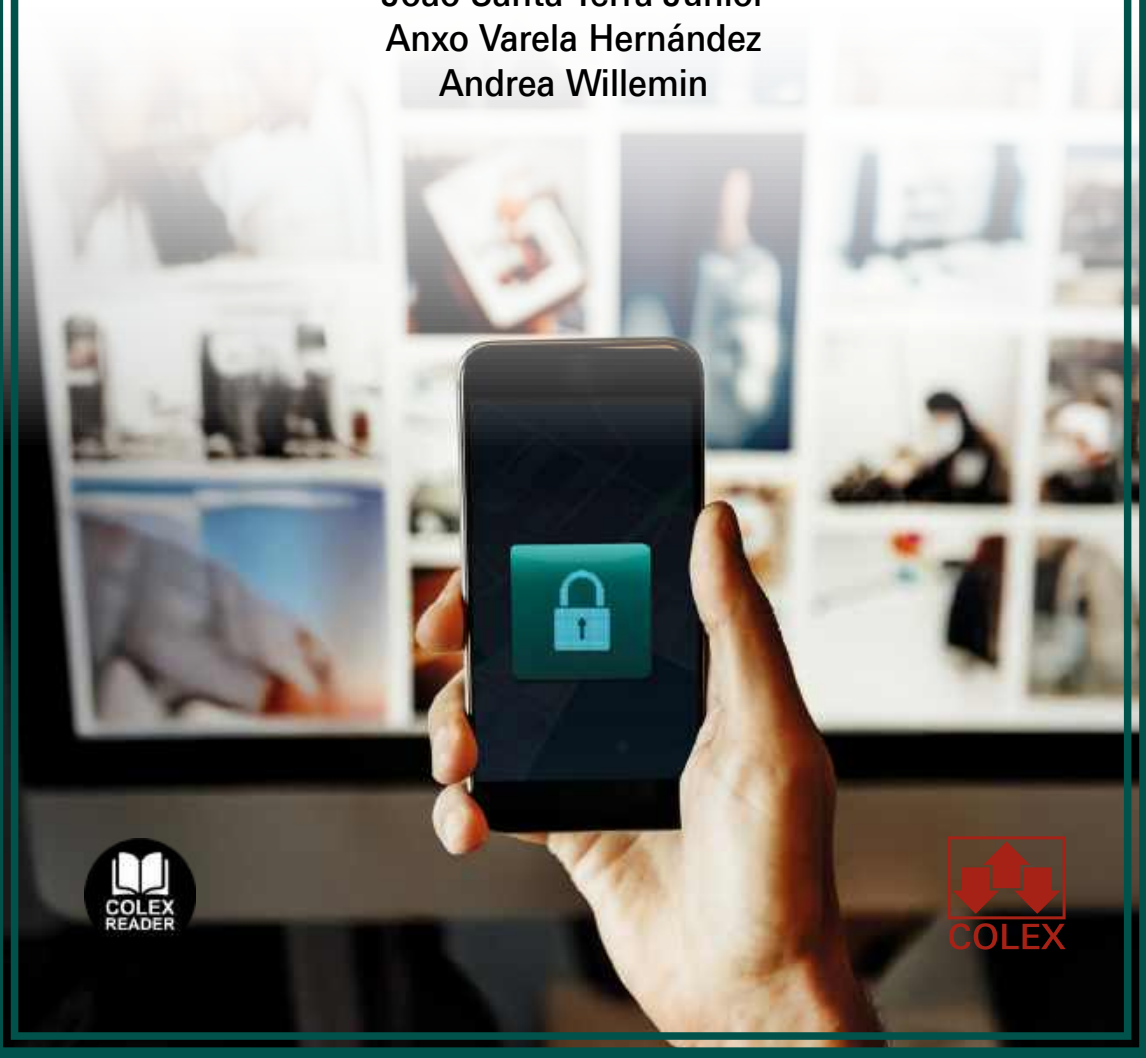
A PROTEÇÃO DE DADOS PESSOAIS SOB A ÓTICA DO MINISTÉRIO PÚBLICO BRASILEIRO

Diretores
João Santa Terra Júnior
Anxo Varela Hernández
Andrea Willemin



COLEX READER
COLEX

¡Gracias por confiar en nosotros!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook

Acceso desde cualquier dispositivo con conexión a internet

Idéntica visualización a la edición de papel

Navegación intuitiva

Tamaño del texto adaptable

Síguenos en:

A PROTEÇÃO DE DADOS PESSOAIS SOB A ÓTICA DO MINISTÉRIO PÚBLICO BRASILEIRO

A PROTEÇÃO DE DADOS PESSOAIS SOB A ÓTICA DO MINISTÉRIO PÚBLICO BRASILEIRO

Diretores

João Santa Terra Júnior

Anxo Varela Hernández

Andrea Willemin

COLEX 2025

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

SUMARIO

PREFÁCIO

La importancia de la protección de datos se colige fácilmente a partir de dos ideas-fuerza: por un lado, se trata de un derecho fundamental, que por ello garantiza ciertas facultades derivadas de la dignidad de las personas; y, por otro, este derecho es la respuesta jurídica específica a la problemática que ha planteado desde hace décadas el desarrollo de la tecnología. Así las cosas, su carácter de derecho fundamental y la incierta evolución tecnológica futura evidencian esa dimensión clave en los actuales sistemas democráticos.

Europa ha sido la punta de lanza en el asentamiento y construcción de la protección de datos a nivel mundial, evidenciando, una vez más, que el Viejo Continente apuesta habitualmente por la lógica de los derechos, aunque a veces la geopolítica difumina tal planteamiento. Las distintas normas europeas sobre este tema han sido ejemplo para otras partes del mundo, en especial entre los países del continente americano, como Argentina o Brasil. Aquí es forzoso traer a colación el actualmente vigente Reglamento UE 2016/679, general de protección de datos (RGPD), cuya influencia en parte trasformadora se manifiesta en varios aspectos, aunque existen otras normas relevantes de las que ahorramos la cita en este momento.

