Revista de Investigações Constitucionais*, Vol.1, nº2, Núcleo de Investigações Constitucionais da UFPR, Curitiba, 2014.

Lexis News. *Roberson v. Rochester Folding Box Co, disponível em: https://www.lexisnexis.com/community/casebrief/p/casebrief-roberson-v-rochester-folding-box-co, acesso em: 13/04/2023.*

LUGARESI, N. *Internet, privacy e pubblici poteri negli Stati Uniti,* Giuffrè, Bologna, 2000.

MILLER, A.R. & BERKMAN, B.A. *The assault on privacy, computers, data banks and dossier*, University Michigan Press, Michigan, 1971.

NIGER, S. *Le nuove dimensioni della privacy: dal diritto alla riservatezza, alla protezione dei dati personali*, CEDAM, Padova, 2016.

OSCE. *Legislation Online*, disponível em: https://www.legislationline.org/download/id/3521/file/Case_of_Leander_v_Sweden_1987_en.pdf, acesso em: 29/03/2023.

ORLANDO, S. "I limiti della tutela penale del tratamento illecito dei dati personali nel mondo digitale*", Diritto Penale Contemporaneo*, Tribunale de Milano, Milano, 2019.

PAGALLO, U. *La tutela della 'privacy' negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano, 2008.

PICOTTI, L. *Il diritto penale dell'informatica nell'epoca di internet,* Cedam, Roma, 2005.

PROSSER, W.L. "Privacy*", California Law Review*, nº 3, vol.48, Berkeley, 1960.

PROPUBLICA. *Investigative Journalism in the Public Interest*, *In*: https://www.propublica.org, acesso em 14/04/2023.

RODOTÀ, S. *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

_____. *Il mondo nella rete – quali i diritti, quali i vincoli*, Laterza, Roma, 2014.

RM. *Convenção de Budapeste*, disponível em: https://rm.coe.int/16802fa428, acesso em: 13/04/2023.

STF. ADC 51, disponível em:http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379, acesso em: 11/04/2023.

STJ. REsp nº 1806792/SP, disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp, acesso em 14/04/2023.

TAYLOR, Mark. Genetic data and the law – a critical perspective on privacy protection, Cambridge University Press, New York, 2012.

UOL. *Vazamento do facebook*: descubra se seus dados foram expostos, disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/04/05/vazamento-do-facebook-descubra-se-seus-dados-foram-expostos.htm, acesso em: 08/04/2023.

VLEX. *Pavesich V. New England Life Insurance Co.*, disponível em: https://case-law.vlex.com/vid/pavesich-v-new-england-888103034, acesso em: 14/04/2023.

WARREN, S. & BRANDEIS, L.D. "The Right of Privacy*"*, *Harvard Law Review*, vol.4, nº5, December,15, Boston, 1890, pp.193/220, disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf, acesso em 08/03/2023.