

A proteção de dados pessoais e a atuação do Ministério Público enquanto garantia institucional

Emerson Garcia*

Sumário

Introdução; 1. Direito à intimidade e à vida privada; 2. Direito à autodeterminação informativa; 3. O direito fundamental à proteção dos dados pessoais; 4. A Lei Geral de Proteção de Dados Pessoais; 5. O Ministério Público enquanto garantia institucional; 6. O dever de proteção e a estruturação administrativa do Ministério Público; Conclusão; Referências bibliográficas.

Resumo

O artigo busca contribuir para a compreensão de como a intimidade pode dialogar com a autodeterminação informativa e o direito fundamental à proteção de dados, em um ambiente tecnológico em que a pessoa humana, voluntariamente, muitas vezes comprime sua própria intimidade. A partir daí, podemos avançar na funcionalidade do Ministério Público enquanto garantia institucional que deve participar ativamente do dever de proteção desses bens e valores, de modo a assegurar a sua efetividade.

Abstract

This paper seeks to contribute to the understanding of how privacy can interact with informational self-determination and the fundamental right to data protection, in a technological environment in which a human being, voluntarily, often compresses his or her own privacy. From there, we can advance in the functionality of the Public Prosecutor's Office as an institutional guarantee that must participate in the duty to protect these assets and values, in order to guarantee its effectiveness.

Palavras-chave

Ministério Público; dados pessoais; intimidade; internet; dever de proteção; garantia institucional.

* Doutor e Mestre em Ciências Jurídico-Políticas pela Universidade de Lisboa. Especialista em *Education Law and Policy* pela *European Association for Education Law and Policy* (Antuérpia – Bélgica) e em Ciências Políticas e Internacionais pela Universidade de Lisboa. Membro do Ministério Público do Estado do Rio de Janeiro, Consultor Jurídico da Procuradoria-Geral de Justiça e Diretor da Revista de Direito. Consultor Jurídico da Associação Nacional dos Membros do Ministério Público (CONAMP). Membro Honorário do Instituto dos Advogados Brasileiros (IAB).

Keywords

Public Prosecutor's Office; personal data; privacy; internet; duty to protect; institutional guarantee.

Introdução

A influência da tecnologia sobre a humanidade tem sido não só intensa como disruptiva (GARCIA, vol. 1, 2023: 172-173). Modos de vida são alterados, facilidades construídas e novas dificuldades enfrentadas. O fenômeno também se projeta nas relações do cidadão com as estruturas estatais de poder. A denominada democracia digital reflete o uso da comunicação e da informação tecnológica, em todas as espécies de mídia, com o objetivo de ampliar a participação política dos cidadãos, o que se dá sem os limitadores de tempo e espaço, bem como de outras condicionantes físicas, próprias do ambiente analógico. Cf. Kenneth L. Hacker e Jan van Dijk (2000: 1). Há autores, no entanto, que são pessimistas em relação à possibilidade de a tecnologia, com destaque para a rede mundial de computadores, efetivamente mudar a democracia, considerando as instituições tradicionais, ao que se soma “a diferença entre falar e ser ouvido” (HINDMAN, 2009: 16).

Limites e oportunidades oferecidos pela democracia digital tendem a apresentar variações conforme o arquétipo de democracia adotado e, principalmente, o modo como se projeta na realidade. Em uma democracia procedimental, na qual as atenções são direcionadas aos requisitos formais de acesso ao poder, sem a correlata preocupação com certos objetivos relacionados à participação política, as manifestações no ambiente digital tendem a ser analisadas apenas sob essa perspectiva. Democracias competitivas, nas quais a preocupação é direcionada à preservação da igualdade entre os concorrentes, de modo a evitar que fatores outros, que não os ideológicos, influam no pleito, tendem a dispensar especial atenção às possibilidades de acesso e ao uso dos meios digitais. Democracias pluralistas buscam assegurar que todas as correntes de opinião possam ser ouvidas, o que também se reflete na possibilidade de acesso à comunicação e à informação tecnológica. Na democracia plebiscitária, a preocupação é direcionada à outorga de legitimidade a decisões previamente tomadas pelas estruturas estatais de poder, de modo que as atenções não são direcionadas ao engajamento popular no processo formativo dessas decisões. Na democracia participativa, o objetivo almejado é o de ampliar o nível de conscientização e de interação dos cidadãos, de modo que possam efetivamente participar do processo decisório, não se limitando à escolha dos seus representantes. Por fim, na democracia libertária, são apregoados níveis máximos de liberdade, com intervenção mínima do Estado, o que se projetará na existência de reduzidos balizamentos na comunicação e na informação digital. Cf. Jan Van Dijk (2000: 39 e ss.).

A democracia digital se desenvolverá em conformidade com certos padrões de comunicação e de informação, que podem ser divididos em (a) alocação, caracterizada pela transmissão unilateral da informação; (b) consulta, na qual são recuperadas

informações disponíveis na rede mundial de computadores; (c) registro, no qual as manifestações individuais são declinadas, de modo a alcançar um propósito específico (v.g.: televoto); e (d) conversação, em que se verifica a troca de experiências, informações e opiniões (v.g.: mensagens eletrônicas). Cf. Jan Van Dijk (2000: 46-47).

São muitos os aspectos positivos da democracia digital, que se manifestam em diversas vertentes do processo de interação política. Em primeiro lugar, é exponencialmente ampliada a facilidade de acesso aos documentos públicos e às políticas de governo, o mesmo ocorrendo em relação à possibilidade de os cidadãos encontrarem e se unirem a grupos políticos, ampliando com isso o universo de debate. Como desdobramento, as opiniões externadas são difundidas com rapidez e para além de qualquer fronteira física, além de tornar o debate mais plural. Daí se afirmar, como a Suprema Corte norte-americana, que *"o conteúdo da internet é tão diversificado quanto o pensamento humano"* (*Reno v. American Civil Liberties Union*, 521 U.S. 844, 1997). Na medida em que as opiniões são difundidas, tende a aumentar o nível de influência na formação da agenda e no processo decisório das estruturas estatais de poder que possuem legitimidade democrática, as quais, em razão das eleições periódicas, não podem permanecer de todo insensíveis aos anseios da coletividade. A tecnologia também aproxima os políticos dos cidadãos, eliminando mediadores.