Así, el RGPD ha sido una clara inspiración para la armonización legislativa en otras latitudes, convirtiéndose en un modelo a seguir para la creación de marcos legales más robustos y protectores de la privacidad. Varios países iberoamericanos han revisado y actualizado sus propias leyes de protección de datos personales para alinearse con los principios y estándares del RGPD. Brasil es un claro ejemplo, con la promulgación de la Lei Geral de Proteção de Dados Pessoais en 2018 (con entrada en vigor en 2020), la cual está fuertemente inspirada en el RGPD al establecer obligaciones similares en cuanto a la recopilación, procesamiento, almacenamiento y transferencia de datos personales, así como los derechos de los titulares de los datos. En 2022 se da un paso más y se reforma la Constitución brasileña para integrar la protección de datos en sus derechos fundamentales (art. 5.LXXIX). También Argentina ha mirado de cerca a Europa. Este país ya contaba con una ley de protección de datos (Ley N° 25.326 de 2000) considerada "adecuada" por la Unión Europea, pero ha iniciado un proceso de actualización para armonizar su normativa con los nuevos lineamientos del RGPD. Se han presentado proyectos de ley que buscan incorporar aspectos como la ampliación del concepto de dato sensible, el consentimiento para niños a partir de los 13

años, y la evaluación de impacto en la protección de datos, entre otros. En Perú sucede algo parecido: este país andino cuenta con la Ley N° 29733 de Protección de Datos Personales, promulgada en 2011 y reglamentada en 2013. Si bien es anterior al RGPD, se han propuesto y se discuten continuamente reformas para modernizarla y acercarla a los principios y derechos del reglamento europeo. Por su parte, Colombia aprobó la Ley 1581 de 2012 (Ley de Protección de Datos Personales), también anterior al RGPD. Sin embargo, su interpretación y la jurisprudencia de la Corte Constitucional, así como las directrices de la Superintendencia de Industria y Comercio, han tendido a incorporar principios de buenas prácticas y derechos que son coherentes con el espíritu del RGPD, como la rendición de cuentas y la necesidad de consentimiento explícito.

En este sentido, el RGPD ha introducido conceptos como la responsabilidad proactiva (*accountability*), la obligación de notificar las violaciones de datos en plazos específicos (72 horas), y la necesidad de realizar evaluaciones de impacto de protección de datos. Estas prácticas están siendo adoptadas en diversas legislaciones iberoamericanas. También la lógica sancionadora europea ha sido vista con atención. Sin llegar a los niveles del RGPD, con multas que pueden alcanzar hasta el 4% de la facturación global anual de una empresa o 20 millones de euros, su influencia ha llevado a un endurecimiento de los regímenes sancionadores en la región. La Ley de Brasil, por ejemplo, prevé multas de hasta el 2% de la facturación de una empresa o hasta 50 millones de reales brasileños.

En suma, el RGPD ha actuado como un catalizador para la modernización y el fortalecimiento de las leyes de protección de datos en América Latina. Ha impulsado la adopción de un enfoque más riguroso y centrado al individuo en la protección de la privacidad, influyendo en la creación de marcos legales más completos, el reconocimiento de derechos más amplios y la imposición de mayores responsabilidades a las organizaciones que manejan datos personales.

Además, hay que tener presente el carácter extraterritorial del RGPD, lo que implica que cualquier empresa que ofrezca bienes o servicios a ciudadanos europeos, o que monitoree su comportamiento dentro de la UE, debe cumplir con ese Reglamento, sin importar dónde se encuentre la empresa. Esto ha obligado a muchas empresas americanas que tienen negocios con Europa a adaptar sus prácticas para cumplir con los estándares del RGPD.

Pues bien, el Ministerio Público del Brasil, con base en las relevantes funciones constitucionales que debe desempeñar, necesariamente debe asir con fuerza el reto de garantizar con eficacia el derecho fundamental de protección de datos. Se acercan tiempos de dudas e incertezas, cuando el salto tecnológico que ya hemos iniciado se abra a realidades todavía no vislumbradas en la actualidad. Por ello el Ministerio Público debe estar sometido a un proceso de actualización permanente, sobre todo en el campo de los derechos de las personas. El art. 127 de la Constitución federal

brasileña le otorga el rol fundamental de defensa del orden jurídico, del régimen democrático y de los intereses sociales e individuales indisponibles, lo que no hace más que enfatizar el papel esencial que debe desempeñar de forma continua esa institución para asegurar la calidad del sistema público. Y la protección de datos se registra con letras luminosas en esa encomiable tarea. Por estas razones en 2021 se crea la figura de encargados para el tratamiento de datos del Ministerio Público de Brasil, con atribuciones específicas en la garantía del cumplimiento de las obligaciones de protección de datos, a lo que habrá que sumar una capacitación permanente en el tema.

Saludo por lo tanto con fruición esta interesantísima iniciativa capitaneada por mis colegas y amigos João Santa Terra, Anxo Varela y Andrea Willemin, hábiles directores de la presente obra que han podido y sabido recopilar un sugerente grupo de trabajos que ahora se muestran al lector. Todos los autores son encargados de tratamiento en el Ministerio Público brasileño, lo que demuestra la concienciación digna de elogio que se ha instalado en esa institución. Se abordan temas dispares, pero todos bajo la cobertura de la protección de datos, un derecho que encuentra específicos problemas en las tierras brasileñas. Por ello, libros como este son necesarios en el momento presente para ofrecer un análisis riguroso de esos retos, aportar posibles soluciones y ofrecer ideas a los decisores públicos que mejoren el estándar normativo y aplicativo en protección de datos y privacidad.

En este sentido, se recogen trabajos sobre la posible reforma de la legislación penal para incrementar la efectividad del derecho de protección de datos, la tutela de ese derecho por el Ministerio Público, los desafíos que dicho Ministerio encuentra para garantizar la protección de datos, la aplicación de la normativa sobre protección de dados en el seno del Ministerio Público, el registro de operaciones de tratamiento, el específico caso de la actuación ministerial frente a Facebook y Google, la grabación audiovisual de las audiencias judiciales, el planeamiento estratégico nacional, y la contraposición entre el secreto de negocio y la transparencia algorítmica. Este rápido bosquejo a lo que viene a continuación evidencia el interés objetivo que presenta el libro y la preocupación de sus coautores por ofrecer aspectos relevantes que requieren un examen detenido para hallar soluciones.

No cabe duda de que la obra justifica la necesidad de una respuesta institucional robusta e integrada ante los obstáculos que se alzan para la eficacia de la protección de datos, lo que incluye la posible intervención del Derecho Penal para garantizar la efectividad de este derecho fundamental en la era digital. El texto recoge la interesante evolución legislativa en Brasil en esta temática, un largo camino que ha llevado más de 25 años, al mismo tiempo que enfatiza el rol del Ministerio Público en la defensa de este derecho fundamental, un rol central y diferenciado que abarca desde la fiscalización del cumplimiento de la normativa hasta la promoción de acciones civiles públicas y la defensa colectiva de los titulares de datos. Pero la obra también identifica los desafíos que impone la creciente digitalización

de las relaciones sociales y la complejidad de los flujos de información, incluyendo la "espectacularización" de las grabaciones audiovisuales en audiencias judiciales y la proliferación de la desinformación y el "linchamiento virtual". Asimismo, el libro subraya la relevancia del diálogo entre Europa y América Latina en la defensa de los datos personales, ya que la protección de datos todavía integra las agendas pendientes y en consolidación en América Latina. Realmente aún nos hallamos en una situación en la que urgen políticas públicas y normativas que integren aspectos tecnológicos, jurídicos y sociales para garantizar la efectividad de la protección de datos en el mundo tecnológico.

En fin, vivimos tiempos agitados, en los que la presión irreflexiva de lo cotidiano nos guía en demasiadas ocasiones. Frente a ello, los juristas debemos aportar elementos racionales que sean capaces de marcar el paso del sistema público. Este libro se inserta en esa línea, por lo que esperamos que logre una adecuada difusión de la que resulte un verdadero progreso en la nación hermana de Brasil.

José Julio Fernández Rodríguez

Catedrático de Derecho Constitucional

Universidad de Santiago de Compostela (España)

A Barcia, a 22 de julio de 2025

APRESENTAÇÃO DA OBRA

A proteção de dados pessoais no Brasil percorreu um longo caminho até alcançar o status de direito fundamental. Desde os primeiros debates sobre privacidade na década de 1990, passando pela promulgação do Marco Civil da Internet em 2014, até a entrada em vigor da Lei nº 13.709/2018 — a Lei Geral de Proteção de Dados Pessoais (LGPD) — o país consolidou seu arcabouço normativo voltado à tutela da autodeterminação informativa. Esse processo culminou, em 2022, com a promulgação da Emenda Constitucional 115, que inseriu expressamente a proteção de dados pessoais no rol dos direitos e garantias fundamentais da Constituição Federal, conferindo-lhe a máxima hierarquia jurídica no ordenamento brasileiro.

Nesse contexto, o Ministério Público brasileiro assume papel central e diferenciado na defesa desse direito fundamental. Diferente de muitos Ministérios Públicos europeus, cuja atuação na seara da proteção de dados é mais restrita ou especializada, o Ministério Público no Brasil possui atribuições constitucionais amplas e multifacetadas para a proteção dos seres humanos no âmbito metaindividual, que o colocam como verdadeiro guardião dos direitos fundamentais. Sua atuação abrange desde a fiscalização do cumprimento da LGPD por entes públicos e privados, até a promoção de ações civis públicas e a defesa coletiva dos titulares de dados.

Reconhecendo a importância dessa missão institucional, o Conselho Nacional do Ministério Público (CNMP) editou a Resolução 281/2023, que estabelece diretrizes para a implementação da proteção de dados pessoais no âmbito do Ministério Público brasileiro. Essa norma criou a figura do Encarregado pelo Tratamento de Dados Pessoais em cada unidade e ramo do MP, atribuindo-lhe responsabilidades específicas quanto à governança, conformidade e orientação interna sobre o tema. A resolução também prevê a capacitação contínua desses encarregados, como forma de garantir a efetividade da proteção de dados pessoais no seio da própria Instituição.

Foi nesse espírito que se realizou, em abril de 2024, curso de capacitação em proteção de dados pessoais promovido pelo *Centro de Estudios de Seguridad* (CESEG) da *Universidad de Santiago de Compostela* (USC), na Espanha, a pedido do Colégio dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público (CEDAMP). O evento contou com a participação de membros e servidores do Ministério Público brasileiro que

atuam diretamente com a proteção de dados pessoais, proporcionando um espaço de formação, reflexão e intercâmbio de experiências. Este livro é fruto direto dessa iniciativa.

A presente obra parte da constatação de que a proteção de dados pessoais, alçada à categoria de direito fundamental pela Emenda Constitucional nº 115/2022, exige uma resposta institucional robusta e integrada, especialmente por parte do Ministério Público. A atuação do MP, tanto na esfera administrativa quanto na judicial, revela-se essencial para garantir a efetividade desse direito em um cenário marcado pela crescente digitalização das relações sociais e pela complexidade dos fluxos informacionais.

Nesse âmbito, os artigos que compõem este livro foram organizados com o propósito de oferecer uma análise multidisciplinar e aprofundada sobre os desafios e perspectivas da proteção de dados pessoais no Brasil, com especial atenção à atuação do Ministério Público. Almeja-se, assim, permitir ao leitor compreender os fundamentos jurídicos, institucionais e tecnológicos que sustentam a tutela coletiva e penal dos dados pessoais.

A publicação, portanto, reúne artigos elaborados por alunos do curso, que compartilham suas vivências, desafios e propostas no exercício da função de encarregados pela proteção de dados pessoais. Mais do que um repositório de boas práticas, este livro representa um marco na construção de uma cultura institucional voltada à proteção de dados no Ministério Público brasileiro.

Cada artigo contribui, a seu modo, para o fortalecimento da cultura de proteção de dados no Brasil, oferecendo subsídios teóricos e práticos para a atuação do Ministério Público e demais instituições comprometidas com a defesa dos direitos fundamentais na era digital.

Esta obra retrata a relevância do diálogo entre a Europa e a América Latina na seara da defesa dos dados pessoais. Enquanto países europeus já contam com décadas de amadurecimento normativo e institucional sobre o tema, na América Latina a proteção de dados ainda é uma agenda em consolidação. A troca de conhecimentos, experiências e perspectivas entre esses contextos é essencial para o fortalecimento de uma abordagem global, cooperativa e eficaz na defesa da privacidade, da intimidade, da autodeterminação informativa e da dignidade humana na era digital.

A consolidação da proteção de dados pessoais como direito fundamental impõe ao ordenamento jurídico brasileiro o desafio de desenvolver uma doutrina específica que contemple as particularidades desse novo campo, especialmente no contexto da tutela coletiva dos direitos fundamentais. A atuação do Ministério Público, como defensor da ordem jurídica e dos interesses sociais, exige não apenas adequação normativa e institucional, reclama, também, a construção de fundamentos teóricos sólidos que orientem sua prática.

Nesse sentido, a presente obra representa uma contribuição inaugural e relevante para esse processo. Ao reunir reflexões de membros do Ministério Público e estudiosos do tema, o livro lança as bases para a edificação de uma doutrina própria, crítica e comprometida com a efetividade do direito fundamental à proteção de dados pessoais no Brasil. Trata-se de um passo essencial rumo à consolidação de um novo paradigma jurídico, capaz de responder aos desafios da sociedade da informação com responsabilidade, técnica e sensibilidade social.

João Santa Terra Júnior

Promotor de Justiça do Ministério Público do Estado de São Paulo e secretário de estudos e relações com Iberoamérica do Centro de Estudios de Seguridad (CESEG)

Anxo Varela Hernández

Professor do Departamento de Direito Público e Teoria do Estado da Universidade de Santiago de Compostela (USC) e secretário de publicações, convênios e relações com estudantes do Centro de Estudios de Seguridad (CESEG)

Andrea Willemin

Data Protection Officer, colaboradora da Unidade de Proteção de Dados Pessoais do Conselho Nacional do Ministério Público (CNMP) e secretária de desenvolvimento tecnológico e ciberseguridade do Centro de Estudios de Seguridad (CESEG)

Santiago de Compostela, 23 de junho de 2025

A NECESSIDADE DA EVOLUÇÃO DA LEGISLAÇÃO PENAL EM PROL DA EFETIVIDADE DA TUTELA DO DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS PESSOAIS PELO MINISTÉRIO PÚBLICO