De modo correlato aos aspectos positivos, há os negativos. O primeiro e mais perceptivo é uma espécie de degeneração da personalidade de alguns, que parecem ser alçados a um empoderamento ilimitado quando se encontram no controle do teclado, da câmara e do microfone. Para esses, não há limites. Perdem, por completo, a percepção de que se encontram sob a égide de um Estado de Direito e de uma ordem jurídica preestabelecida, praticando abusos de toda ordem. Conectada a essa constatação, surge o questionamento: todas as práticas de comunicação política, na democracia digital, devem ser consideradas democráticas, incluindo aquelas que busquem a derrocada da própria democracia e das políticas liberais de expansão do acesso individual ao sistema político? À evidência que não. Um sistema autofágico é uma *contradictio in terminis*. Admitir que o sistema democrático ampare iniciativas que almejem a sua destruição, como apregoar os benefícios da ditadura, não encontra amparo na lógica ou na razão, o que permite concluir que essa espécie de conduta deve ser considerada um ato ilícito.

Ainda existem outros complicadores a serem enfrentados: o efeito lesivo das *fake news* é sensivelmente potencializado em uma coletividade com baixa instrução e limitada capacidade crítica; o uso de robôs, difundindo opiniões favoráveis ou contrárias a certos aspectos da realidade, principalmente com a sua deturpação, pode acarretar sério desequilíbrio na disputa eleitoral; e algoritmos específicos, muito em voga entre os buscadores disponíveis na rede mundial de computadores, podem analisar as preferências pessoais do usuário e direcionar suas decisões — essa última prática é diariamente direcionada por interesses comerciais, mas pode ser facilmente utilizada em prol de ideologias ou interesses outros. Cf. Emerson Garcia (2020: 41).

Em relação aos fatores de desestabilização sistêmica do ambiente digital, a Carta portuguesa de Direitos Humanos na Era Digital (Lei n.º 27/2021) buscou remediar o seu potencial lesivo. Foi previsto que o Estado deveria assegurar o direito à proteção contra a desinformação, sendo assim considerada “toda a narrativa comprovadamente falsa ou enganadora criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que seja suscetível de causar um prejuízo público, nomeadamente ameaça aos processos políticos democráticos, aos processos de elaboração de políticas públicas e a bens públicos” (Art. 6º, 2).

Acresceu, ainda, que, no uso da inteligência artificial e de robôs, as decisões com impacto significativo na esfera dos destinatários, tomadas com o uso de algoritmos, devem ser comunicadas aos interessados, sendo suscetíveis de recurso e auditáveis (art. 9º, 2). O Estado, ademais, deve contribuir para o desenvolvimento da educação digital (art. 11).

A tendência é que cada Estado de Direito, direcionado pelos aspectos culturais do ambiente sociopolítico, busque moldar a respectiva democracia digital, de modo a ampliar a participação política dos cidadãos, maximizar os aspectos positivos e minimizar os negativos. No contexto das medidas protetivas, têm merecido atenção detida aquelas direcionadas aos dados pessoais, não só com a instituição de balizamentos afetos ao seu tratamento, como a atuação de instituições que possam atuar tanto no plano preventivo como no repressivo, sempre com o objetivo último de assegurar a higidez do bem jurídico tutelado.

Com os olhos voltados a essa constatação, dedicaremos algumas breves linhas à compreensão de como a intimidade pode dialogar com a autodeterminação informativa e o direito fundamental à proteção de dados em um ambiente tecnológico em que a pessoa humana, voluntariamente, comprime a referida intimidade. A partir daí, podemos avançar na funcionalidade do Ministério Público enquanto garantia institucional que deve participar ativamente no dever de proteção desses bens e valores, de modo a assegurar a sua efetividade.

1. Direito à intimidade e à vida privada

O direito à intimidade, ou *right to privacy* para os anglo-saxões, pode ser definido como a faculdade jurídica de manter fora do conhecimento público informações que só à pessoa interessam. O seu alicerce doutrinário remonta ao artigo intitulado *The right to privacy*, publicado por Samuel Denis Warren e Louis Dembitz Brandeis, este último futuro *justice* da Suprema Corte norte-americana, no final do século XX (1890: 193 e ss.). Os aspectos fáticos subjacentes ao texto estavam associados às colunas sociais de jornais que desnudavam a vida de personagens ilustres da sociedade, a exemplo de Warren, destacado advogado e industrial em Boston. Cf. GARCIA (vol. 2, 2023: 167 e ss.).

A compreensão do alcance desse direito, oponível não só ao Estado, como aos particulares, e que assume indiscutível relevância no livre desenvolvimento da

personalidade, exige que sejam devidamente compreendidos os referenciais de vida privada e de relevância social.

A vida privada compreende as ações iniciadas e concluídas num plano de análise cujos lindes envolvem tão somente a individualidade da pessoa humana ou um estrito círculo de relacionamento (v.g.: a família), sendo de reduzida ou de nenhuma relevância os pontos de contato com interesses afetos à coletividade (v.g.: assuntos afetivos inerentes à relação conjugal). Trata-se de esfera pessoal em que o indivíduo pode expressar livremente a própria identidade, quer sozinho, quer no relacionamento com terceiros (JAYAWICKRAMA, 2002: 604), alcançando a formação de sentimentos, hábitos, crenças, relações familiares e amizade. A preocupação com a intimidade já foi encampada por diversos atos de direito internacional. A Declaração Universal dos Direitos Humanos (art. 12), de 1948, dispôs que ninguém seria objeto de “interferências arbitrárias em sua vida privada”. A Convenção Europeia dos Direitos do Homem (art. 8º, 1), de 1950, e a Convenção Americana dos Direitos do Homem (art. 11), de 1969, também asseguraram o direito ao respeito à vida privada. Se o *modus vivendi* é voluntariamente levado ao espaço público pelo seu titular, qualquer que seja o móvel, a vida privada passa a assumir o colorido de vida pública.

Esses referenciais, no entanto, nem sempre evitarão o surgimento de dúvidas quanto à linha limítrofe entre as questões que só à pessoa interessam e aquelas que gerem reflexos na coletividade. Ao contextualizarmos a análise do problema em um Estado de Direito, pode-se afirmar que incumbe à ordem jurídica desempenhar a função de elemento de transposição, para o contexto social, de acontecimentos inicialmente situados no plano da vida privada. Justifica-se a conclusão na medida em que somente o Estado pode delinear os bens jurídicos a serem tutelados e estabelecer os padrões imperativos a serem seguidos, ainda que tal resulte numa contraposição de forças, de modo a afrontar a essência de determinadas realidades existenciais. Autoridades públicas, por exemplo, em especial aquelas eleitas pelo sufrágio universal, têm uma esfera de intimidade sensivelmente inferior ao *homo medius*, isso porque questões tipicamente afetas à esfera privada, como, por exemplo, o seu estado de saúde e as pessoas com as quais mantêm relações pessoais, podem influir na sua escolha pelos eleitores, passando a ostentar um inegável interesse coletivo; afinal, o falecimento prematuro, antes da conclusão do mandato, pode ensejar a sua substituição por um suplente indesejado ou, mesmo, a realização de novas eleições; o relacionamento com pessoas de moral e honestidade duvidosas pode ser indicativo de que o indivíduo comunga de valores similares, etc. Cf. Tommaso Amedeo Auletta (1978: 104-106).

O direito à intimidade é especialmente relevante não só por proteger a individualidade da pessoa, como, também, por oferecer um espaço para o livre desenvolvimento da personalidade. A proteção à intimidade pode ser concebida como a *ratio essendi* de inúmeros direitos fundamentais, como a liberdade de consciência e de crença (art. 5º, VI), a inviolabilidade do domicílio (art. 5º, XI) e a inviolabilidade do sigilo

da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII).

A preocupação com a intimidade tornou-se particularmente intensa face ao crescente aumento dos meios existentes para o conhecimento e a difusão da informação, o que aumenta o potencial lesivo de uma exposição pública indesejada (AULETTA, 1978: 4).

Cabe ao Estado regular a vida em sociedade e somente o Estado pode definir em que medida acontecimentos individuais são relevantes para a sociedade. Nessa linha, assumirão relevância social os acontecimentos que, inicialmente afetos à vida privada, transcendam a individualidade que a originou, quer em decorrência de uma violação à ordem jurídica (v.g.: a infração penal praticada a partir de uma discussão conjugal), quer pelo simples fato de a ordem jurídica considerá-los relevantes à coletividade (v.g.: a necessidade de intervenção judicial para a dissolução do vínculo conjugal). A assunção de relevância social, no entanto, não exige uma previsão normativa pormenorizada de todo e qualquer acontecimento da vida privada que desperte um legítimo interesse da coletividade. Em verdade, o que se exige é que tal interesse esteja amparado pela ordem jurídica, legitimando os atos que nele estejam baseados.

Ainda que seja lícita a divulgação da informação, a proteção à intimidade, à “realidade do indivíduo”, torna imperativo o seu comprometimento com a verdade, sendo injurídico qualquer ardil utilizado para manipulá-la ou afrontá-la (AULETTA, 1978: 10). Não sendo verificada a possibilidade de utilização do elemento de transposição anteriormente referido, terceiros somente poderão penetrar no plano da vida privada caso haja autorização de seu titular, que poderá realizar o controle dos atos daí resultantes ou mesmo retirar a autorização concedida.

2. Direito à autodeterminação informativa

O mundo contemporâneo tem se caracterizado por referenciais de facilidade e de celeridade na circulação da informação, que tanto pode dizer respeito a estruturas orgânicas, personalizadas ou não, quanto a indivíduos concebidos em sua individualidade. É factível existirem informações que, ontologicamente, não se afeiçoam ao conceito de privacidade, mas que, no extremo oposto, também estão longe de serem consideradas de interesse público. Em verdade, embora digam respeito à pessoa, são publicizadas na medida do seu interesse. A existência desse tipo de informação, caracterizado por um potencial de circulação limitado, certamente teve grande influência no delineamento da “autodeterminação informativa” (*informationelle Selbstbestimmung*), que nada mais é que o direito fundamental, atribuído a cada indivíduo, de decidir a quem devem ser entregues e como serão usados os seus “dados pessoais” (*personenbezogenen*). Cf. Marko Haselböck (2006: 4) e Florian Trost (2009: 3). A essência desse direito foi assim delineada pelo Tribunal Constitucional Federal alemão, ao apreciar a constitucionalidade da lei que disciplinava o “censo da população” (*Volkszählung*). Entendeu-se, à época, que o questionário a ser respondido

pelos recenseados deveria ser repassado às distintas esferas de governo com a omissão dos dados que permitissem a identificação dos cidadãos (65 *BVerfGE* 1, 1983). Afinal, cada indivíduo teria a faculdade de determinar “quando o Estado pode usar ou divulgar os seus dados pessoais”.

Gomes Canotilho (2003: 515) conceitua o direito à autodeterminação informativa como sendo a “faculdade de o particular determinar e controlar a utilização dos seus dados pessoais”. Sua relevância, na era da informação digital, é simplesmente incontestável, máxime quando lembramos, com Marko Haselböck (2006), a luta contra o terrorismo digital (*der digitalen Terrorismusbekämpfung*). A Constituição portuguesa de 1976, em seu art. 35, 3, dispõe que “a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis”.