Maria Fernanda Tonini Blazius de Oliveira[1]
Rui Carlos Kolb Schiefler[2]

Resumo: O presente estudo objetiva discutir o papel do Direito Penal na proteção de direitos fundamentais, com foco na proteção de dados pessoais [e explorar, inclusive, a interseção entre infrações administrativas e crimes correspondentes], e como tal implica na efetividade da sua tutela pelo Ministério Público. Busca exemplificar condutas que podem, após o devido debate e reflexão, ser tratadas pelo Direito Penal como típicas, na busca de uma efetiva proteção desse direito fundamental, inclusive a partir da identificação e indicação de uma série de figuras criminais já existentes nos ordenamentos pátrio e estrangeiro, resultantes da expansão do Direito Penal em outras matérias. Destaca a importância de uma política criminal assertiva, sob pena da construção de um direito penal ineficiente ou demasiado rigoroso. E espelhado no tratamento dispensado ao direito fundamental em voga não só pelo Estado, mas também por seus próprios titulares (seja por desconhecimento, seja por negligência), bem como na fragilidade dos atuais mecanismos de defesa no Brasil para proteção dos dados pessoais - ainda em descompasso com o desenvolvimento tecnológico mundial, justificante do reconhecimento da vulnerabilidade do indivíduo no meio digital -, conclui pela necessidade de evolução do Direito Penal no país, para enfrentar os desafios impostos pela modernidade, com a consequente maior intervenção pelo Ministério Público, porque titular exclusivo da ação penal pública.

---

1. Assessora jurídica do Ministério Público do Estado de Santa Catarina (MPSC).

2. Procurador de Justiça do Ministério Público de Santa Catarina (MPSC). Integrante da Unidade Especial de Proteção de Dados Pessoais (UEPDAP) do Conselho Nacional do Ministério Público (CNMP).

Palavras-chave: Ministério Público. Direito fundamental. Proteção de dados pessoais. Expansão do Direito Penal. Tipos penais.

Resumen: El presente estudio tiene como objetivo discutir el papel del Derecho Penal en la protección de los derechos fundamentales, enfocándose en la protección de los datos personales [e incluyendo la intersección entre infracciones administrativas y los delitos correspondientes], y cómo esto influye en la efectividad de su tutela por parte del Ministerio Público. Busca ejemplificar conductas que, tras el debido debate y reflexión, puedan ser tratadas por el Derecho Penal como típicas, en la búsqueda de una protección efectiva de ese derecho fundamental, incluso a partir de la identificación e indicación de una serie de figuras criminales ya existentes en los ordenamientos nacionales y extranjeros, resultado de la expansión del Derecho Penal a otras materias. Destaca la importancia de una política criminal asertiva, bajo pena de construir un Derecho Penal ineficiente o excesivamente rígido. Además, se refleja en el tratamiento otorgado al derecho fundamental en cuestión, no solo por el Estado, sino también por sus propios titulares (ya sea por desconocimiento o negligencia), así como en la fragilidad de los actuales mecanismos de defensa en Brasil para la protección de los datos personales, aún desajustados con el desarrollo tecnológico mundial, lo que justifica el reconocimiento de la vulnerabilidad del individuo en el ámbito digital-, concluye por la necesidad de una evolución del Derecho Penal en el país, para enfrentar los desafíos impuestos por la modernidad, con la consecuente mayor intervención del Ministerio Público, dado que es el único titular de la acción penal pública.

Palabras clave: Ministerio Público. Derecho fundamental. Protección de datos personales. Expansión del Derecho Penal. Tipos penales.

1. INTRODUÇÃO

A evolução humana, social e econômica das últimas décadas, somada ao impressionante desenvolvimento das tecnologias da informação e da comunicação, trouxe desafios significativos para a proteção dos direitos fundamentais previstos na Constituição da República Federativa do Brasil de 1988 (CRFB/88), em especial, no caso, o da proteção dos dados pessoais - incluído expressamente em nossa Magna Carta, precisamente em seu artigo 5°, inciso LXXIX, por meio da Emenda Constitucional n. 115/2022 -, elevando a preocupação com a privacidade, a dignidade e a segurança dos indivíduos.

Nesse contexto, questiona-se sobre a possibilidade de o Direito Penal emergir como um mecanismo de reforço na proteção desse novel e autônomo direito fundamental, especialmente por meio da tipificação de condutas que ameacem o tratamento, a sensibilidade, a integridade e a confidencialidade dos dados pessoais.

Este artigo reconhece a necessidade de uma articulação entre os ramos do Direito para uma melhor proteção dos direitos fundamentais, objetivando, em particular, discutir o papel do Direito Penal na proteção deles, com foco na proteção de dados pessoais [e, inclusive, explorar a interseção entre infrações administrativas e crimes correspondentes], e como tal implica a efetividade dessa tutela pelo Ministério Público.

A expansão do Direito Penal - fenômeno já observado no ordenamento jurídico brasileiro em outras áreas, como na tutela da Administração Pública e do consumidor, por exemplo -, estendida à proteção dos dados pessoais, reflete, necessariamente, em uma maior intervenção do Ministério Público na defesa desse direito, na medida em que é titular exclusivo da ação penal pública.

E não é só. Esse acréscimo aos instrumentos e meios de resguardo do direito à proteção dos dados pessoais, também por reflexo, resguardará seus pares, como o direito à liberdade, à igualdade, à dignidade, à privacidade e à segurança, evitando-se uma proteção ineficiente, com consequências ainda não conhecidas na sua totalidade [considerando-se o atual estágio e o que se prospecta do desenvolvimento da tecnologia, de um lado, e o desconhecimento, pela maioria da população mundial, do tratamento de dados pessoais em larga escala, de outro] -, tudo sem se olvidar do caráter fragmentário e subsidiário da matéria criminal.

A dúvida que se pretende dirimir - ou pelo menos se estabelecer, diante da dificuldade do tema - diz respeito exatamente a essa *quaestio*: pode o Direito Penal auxiliar no necessário combate aos visíveis abusos e na proteção do direito fundamental em testilha?

2. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Seguindo tendência mundial voltada à efetividade na proteção dos dados pessoais, inclusive e principalmente nos meios digitais, notadamente empós a aprovação do *General Data Protection Regulation* (GDPR) n. 2016/679, ocorrida em 27 de abril de 2016, com efeitos para além dos limites territoriais europeus, no Brasil foi editada a Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a qual entrou em vigor, na íntegra, apenas no mês de setembro de 2020.

A LGPD - impositiva tanto às pessoas naturais, quanto às pessoas jurídicas de direito público ou de direito privado, que realizem o tratamento de dados pessoais, e, tal qual o sobredito normativo estrangeiro, com efeitos extraterritoriais - surgiu como novo marco regulatório na proteção de dados pessoais, sobrevindo e alterando a Lei n. 12.965/2014 (Marco Civil da Internet) (Schiefler; Oliveira, 2019).

No ordenamento jurídico pátrio - em momento prévio à estruturação do recente arcabouço normativo de proteção dos dados pessoais, coroado com a disruptiva LGPD -, havia um entendimento de que os problemas relacionados a bancos de dados com informações pessoais seriam vencidos com um sistema mais simplificado, com autorização ou vedação para o uso de determinados dados, desprezando-se os riscos potencializados pelo tratamento informatizado dos dados pessoais. Parte da doutrina encarava a privacidade como um direito fundamental, enquanto relegava às informações pessoais uma preocupação restrita à inviolabilidade da comunicação de dados, resultando essa diferenciação de tratamento em uma potencial violação aos dados pessoais, nos casos em que a privacidade ou outros direitos fundamentais não fossem diretamente ofendidos (Doneda, 2021).

Bioni (2018) já destacava a necessidade de se reconhecer a autonomia do direito à proteção de dados pessoais, não atrelado a uma categoria determinada, mas sim como nova espécie do elenco dos direitos da personalidade.

Sem destoar, acompanhando os estudiosos do tema, Artese (2019) reconheceu imprescindível a discussão da matéria a partir dos direitos fundamentais, ressalvando, porém, que o ponto nodal da proteção de dados pessoais é que o tratamento deles constitui atividade de risco, devendo aquele que a realizar assumir esse risco e se responsabilizar por eventuais danos causados ao titular.

Nesse cenário, em 3 de julho de 2019, foi apresentada pelo Senado Federal brasileiro a Proposta de Emenda Constitucional (PEC) n. 17/2019, propondo a alteração da Constituição Federal de 1988 para incluir a proteção de dados pessoais no rol dos direitos e das garantias fundamentais e para estabelecer a competência privativa da união para legislar a respeito da proteção e do tratamento desses dados.

No mês de maio de 2020, recordam Frazão, Carvalho e Milanez (2022, p. 65/67):

> [...] ao referendar a Medida Cautelar concedida pela Ministra Rosa Weber, relatora das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, o Supremo Tribunal Federal reconheceu o direito fundamental à proteção de dados como direito autônomo, extraído a partir da leitura e interpretação sistemática do texto constitucional brasileiro.
>
> Tratava-se da edição da Medida Provisória 954, de 17 de abril de 2020, que determinou que as empresa de telecomunicações prestadoras do Serviço Telefônico

> Comutado (STFC) e do Serviço Móvel Pessoal (SMP) compartilhassem, em meio eletrônico, dados pessoais de seus consumidores, mais especificamente dos seus nomes, números de telefone, endereços, para que a Fundação Instituto Brasileiro de Geografia e Estatísticas (IBGE) realizasse entrevistas em caráter não presencial no âmbito de pesquisas domiciliares para produção estatística oficial[3][...].

A referida PEC foi aprovada, por unanimidade, em 10 de fevereiro de 2022, e publicada no dia seguinte nos Diários Oficiais da União, do Senado Federal e da Câmara dos Deputados, sendo convertida na Emenda Constitucional n. 115/2022, que, entre outros, acresceu o inciso LXXIX ao *caput* do artigo 5° da CRFB/1988, *verbis*: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

A partir de então, o direito à proteção dos dados pessoais, inclusive nos meios digitais, passou a figurar expressamente como direito fundamental na CRFB/88, exigindo, como tal, diferenciada atenção, a exemplo do que se propõe no presente estudo: acrescer à legislação criminal brasileira previsão de tipificação e punição para condutas ofensivas específicas ao direito à proteção de dados pessoais, em prol da efetividade da sua tutela, notadamente pelo Ministério Público.

Aliás, nesse cenário, merece destaque a recente edição, pelo Conselho Nacional do Ministério Público brasileiro, da Resolução CNMP n. 281, de 12 de dezembro de 2023[4] - a qual instituiu a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público -, normativa de vanguarda e que firma a posição da Instituição no enfrentamento de tão importante temática no âmbito nacional (com repercussão para além das fronteiras brasileiras).

3. A FUNÇÃO E A EXPANSÃO DO DIREITO PENAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DOS DADOS PESSOAIS

Na constatação de que a vida em sociedade precisa ter limites contra abusos, além de regras de convivência pessoal, coletiva e social - sob pena de não ser possível o estabelecimento de uma sociedade de humanos -,

---

3. Curiosamente, a controvérsia do [...] julgamento do Tribunal Constitucional alemão de 1983 tinha como pano de fundo a realização de pesquisas estatísticas para elaboração do censo alemão de 1982 e, era, portanto, análoga ao caso enfrentado em 2020 pelo STF. Ambos culminaram no debate a respeito dos riscos advindos da coleta massiva de dados pessoais pelo Estado e da possibilidade de cruzamento das informações retidas com aquelas constantes em outros bancos de dados estatais. Ver: MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumir: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014 (Nota dos autores).

4. Disponível em <https://www.cnmp.mp.br/portal/atos-e-normas/norma/10515>.

exsurge o Direito Penal, dentre outros mecanismos de controle e ação, como um conjunto de normas jurídicas voltadas exatamente para essa finalidade: controle e pacificação social.

E, resumidamente, para que serve o Direito Penal?

Tradicionalmente, é o ramo do Direito que impõe as sanções mais severas para condutas consideradas lesivas à sociedade, de forma imperativa e geral, impessoal e abstrata, possuindo particular papel na proteção de direitos fundamentais, sendo crucial, pois é por intermédio da tipificação criminal que o Estado sinaliza a importância de certos bens jurídicos e estabelece limites claros para a conduta dos indivíduos e das organizações. É a explicitação da sua utilidade, ou seja, do caráter preventivo-geral do Direito Penal.

Já que a finalidade do Estado - ditando normas necessárias à harmonia e ao equilíbrio sociais - é a convivência humana, isto é, "a consecução do bem coletivo" (Noronha, 1987, p. 94), sendo violado esse bem pela prática de um crime exsurge a necessidade também social-coletiva, via Direito Penal, de se tentar buscar evitar tais condutas e, elas ocorrendo, de uma reação punitiva.

Entende-se como bem aquilo que satisfaz as necessidades da existência do indivíduo na vida em sociedade, podendo ser um bem comum, inclusive, quando reúne condições éticas e materiais basilares para a coletividade.

Em uma primeira perspectiva, aliás, pode-se até dizer que o Direito Penal existe para impor limites ao poder-dever punitivo soberano do Estado. E, nessa seara, seleciona condutas que passam a ser consideradas proibidas, que passam a ser tipificadas como infrações penais, às quais são impostas as sanções correspondentes, dentro de uma escala de menor e maior gravidade e necessidade de retribuição.