No âmbito da União Europeia, a matéria foi disciplinada pela Diretiva n.º 95/46, “relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados”, que há de ser observada por cada Estado-Membro com a correlata adaptação de sua ordem interna. O art. 7.º da diretiva dispõe sobre a autorização do titular dos dados pessoais e as exceções que devem ser consideradas (v.g.: o disposto na alínea e – “O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados”).

3. O direito fundamental à proteção dos dados pessoais

A pessoa humana, tal qual um poliedro, pode ser compreendida e protegida em distintas perspectivas de análise. A Emenda Constitucional nº 115/2022, ao inserir o inc. LXXIX no art. 5º, preocupou-se com um aspecto em particular, a “proteção de dados pessoais”, inclusive nos meios digitais.

Pessoais, com escusas pela tautologia, são as informações afetas à pessoa. Informações dessa natureza assumem contornos bem mais amplos que aqueles protegidos pelo inc. X do mesmo art. 5º, que consagra a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Toda informação afeta à pessoa consubstancia um dado pessoal, mas nem todo dado pessoal retrata a sua intimidade ou a vida privada. Informações que a individualizem perante os órgãos públicos ou apontem o local de sua residência não dizem respeito ao círculo mais estreito de sua realidade existencial. Afinal, intimidade é aquilo que somente interessa a ela própria e a ninguém mais. A vida privada, por sua vez, alcança os distintos aspectos afetos à forma como a pessoa projeta a sua personalidade em um círculo estreito de relacionamentos, a exemplo do que se verifica com a família e os amigos, o que justifica a proteção da ordem jurídica (v.g.: o acesso ao teor de comunicações telefônicas, sem

o consentimento dos envolvidos, exige ordem judicial, nos termos do art. 5º, XII). Essas relações podem apresentar, ou não, relevância para o interesse público (v.g.: uma agressão praticada no ambiente familiar), também não sendo incomum que aspectos da vida privada sejam tornados públicos por iniciativa da própria pessoa, a exemplo do que se verifica rotineiramente nas redes sociais. Ressalte-se que a só publicização dos dados não transmuta a vida privada em pública. Afinal, os fatos não deixam de dizer respeito a círculos mais estreitos de relacionamento da pessoa. Da parcela não publicizada da vida privada advém o conceito de privacidade, que não apresenta uma relação de sobreposição com a intimidade, tendo contornos mais amplos. Registre-se que há quem associe a intimidade à vida particular (OLIVEIRA, 1980: 99).

Dados pessoais, portanto, albergam as informações afetas à intimidade e à vida privada, tanto na parte publicizada quanto na não publicizada. A reforma constitucional buscou ampliar a proteção individual ao inserir a norma programática do inc. LXXIX do art. 5º, cabendo à lei ordinária delinear a forma como essa proteção se tornará operativa. A esse respeito, em momento anterior à própria reforma, foi editada a Lei n.º 13.709/2018, que veiculou a Lei Geral de Proteção de Dados (LGPD). Também merece menção a Lei n.º 12.527/2011 (Lei de Acesso à Informação) e a Lei n.º 12.965/2014 (Marco Civil da Internet), que também estabeleceram mecanismos de proteção. A existência desse microsistema protetivo dos dados pessoais, com merecido destaque para a Lei n.º 13.709/2018, ao que se somava a tutela de situações existenciais dos titulares de dados, já tinha levado parte da doutrina a reconhecer que a proteção de dados consubstancia direito fundamental autônomo e implícito, alicerçado na liberdade, na intimidade, na vida privada e, em última *ratio*, na dignidade humana. Cf. Ana Frazão (2019: 103); e Ingo Wolfgang Sarlet (2020: 184), concepção que veio a ser formalmente acolhida pelo poder reformador.

Com o reconhecimento da fundamentalidade do direito, além da dimensão subjetiva, afeta aos respectivos titulares, não se pode descurar de sua dimensão objetiva, da qual se desprendem o direcionamento interpretativo dos demais enunciados normativos, constitucionais ou infraconstitucionais, e os deveres de (a) proteção, de modo que o Estado deve zelar pela sua observância por todos os atores do ambiente sociopolítico, públicos ou privados; (b) organização das estruturas estatais de poder, de modo a preservá-los; e (c) procedimento, que há de ser estruturado visando à sua efetividade. Cf. Ingo Wolfgang Sarlet (2020: 198).

A referência, contida na parte final do inc. LXXIX do art. 5º, de que a proteção dos dados pessoais também alcança aqueles que se encontram em “meios digitais”, torna-se particularmente relevante em razão da evolução da tecnologia a respeito do armazenamento e do acesso a dados. A “internet das coisas” é um nítido exemplo dessa perspectiva de análise. A internet passou a alcançar tanto computadores quanto diversos objetos utilizados no dia a dia, permitindo a comunicação e a troca de dados, de modo que provedores de serviço realizam o controle remoto dos objetos. Cf. Bárbara Brito de Castro (2019: 84-85). Com isso, os aspectos mais recônditos da existência

humana podem ser desnudados sem que a pessoa sequer perceba o desenvolvimento de um processo no qual figura como verdadeira protagonista.

A Emenda Constitucional n.º 115/2022 também concentrou na União a competência privativa para legislar sobre “proteção e tratamento de dados pessoais”, o que significa dizer que não mais subsiste o disposto no parágrafo único do art. 1º da Lei n.º 13.709/2018, segundo o qual esse diploma normativo apenas veicularia “normas gerais” a serem observadas pelos demais entes federativos. A partir da reforma, somente a União pode legislar sobre a temática, conforme passou a dispor o inc. XXX do art. 22. Também é incumbência desse ente federativo “organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei”, o que também foi previsto na Lei n.º 13.709/2018, que criou, inclusive, a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (arts. 55-A a 58-B). A Lei n.º 14.460/2022 transformou a ANPD em autarquia de natureza especial.