Sob outro enfoque, esse regramento criminal estatal traz à lume um estado democrático de condutas e regras, é repetir, a imposição de limites ao próprio poder punitivo estatal, com princípios e regras previstas em lei que garantem a segurança jurídica necessária à sociedade para que ela saiba quais são as condutas estabelecidas. Somente essas condutas selecionadas e tipificadas - excepcionais - é que passam a compor o rol de infrações penal e socialmente relevantes. Aqui, registre-se, há que se respeitar a Carta Magna e a legislação penal, no sentido de se dar a máxima efetividade aos direitos e às garantias fundamentais, sobretudo ao princípio da reserva legal ou da legalidade estrita, previsto no art. 5º, inciso XXXIX, da CRFB/88, assim como ao art. 1º do Código Penal brasileiro (1940), que reza: "Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal".

Ainda, sob outro viés, pode-se afirmar que o Direito Penal trata de regras que protegem a sociedade em geral e que tentam garantir a vida em sociedade, longe da barbárie e da lei do mais forte. Serve, em outras palavras,

para assegurar as condições de existência em sociedade e a continuidade da organização social. É o Direito Penal visto como o direito de defesa da sociedade contra a ameaça permanente do crime.

A respeito, segundo Masson (2017, p. 9):

> O Direito Penal tem como função a proteção de bens jurídicos, isto é, valores ou interesses reconhecidos pelo Direito e imprescindíveis à satisfação do indivíduo ou da sociedade[5]. [...] A proteção de bens jurídicos é a missão precípua, que fundamenta e confere legitimidade ao Direito Penal.

Da mistura desses múltiplos e resumidos entendimentos - e de tantos outros -, para o que importa no presente trabalho, pode-se firmar o caráter retributivo e a função utilitária do Direito Penal, o qual, aliás, "está se convertendo, cada vez mais, em um instrumento de direção ou orientação social, sobretudo em matéria de tutela de bens jurídicos transindividuais" (Prado, 2010, p. 65).

Daí que o direito fundamental à proteção dos dados pessoais, neste sentido, exsurge e constitui um bem jurídico novo, digno de tutela penal, dada a sua relevância para a dignidade, a liberdade e a privacidade dos indivíduos.

Porém, ao que consta e se deduz, atualmente não tem sido protegido, nem aqui, tampouco em outros países, ao menos de forma eficaz e direta.

4. O DIREITO PENAL E A POLÍTICA CRIMINAL: CORRELAÇÃO NECESSÁRIA

O Direito Penal, por outro lado, tem total relação com a Política Criminal, a qual influencia na escolha das condutas e dos institutos político-jurídicos sociais, na missão do controle social pelo direito penal. A Política Criminal, de seu turno, "tem no seu âmago a específica finalidade de trabalhar estratégias e meios de controle social da criminalidade (caráter teleológico)", sendo-lhe "característica [...] a posição de vanguarda em relação ao direito vigente, vez que, enquanto ciência de fins e meios, sugere e orienta reformas à legislação positivada" (Cunha, 2023, p. 36).

A correlação da Política Criminal com o Direito Penal, portanto, sobreleva-se, na medida em que ambas possuem a missão de solucionar conflitos de diversificadas espécies. No presente caso em estudo, conflitos decorrentes do novo direito fundamental em voga.

---

5. Para uma análise minuciosa do assunto: Roxin, Claus. A proteção de bens jurídicos como função do direito penal. Org. e trad. André Luís Callegari e Nereu José Giacomolli. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2006 (Nota do autor).

A propósito, como defende Dotti, os crimes devem ser combatidos tanto por instâncias formais como materiais. Nesse sentido, por instâncias formais deve-se compreender: "a lei, a Polícia, o Ministério Público, o poder Judiciário, as instituições e os estabelecimentos penais." (Dotti, 2018, p. 85). Já as instâncias materiais são aquelas compreendidas como não penais, não repressivas e não estatais, que se apartam da esfera penal, como "a família, a escola, a comunidade (associações, sindicatos) etc." (Dotti, 2018, p. 85).

Há muito, sobre a relação do Direito Penal com a Política Criminal, Noronha (1987, p. 17) ensina que:

> [...] consideram-na alguns como o estudo dos meios de combater o crime depois de praticado; outros, entretanto, ampliam-lhe o conteúdo, para a conceituarem como crítica e reforma das leis vigentes. A maioria nega-lhe caráter científico, reduzindo-a antes à arte de legislar em determinado momento, segundo as necessidades do povo e de acordo com os princípios científicos imperantes. É ela crítica e reforma. Crítica quando examina e estuda as instituições jurídicas existentes, e reforma quando preconiza sua modificação e aperfeiçoamento.

E depois conclui: "Compreende-se sua estreita relação com a dogmática penal, porque pertence a esta a crítica objetiva da legislação vigente, e é dela que se há de partir para novas concepções e mesmo para a criação de um novo direito" (Noronha, 1987, p. 17).

Já para Santa Terra Júnior (2023, p. 324):

> [...] entre as principais decisões político-criminais a serem alcançadas por um Estado despontam-se aquelas relativas à escolha por um maior ou menor nível de intervenção estatal nas liberdades individuais em prol da efetividade da tutela penal, isso, principalmente, por meio de opções legislativas concernentes à criminalização ou à descriminalização de condutas, e quanto à elevação ou à redução do sancionamento penal de hipóteses já contempladas em tipos penais incriminadores. A Revolução tecnológica das comunicações e das informações ocasionou um tsunami de demandas político-criminais nessas duas específicas searas que resultou, como acima afirmado, em uma irrefreável (e ainda necessária) expansão do Direito Penal.

Há de se ter bem clara, portanto, qual a política criminal que serve de base na construção do Direito Penal em determinada sociedade e época, para se evitar um direito criminal muito brando ou, ao contrário, muito rigoroso; em ambos os casos, insuficientes ao equilíbrio e à harmonia social pela aplicação desse poder-dever do Estado. A ausência de uma política criminal correta, equilibrada e, principalmente, bem definida, pode implicar um ordenamento jurídico-penal desconexo, insuficiente, mal construído e injusto, com falhas, omissões e até contradições, sobrecarregando as instituições públicas na busca da proteção de direitos e na tutela social.

A propósito, Nucci (2023, p. 5) pontua que "qualquer país que pretenda acertar na criação de leis para o combate à criminalidade necessita, antes, ter uma política criminal definida. É justamente o que carece no Brasil".

Nesse viés, cumpre dizer que, além do combate à criminalidade, no Brasil há a carência da efetividade da implementação dos direitos fundamentais mínimos, mais caros ao cidadão, entre eles, no recorte, a proteção dos dados pessoais. Daí a necessidade de se buscar a interação do Direito Penal com as demais áreas do conhecimento, notadamente a proteção de direitos, forçando a implementação dos direitos fundamentais como exercício da cidadania e dos direitos humanos.

Será que, portanto, o Direito Penal pode ser essa força, essa diretriz, essa "ameaça legal extra" a ser utilizada com esse desiderato: a ameaça/possibilidade estatal da punição para aquele que não respeitar o direito fundamental da proteção de dados pessoais? É dizer: o Direito Penal pode servir, com eficácia/efetividade, à proteção de direitos fundamentais? No caso, ao direito fundamental da proteção dos dados pessoais? Teria esse caráter intimidatório da coletividade, segundo a doutrina de Feuerbach?