4. A Lei Geral de Proteção de Dados Pessoais

A Lei n.º 13.709, de 14.8.2018, tem origem no Projeto de Lei n.º 53/2018, cognominado pelos parlamentares de “marco legal de proteção, uso e tratamento de informações”. De acordo com sua epígrafe original, dispunha sobre “a proteção de dados pessoais”, o que veio a ser alterado, pela Lei n.º 13.853/2019, para “Lei Geral de Proteção de Dados Pessoais (LGPD)”.

A Lei n.º 13.709/2018 manteve a mesma estrutura do referido projeto de lei, à exceção dos vetos opostos pelo presidente da República. Inspirou-se no Regulamento Geral de Proteção de Dados (GDPR – *General Regulation for Data Protection*), lei europeia que está em vigor desde 25.5.2018. Mesmo em momento anterior, no direito europeu, o direito à proteção de dados era obtido a partir do direito à privacidade, encampado pelo art. 17 do Pacto Internacional dos Direitos Civis e Políticos, de 1966 e pelo art. 8º da Convenção Europeia dos Direitos do Homem, de 1950; e ainda de modo mais preciso, a partir da Convenção n.º 108, direcionada à Proteção dos Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, de 1981, sendo reforçado pelo art. 8º da Carta dos Direitos Fundamentais da União Europeia, de 2000. Este último preceito assim dispõe que: “1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”.

Especificamente em relação à GDPR, observa-se que esse diploma normativo visa a assegurar a proteção de dados dos cidadãos europeus, obrigando todas as sociedades empresárias de pequeno, médio e grande porte a investirem em

cibersegurança. Para tanto, estabeleceu obrigações direcionadas a todas as companhias que mantenham negócios com os países da União Europeia. É nesse contexto que foi editada a Lei n.º 13.709/2018. Outros países da América do Sul já tinham se antecipado na disciplina dessa temática: a Argentina em 2000, com a Lei n.º 25.326; e o Uruguai em 2008, com a Lei n.º 18.331.

A Lei n.º 13.709/2018 visa a estabelecer maior proteção aos titulares de dados, os quais passarão a ter maior controle sobre todo o processamento dos seus dados. O art. 5º ainda estabelece o conceito de (a) “*dado pessoal*”, assim entendido como qualquer informação que identifique diretamente ou torne identificável uma pessoa natural, o que denota a utilização de um “*conceito expansionista*”, distinguindo-se do dado anônimo, que não conduz à individualização de uma pessoa. Cf. Eduardo Ramos Caron Tesserolli e Rodrigo Pironti (2020: 65-66); (b) “*dado pessoal sensível*”, quando relativo à 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, os quais somente podem ser objeto de tratamento nas hipóteses do art. 11, formando o “*núcleo duro da privacidade*”, o qual tem potencial para a discriminação ilícita ou abusiva do titular. Cf. Gustavo Tepedino e Chiara Spadaccini de Teffé (2020: 104); (c) “*dado anonimizado*”, relativo a titular que não possa ser identificado, considerando os meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; (d) “*anonimização*”, assim considerado qualquer procedimento por meio do qual um dado deixa de poder ser associado, direta ou indiretamente, a um indivíduo. A lei define, ainda, a forma de armazenamento dos dados (banco de dados – art. 5º, IV), bem como os responsáveis pela manipulação desses dados (art. 5º, VI e VII).

Especificamente em relação aos dados pessoais, podem ser considerados como tais o nome, o endereço residencial, o correio eletrônico, o endereço IP (protocolo de *internet*), registros de conexão (*cookies*) etc., os quais possibilitam a identificação de uma pessoa. A LGPD, portanto, protege a identidade do denunciante em sua perspectiva mais ampla. Ainda é oportuno mencionar a distinção entre “*informação sigilosa*” e “*informação pessoal*”, o que foi objeto de distinção pela Lei n.º 12.527/2011 (Lei de Acesso à Informação). Esse diploma normativo estatuiu que, quer estejamos perante informação pessoal, quer perante informação sigilosa, o acesso a ambas é restrito: são consideradas informações sigilosas aquelas submetidas temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. A proteção das informações sigilosas é tratada no art. 25 da Lei n.º 12.527/2011, segundo o qual é dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando sua proteção. O acesso às informações sigilosas é restrito àqueles que tenham a necessidade de conhecer o seu teor. O Decreto n.º 7.845/2012, por exemplo, regulamentou procedimentos para credenciamento de segurança e tratamento da informação classificada em qualquer grau de sigilo.

Merecem especial destaque os direitos dos titulares dos dados pessoais, aos quais foi assegurado o acesso aos seus dados, podendo solicitar aos controladores que lhes forneçam todas as informações que mantêm sobre si, incluindo o direito de retificação das informações, bem como sua atualização (art. 18). Trata-se de desdobramento do direito fundamental à informação, contemplado no art. 5º, XXXIII, da Constituição de 1988, e da própria funcionalidade do *habeas data*, previsto no art. 5º, LXXII. Ainda é oportuno lembrar que a Lei n.º 12.965/2014 (Marco Civil da Internet) também assegurou uma série de direitos aos usuários em seu art. 7º, devendo ser destacados os direitos à inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação (inc. I); à inviolabilidade e ao sigilo do fluxo de suas comunicações pela *internet*, salvo por ordem judicial, na forma da lei (inc. II); e à inviolabilidade e ao sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial (inc. III). Também protegeu, em prol da privacidade, os dados pessoais e as comunicações privadas no âmbito da internet (art. 10); vedou a guarda, na provisão de conexão, dos registros de acesso a aplicações na internet (art. 14), estendendo a mesma vedação ao provedor de aplicações na internet (art. 16); além de dispor sobre a responsabilização civil do provedor de aplicações de internet caso sejam veiculados conteúdos à margem da ordem injurídica, o que pressupõe ordem judicial (art. 19).

A Lei n.º 13.709/2018 define duas espécies de agentes responsáveis pela manipulação de dados pessoais, (a) os “controladores”, responsáveis pelas decisões sobre o tratamento dos dados, e (b) os “operadores”, aqueles que tratam os dados por ordem dos controladores. Mais especificamente, é “responsável” a sociedade empresária, entidade ou órgão que tomar decisões em relação a como se dará o tratamento de dados pessoais e “operador” a sociedade empresária ou entidade vinculada ao “responsável” encarregada de realizar tais atividades. Essa distinção é relevante para se apurar as responsabilidades ante o dano causado ao titular dos dados. Afinal, sobre esses agentes recaem diversas obrigações, inclusive responsabilidades e o dever de reparação. O responsável pela gestão dos dados tem o dever de comunicar casos de “incidente de segurança”, como vazamentos, que possam trazer risco ou dano ao titular das informações (art. 48).

São princípios que regem a Lei n.º 13.709/2018: (i) o princípio da finalidade, por meio do qual os dados devem ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares; (ii) o princípio da adequação, pois somente devem ser coletados os dados mínimos necessários para que se possa atingir a finalidade; (iii) o princípio da retenção mínima, que determina a imediata exclusão dos dados, após atingida a finalidade para a qual foram coletados; e o (iv) princípio da prestação de contas, já que o cumprimento integral da norma precisará ser comprovado por todos os agentes que tratem com dados pessoais. E, ainda, necessidade, livre acesso, qualidade, transparência, segurança, prevenção e não discriminação.

O tratamento de dados pessoais, de modo geral, só é possível no termos do art. 7º: (a) com o consentimento livre e inequívoco; (b) para o cumprimento da obrigação legal pelo responsável; (c) pela Administração Pública, no exercício de direitos ou deveres; (d) para pesquisa histórica, científica ou estatística; (e) para a proteção da vida e tutela da saúde; (f) quando necessário para a execução de um contrato; (g) no exercício regular de direitos em processo judicial ou administrativo; e (h) se necessário, para atender aos interesses legítimos do responsável.

Especificamente em relação ao consentimento do titular dos dados pessoais, ele há de ser ofertado, quando necessário, em momento anterior ao tratamento dos dados. Trata-se de projeção da “autodeterminação existencial e informacional do ser humano” (TEPEDINO; TEFFÉ, 2020: 93). Para tanto, deve reunir os atributos referidos no art. 5º, XII, sendo livre, informado e inequívoco, de modo a permitir o tratamento dos dados pessoais para uma finalidade específica. Tratando-se de dados pessoais de acesso público, é dispensável o consentimento do titular para o seu tratamento, conforme dispõe o art. 7º, §3º.

No tocante à aplicação da lei por entidades públicas, inclusive quanto ao uso de banco de dados pelo Ministério Público em investigações de cunho não penal, o Capítulo IV detalha as normas e responsabilidades dos órgãos e setores públicos ante a proteção dos dados pessoais que utilizam, dispondo que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n.º 12.527, de 18.11.2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (arts. 23-32).

Note-se que o art. 4º da Lei n.º 13.709/2018 exclui do seu alcance o tratamento de dados pessoais para as finalidades ali referidas, entre as quais estão aquelas direcionadas à segurança pública, à defesa nacional, à segurança do Estado e às atividades de investigação e repressão de infrações penais, o que será regido por legislação específica. A *contrario sensu*, é possível afirmar que esse diploma normativo incidirá sobre as demais instâncias de responsabilização de caráter não penal, naquilo que diz respeito ao tratamento da informação. Entende-se por tratamento, nos termos do art. 5º, X: “toda operação realizada com dados pessoais, como os que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Esse tratamento recebeu uma sistemática específica, como se disse, em se tratando do Poder Público (Capítulo IV), devendo ser realizado para o atendimento de uma finalidade pública, o que deve ser feito de forma transparente, observadas as regras de segurança e de sigilo de dados (Capítulo VII, Seção I).

A Lei n.º 13.709/2018 ainda estabelece, em seu art. 22, que a defesa dos interesses e dos direitos dos titulares de dados pode ser exercida em juízo de maneira individual ou coletiva.

A Autoridade Nacional de Proteção de Dados (ANPD) foi prevista nos arts. 55-A a 55-L, da Lei n.º 13.709/2018, com a redação dada pela Lei n.º 13.853/2019. Trata-se do órgão central do sistema de proteção de dados, com “competências regulatória, fiscalizatória e punitiva” (art. 55-J, §4º), que poderia ser transformado em autarquia especial, conforme avaliação a ser realizada pelo Poder Executivo nos dois anos subsequentes à entrada em vigor de sua estrutura regimental (art. 55-A), que seria delineada pelo presidente da República (art. 55-G). Os membros do conselho diretor possuem mandato (art. 55-D, §§3º a 4º), e a ANPD deve exercer as competências referidas no art. 55-J. A referida transformação veio a ser efetivada pela Lei n.º 14.460/2022, que também revogou os §§1º a 3º do art. 55-A; o art. 55-B, segundo o qual à ANPD “é assegurada autonomia técnica e decisória”, o que parece ter tido o objetivo de restringir o seu juízo de valor aos balizamentos legais, ao menos em relação à referida autonomia técnica; e o inc. V do caput do art. 55-C, além de acrescentar um art. 55-M à Lei n.º 13.709/2018.

Por fim, o Conselho Nacional de Proteção de Dados (CNPD) foi previsto nos arts. 55-A a 55-L, da Lei n.º 13.709/2018, com a redação dada pela Lei n.º 13.853/2019. Trata-se de órgão essencialmente propositivo, buscando direcionar a atuação da ANPD, que exercerá livremente o seu juízo valorativo em relação às proposições apresentadas.

5. O Ministério Público enquanto garantia institucional

O fato de a Constituição da República, em seu art. 127, *caput*, ter considerado o Ministério Público uma Instituição permanente e essencial à função jurisdicional do Estado traz reflexos outros, limitando, igualmente, o próprio poder de reforma da Constituição. Com efeito, partindo-se da natureza da atividade desenvolvida pelo Ministério Público, toda ela voltada ao bem-estar da coletividade, protegendo-a, em especial, contra os próprios poderes constituídos, a sua existência pode ser considerada como ínsita no rol dos direitos e garantias individuais, sendo vedada a apresentação de qualquer proposta de emenda tendente a aboli-la (art. 60, § 4º, IV, da CR/1988).