Para se buscar uma resposta, vale, antes, uma contextualização. Entre os fenômenos da tecnologia e do desenvolvimento - máximas que estão em pleno vigor na sociedade atual -, temos, no centro, o ser humano, ente portador e titular de dados pessoais. Exatamente esses dados pessoais - já atualmente considerados como o novo petróleo, de enorme valor e sensibilidade, portanto - é que são o objeto do uso das tecnologias em busca do desenvolvimento e, na mesma medida, por isso, precisam ser protegidos.

Aliás, nesse trilhar, Frazão, Carvalho e Milanez (2022, p. 24) comentam que, "vistos como o novo petróleo, os dados hoje são insumos essenciais para praticamente todas as atividades econômicas e tornaram-se eles próprios objeto de crescente e pujante mercado, no contexto do que Klaus Schwab denominou 'Quarta Revolução Industrial'[6]. Não é sem razão que se cunhou a expressão *data-driven economy*, ou seja, economia movida a dados, para designar a centralidade da extração e do uso de dados pessoais no capitalismo do século XXI".

Outrossim, sobre a temática, Santa Terra Júnior (2023*,* p. 318) também escreve:

> [...] Ainda sob a perspectiva sociológica, com a revolução tecnológica e a expansão do mundo virtual, nasceu um novo ator social: o ser humano virtual. A personalidade virtual, na atualidade, pode ser elencada como nova modalidade

6. Schwab, Kalus. The fourth industrial revolution. Genebra World Economics Forum, 2016. p. 56 (Nota do Autor).

> de personalidade fictícia, uma peculiar espécie de personalidade que se soma às pessoas físicas ou naturais e às outras pessoas fictícias, as pessoas jurídicas (dispostas no Título II, do Código Civil brasileiro). Com a personalidade virtual, incomensuráveis reflexos vem ocorrendo no plano jurídico, pois, ela carrega consigo distintos direitos inerentes à sua natureza fático-virtual (como, por exemplo, o respeito à privacidade virtual, a manutenção da identidade virtual, a liberdade de expressão no ambiente virtual etc.), os quais fundamentam a exigência de proatividade estatal para sua tutela, com efetiva proteção normativa e concreta responsabilização daqueles que maculam tais direitos.

O que o autor defende - a necessidade da incrementação do Direito Penal para um combate mais efetivo à cyberdelinquência ou à criminalidade virtual no cyberespaço - também pode ser defendido quando se almeja utilizar o mesmo Direito Penal na proteção dos direitos fundamentais e, no caso, da efetiva tutela pelo Ministério Público, do direito fundamental à proteção dos dados pessoais. Pois é nesse ambiente novo e virtual, então, de uma falsa invisibilidade, de uma errada sensação de que ninguém está sendo visto, de que não há dono nem regras de convívio social, que direitos individuais e bens jurídicos sociais - fundamentais ou não - são expostos e exercidos, sem que se tenha ainda evoluído na esfera do direito penal, para que uma efetiva, rápida e justa proteção estatal possa ser reivindicada/aplicada, como conclui o autor.

E será que há a necessidade e a possibilidade, nesse novo cenário onde fatos sociais acontecem, de uma maior ou mais específica intervenção estatal protetiva? É para tanto que serve o Direito Penal? A tutela penal tem condições de, também, auxiliar na efetivação desse importantíssimo direito fundamental?

A busca a uma boa resposta, continua. Pois a ideia de criminalizar condutas em prol da efetiva proteção de direitos fundamentais, é claro, precisa ser sopesada com a ideia de um Direito Penal mínimo, ou melhor, do princípio da intervenção mínima, segundo o qual somente na proteção de bens jurídicos realmente importantes e vitais à vida em sociedade é que deve se preocupar esse ramo do Direito. Nesse caso, parece não haver dúvidas, no momento político atual, da relevância do direito fundamental da proteção dos dados pessoais.

N'outra medida, como ensina Greco (2011, p. 77), em homenagem ao princípio da proporcionalidade, há que se ponderar, sempre, entre "a proibição do excesso *(Übermassverbot)* e a proibição de proteção deficiente *(Untermassverbot)".*

Acontece que, insiste-se, referente ao novel direito fundamental da proteção dos dados pessoais, inexistem dúvidas de se tratar de um desses cruciais direitos fundamentais, valiosíssimo, talvez de valor único e vital: "Nós somos dados", como ensina Andrea Willemin, decorrendo dessa afirmação todos os demais direitos.

E é quando os outros ramos do Direito fraquejam, revelando-se insuficientes ou incapazes de proteger devidamente os bens jurídicos mais valiosos para a sociedade, que exsurge o Direito Penal como uma solução político-jurídica nesse mister. Os ramos do Direito, nessa hipótese, como deve ser, unem-se em prol da efetividade da proteção de direitos/bens jurídicos.

Então, no debate aqui proposto, não há dúvidas quanto à deficiência atual da tutela do direito fundamental da proteção dos dados pessoais, invocando-se e justificando-se a intervenção do Direito Penal, também, portanto, nesse sentido.

Parecem ser intoleráveis, maldosas, astutas, dissimuladas e graves as formas como estão sendo perpetradas as agressões a tão valioso bem jurídico. Na mesma medida, parecem ser altamente lesivas tais agressões, havendo sérias consequências e ofensas a direitos dos titulares dos dados pessoais, algumas, até, ainda, desconhecidas.

E não se fale em tolerância, indiferença, parcimônia ou consentimento tácito dos titulares em relação ao uso desenfreado e malicioso de seus dados pessoais, por empresas e terceiros - incluindo-se robôs -, atualmente. Não há uma adequação social em relação a esse fenômeno. O que há, na verdade, é o contrário, pois a ignorância das pessoas acerca das malfadadas consequências dos perfilamentos e maldosos tratamentos que estão sendo feitos, de seus dados pessoais, geralmente à sorrelfa, torna essa prática totalmente inadequada no ambiente social, potencializado no ambiente virtual.

Daí a expansão do Direito Penal, no ponto, como um fenômeno necessário, uma realidade a ser buscada conquanto útil ao que aqui se busca defender: também o Direito Penal na proteção dos direitos fundamentais - e, especificamente no caso, da proteção dos dados pessoais do titular - parece ser uma ferramenta imprescindível, na sua essência.

E, para tanto, essa expansão necessariamente terá que significar o aperfeiçoamento, a contemporaneidade, a modernização desse fenômeno político-jurídico. Tem-se um bem jurídico valioso, uma lesividade (desvalor do resultado) palpável e significativa, com a identificação de possíveis comportamentos humanos inadequados e que são, daí, penalmente relevantes (desvalor da ação).