A correção dessa conclusão pode ser igualmente visualizada a partir da análise do art. 129, II, da Constituição da República (“São funções institucionais do Ministério Público: (...) II – zelar pelo efetivo respeito dos poderes públicos e dos serviços de relevância pública aos direitos assegurados nesta Constituição, promovendo as medidas necessárias à sua garantia;”), que indica claramente a *ratio essendi* da atuação do Ministério Público.

Como a Instituição tem o dever jurídico de zelar pelos direitos alheios, tem-se o correlato direito de toda a coletividade a que tal efetivamente ocorra, daí a inequívoca incidência da norma do art. 5º, § 2º, da Constituição de 1988: “os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte”.

Por ser inócua a previsão de direitos sem a correspondente disponibilização de mecanismos aptos à sua efetivação, parece-nos que a preservação da atividade finalística do Ministério Público está associada à própria preservação dos direitos fundamentais, o que reforça a sua característica de cláusula pétrea e preserva a unidade do texto constitucional.

Além disso, a limitação material ao poder de reforma alcançará, com muito maior razão, qualquer iniciativa que, indiretamente, busque alcançar idêntico efeito prático (v. g.: redução das garantias e prerrogativas de seus membros e supressão da autonomia da Instituição, tornando-a financeiramente dependente do Executivo e, com isso, inviabilizando a sua atuação, que é o elemento indicativo de sua própria existência).

A existência do Ministério Público, assim, deve ser inserida no plano dos direitos-garantia, refletindo uma “garantia institucional” ao exercício de inúmeros direitos assegurados pela ordem constitucional, inclusive de cunho prestacional. Na lição de Paulo Bonavides (2006: 537), as garantias institucionais indicam “a proteção que a Constituição confere a algumas instituições, cuja importância reconhece fundamental para a sociedade, bem como a certos direitos fundamentais providos de um componente institucional que os caracteriza”.

6. O dever de proteção e a estruturação administrativa do Ministério Público

Ao se reconhecer que o Ministério Público brasileiro consubstancia relevante garantia institucional, não sendo incomum que se ponha a jusante de outras estruturas estatais de poder com o objetivo de proteger os direitos fundamentais, afigura-se evidente que a Instituição está funcionalmente comprometida com a efetividade do dever de proteção que recai sobre as estruturas estatais de poder.

A partir da dimensão objetiva dos direitos fundamentais, que tem sido reconhecida pelo Tribunal Constitucional Federal alemão, tem-se uma evidente simbiose entre os direitos de defesa (*Abwehrrechte*) tradicionalmente oponíveis ao Estado (POSCH: 15 e ss.; SCHOCH, 2000: 19) e o seu reconhecido monopólio do uso da força, somente afastado em situações excepcionais (v.g.: legítima defesa), daí decorrendo a obrigação de serem disponibilizados os meios necessários à tutela dos direitos individuais (ALEXY: 2001: 415-420). Os direitos de liberdade, desse modo, podem se transmutar em verdadeiros direitos prestacionais, impondo a adoção de ações positivas (*rectius*: medidas de proteção ou prevenção) por parte do Estado. Cf. *BVerfGE* 77, 170 (214), 1987 (*Lagerung chemischer Waffen*).

O “dever de proteção” tem se mostrado especialmente relevante face ao caráter dinâmico dos riscos sociais, que ultrapassam, com frequência, a esfera protetiva diretamente alcançada pela literalidade da ordem constitucional. Não é incomum que questões envolvendo a utilização de energia nuclear, tecnologia genética ou internet não tenham sido equacionadas pela Constituição, no âmbito dos direitos fundamentais, o que, em um plano estrito, em muito enfraqueceria a esfera de proteção individual (GRIMM, 2006: 85). Esse óbice, no entanto, tem sido contornado com a

identificação do dever de o legislador adotar as medidas necessárias à proteção da liberdade, evitando que a inércia estatal termine por estimular a sua desfiguração. Para tanto, são impostos limites a algumas liberdades ou às liberdades de alguns indivíduos específicos, quer com a restrição do seu potencial expansivo, quer com a imposição de obrigações de cautela (GRIMM, 2006: 141).

O dever de proteção, de acordo com Canaris, será tanto mais intenso quanto mais grave for a intervenção no direito fundamental e maior for o perigo que sobre ele se projete, mostrando-se o titular do direito incapaz de realizar a sua autoproteção, elementos que devem ser necessariamente cotejados com os direitos fundamentais contrapostos (CANARIS, 2003: 113-114).

Esse dever de proteção, longe de assumir contornos meramente formais, deve mostrar-se idôneo à preservação dos direitos fundamentais, daí a possibilidade de controle dos atos praticados pelo Estado com esse objetivo. Quanto à correta amplitude do dever de proteção, ela será encontrada a partir dos valores sociopolíticos que se projetam sobre a realidade e permitem o delineamento da norma constitucional protetora dos direitos fundamentais.

A teoria do dever de proteção é nítido exemplo da evolutividade do Estado de Direito, que transita da posição de opressor, o que justificava a imposição de limites aos seus atos, para a de parceiro operativo, atuando lado a lado com a pessoa humana em busca da concretização de direitos que outrora pressupunham justamente o seu distanciamento.

A estruturação administrativa do Ministério Público, embora comprometida com a tutela da generalidade dos direitos fundamentais, desde que enquadráveis na perspectiva mais ampla da defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis (CRFB/1988, art. 127, *caput*), há de ser constantemente moldada e remoldada para se ajustar às novas exigências do ambiente sociopolítico, o que se mostra particularmente relevante em relação às novas tecnologias e à proteção dos dados pessoais.

Para que a Instituição possa assegurar a proteção desses direitos, é essencial o monitoramento de iniciativas que tenham grande potencial lesivo aos interesses individuais, considerando o evidente interesse social envolvido, de modo a evitar que a esfera jurídica individual seja solapada em prol de interesses menos nobres, inclusive de cunho econômico. Algoritmos tendenciosos, deturpando a base de valores de uma sociedade ou oferecendo conteúdos prejudiciais ao próprio indivíduo; e a utilização indevida e escamoteada de dados pessoais, permitindo uma enxurrada de mensagens, muitas delas fraudulentas, veiculando *malwares*, *phishings* etc., são apenas alguns exemplos de condutas rotineiramente praticadas e que devem ser devidamente valoradas pelo Ministério Público para que seja efetivamente exercido o seu dever de proteção.

A existência de órgãos especializados, administrativos e de atuação funcional, tende a aumentar o nível de eficiência da Instituição. Afinal, aumentar a especialização

em um universo que é simplesmente reinventado em reduzidos lapsos temporais não é propriamente uma opção, mas uma estratégia de sofrimento; como se costuma dizer, ou acompanhamos a evolução ou nos perdemos no meio dela. Além disso, pode ampliar as portas de acesso para a generalidade das pessoas do ambiente sociopolítico, que saberão a que estruturas recorrer em situações corriqueiras do seu dia a dia.

Conclusão

De modo paradoxal, o avanço da tecnologia tem se mostrado não só benéfico como potencialmente lesivo para a coletividade, que não raro causa danos a si própria. A exemplo de todo e qualquer direito fundamental, a proteção de dados pessoais está funcionalmente vocacionada à proteção da pessoa humana. Assegurar que rompa a plasticidade de seus contornos semânticos e alcance a realidade é um dever de todas as estruturas estatais de poder, em especial do Ministério Público, garantia institucional que existe para servir à coletividade.

Referências bibliográficas

ALEX, Robert. *Teoria da argumentação jurídica (Theorie der Juristischen Argumentation)*. Trad. de Zilda Hutchinson Schild Silva. São Paulo: Landy, 2001.

AULETTA, Tommaso Amedeo. *Riservatezza e Tutela della Personalità*, Milano: Dott. A. Giuffrè Editore, 1979.

BONAVIDES, Paulo. *Curso de Direito Constitucional*. 18ª ed. São Paulo: Malheiros, 2006.

BRANDEIS, Louis Dembitz e WARREN Samuel Denis. *The right to privacy*. In: Harvard Law Review, vol. 4, p. 193, 1890.

CANARIS, Claus-Wilhelm. *Direitos fundamentais e direito privado*. Trad. de Ingo Wolfgang Sarlete e Paulo Mota Pinto. Coimbra: Almedina, 2003.

CASTRO, Bárbara Brito de. Direito Digital na era da internet das coisas – o direito à privacidade e a Lei Geral de Proteção de Dados Pessoais. In: *Revista Fórum de Direito na Economia Digital*, vol. 4, p. 79, 2019.

DIJK, Jan van. *Models of Democracy and Political Systems*, in Kenneth L. Hacker and Jan van Dijk. *Digital Democracy, issues of theory and practice*. London: SAGE, 2020, p. 30.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: Gustavo Tepedino; Ana Frazão; e Milena Donato Oliva. *Lei Geral de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 99.

GARCIA, Emerson. *Comentários à Constituição Brasileira*, vols. 1 e 2. Belo Horizonte: Editora Fórum, 2023.

_____. Democracia digital e eleições 2020. In: *Revista Justiça e Democracia*, nº 243, p. 41, nov./2020.

_____. *Ministério Público. Organização, Atribuições e Regime Jurídico*. 6ª ed. São Paulo: Editora Saraiva, 2017.

GRIMM, Dieter. *Constituição e política (Die Verfassung und die Politik)*. Trad. de Geraldo de Carvalho. Belo Horizonte: Del Rey, 2006.

HACKER, Kenneth L. and DIJK, Jan van. *What is Digital Democracy?*, in Kenneth L. Hacker and Jan van Dijk. *Digital Democracy, issues of theory and practice*. London: SAGE, 2020, p. 1.

HASELBÖCK, Marko. *Das Recht auf informationelle Selbstbestimmung im Kontext der digitalen Terrorismusbekämpfung*. Deutschland: Grin Verlag, 2006.

HINDMAN, Mathew. *The Myth of Digital Democracy*. Princeton: Princeton University Press, 2009.

JAYAWICKRAMA, Nihal. *The Judicial Application of Human Rights Law. National, Regional and International Jurisprudence*, Cambridge: Cambridge University Press, 2002.

OLIVEIRA, Moacyr de. Intimidade (Direito à). In: *Enciclopédia Saraiva do Direito*, vol. 46, p. 99, 1980.

POSCHÉ, Ralf. *Grundrechte als Abwehrrechte: reflexive Regelung rechtlich geordneter Freiheit*. Tübingen: Mohr Siebeck, 2003. p. 15 e ss..

SCHOCH, Friedrich. *Übungen im öffentlichen Recht: Verfassungsrecht und Verfassungsprozeßrecht*. Berlin: Walter de Gruyter, 2000.

TEPEDINO Gustavo e TEFFÉ, Chiara Spadaccini de. O consentimento na circulação da dados pessoais. In: *Revista Brasileira de Direito Civil*, nº 25, p. 83, jul./2020.

TROST, Florian. *Informationelle Selbstbestimmung – Persönlichkeitsrecht. Informationen als ökonomisches Gut – Ein Konflikt*. Deutschland: Grin verlag, 2009.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. In: *Direitos Fundamentais & Justiça*, nº 42, p. 179, 2020.

TESSEROLLI, Eduardo Ramos Caron e PIRONTI, Rodrigo. A Lei Geral de Proteção de Dados sensíveis e o tratamento pela Justiça Eleitoral. In: *Revista Fórum Administrativo*, nº 237, p. 64, nov./2020.