A respeito do expansionismo penal, Suxberger e Gomes Filho (2016, p. 377) pontuam:

> A expansão do direito penal, com a tutela de novos bens jurídicos a partir da segunda metade do século XX, sempre foi um fenômeno discutido pela Política Criminal. Muitas vezes abordada sob uma perspectiva negativa, a expansão do Direito Penal é confrontada pela contribuição do Direito Penal iluminista, que se apresentaria como única conformação do poder punitivo estatal em consonância com os princípios constitucionais de um Estado Democrático de Direito.
>
> [...]

> É certo que a tutela de bens jurídicos individuais como a vida, a liberdade e o patrimônio não constituem o único espaço de atuação do Direito Penal nas legislações atuais. Os bens jurídicos supraindividuais, também chamados de coletivos e difusos, como o meio ambiente, as relações de consumo, a ordem econômica e financeira passaram a constituir objeto da tutela penal.

Esse o caso, pois, do direito fundamental à proteção dos dados pessoais, cuja imprescindibilidade e urgência da tutela eclodiu nessa era de tratamento massificado e sorrateiro dos dados pessoais, decorrente do ininterrupto e acelerado desenvolvimento das tecnologias da informação e da comunicação.

Nesse cenário, presente uma política criminal definida e moderna, consentânea com as novidades sociais e, notadamente, com os conflitos, desafios e segredos desse novo mundo presente - principalmente no mundo virtual, onde tudo parece ser possível, porém, por certo, nem tudo é possível, tampouco permitido -, conclui-se pela necessidade da intervenção do direito penal no debate em testilha.

E, no momento, parece estar havendo uma proteção deficiente de tal direito fundamental. É possível afirmar, até, mais do que isso, que na verdade essa proteção é inexistente, haja vista a ausência de previsão de punição pela sua violação também na esfera penal.

Ainda mais se se considerar que, no atual estágio, o titular desse direito fundamental não tem ideia - sequer noção - da importância desse novo direito fundamental que lhe é inerente e constitucionalmente garantido, quiçá das possíveis e graves agressões, repita-se, de que pode estar sendo vítima.

Ensina Andrea Willemin que o titular dos dados pessoais, hoje, no Brasil, é um absolutamente incapaz, totalmente ignorante, a desafiar a proteção estatal inclusive por intermediação de um curador, que será, na maioria das vezes, o próprio Ministério Público brasileiro, guardião dos direitos conforme previsão constitucional.

Sim, nos termos do artigo 129, inciso I, da CRFB/1988, é função institucional e privativa do Ministério Público promover a ação penal pública na forma da lei, enquanto a tutela dos direitos difusos, embora também esteja inserta nas suas atribuições (artigo 127, *caput*, da CRFB/1988), é fracionada com outros autores.

Assim, é correto afirmar que a efetividade da tutela do direito fundamental à proteção de dados pessoais pelo Ministério Público perpassa, inevitavelmente, pela existência de previsão de punição de condutas que violem esse novel direito fundamental também na seara penal. Novas condutas sociais (a serem) acrescidas ao rol de ações penalmente relevantes, (a serem) combatidas e punidas, visando-se, sempre, frise-se, à proteção de direitos fundamentais e à pacificação e o controle social.

Em prol da proteção do direito fundamental invocado precisam ser identificadas e tipificadas as condutas jurídica e politicamente danosas à segurança dos cidadãos, que perturbem a tranquilidade pessoal e social, que provoquem danos imediatos (ao ofendido) e mediatos (alarme ou repercussão social).

Isso porque, há de se reconhecer que o direito fundamental à proteção dos dados pessoais ainda é um bem jurídico desprotegido normativamente, a despeito da sua enorme importância; a despeito de se tratar atualmente de um direito fundamental consagrado e que, muitas vezes, inclusive, é dele que derivam os demais direitos fundamentais, como a liberdade e a dignidade da pessoa humana. É um bem jurídico desvalorizado, esquecido, cujos titulares são relapsos na sua compreensão e proteção.

E, também, não se cogite, *in casu*, de se tratar de um direito penal de emergência ou simbólico, isto é, de uma sugestão de inflação legislativa penal para tratar de qualquer fato social ou conduta. Definitivamente a proteção dos dados pessoais não é um bem jurídico menor ou menos valioso que tantos outros, como a liberdade, a vida, a honra e a dignidade humana. A ideia é que se aumentem os instrumentos legais em favor do titular dos dados pessoais, inclusive penais, sem que tal constatação signifique uma tutela simbólica ou derivada de uma política criminal de menos valia.

A propósito, como aqui se defende, esse fenômeno da utilização do Direito Penal para forçar a concretização de direitos e valores pode ser constatado em outras áreas do direito brasileiro, como, por exemplo, no Direito Administrativo, na área de licitações públicas e contratos administrativos. Da mesma forma, na área ambiental, do consumidor e da proteção dos direitos das crianças e dos adolescentes. Na área tributária, inclusive. E na proteção/regulamentação do trânsito brasileiro, entre outros exemplos.

Por certo, com o passar do tempo, algumas condutas que até então apenas tinham repercussão na seara administrativa, por política criminal e opção social-legislativa, em determinado momento, foram alçadas à categoria de infrações penais e passaram a incrementar a legislação penal visando a essa finalidade.

E, repise-se, não são institutos simbólicos ou inaplicados.

De fato, como dito, existem na legislação pátria, hoje, infrações administrativas na área de licitações públicas e contratos administrativos que também são consideradas condutas tipificadas como criminais. A legislação brasileira estabelece uma série de normas e procedimentos para a realização de licitações e a execução de contratos administrativos, visando garantir, como princípios, notadamente, a legalidade, a impessoalidade, a moralidade, a igualdade, a publicidade, a eficiência e a obtenção da proposta mais vantajosa para a administração pública. Desvios dessas normas podem configurar, então, na prática, tanto infrações administrativas quanto penais, dependendo da natureza e da gravidade da conduta.

Um exemplo claro dessa dualidade pode ser observado no contexto da Lei n. 8.666/1993 (Lei de Licitações e Contratos), a qual, apesar de revogada pela Lei n. 14.133/2021 (Lei de Licitações), ainda fornece uma base relevante para compreender a matéria.

A Lei n. 8.666/1993 previa, em seus artigos 89 a 98, uma série de condutas ilícitas no âmbito das licitações e contratos, tratando de crimes específicos, como a dispensa indevida de licitação (art. 89) e a modificação ilegal de contrato administrativo (art. 92), com penas que incluíam detenção e multa. Adicionalmente, o Código Penal brasileiro (1940), em sua Parte Especial, foi acrescido do Capítulo II-B – Dos Crimes em Licitações e Contratos Administrativos, por meio dos artigos 337-E a 337-M, como indicado no contexto fornecido. Esse capítulo aborda uma variedade de crimes relacionados a licitações e contratos administrativos, como a "contratação direta ilegal" (art. 337-E), a "frustração do caráter competitivo de licitação" (art. 337-F) e a "contratação inidônea" (art. 337-M), demonstrando a seriedade com que o ordenamento jurídico trata tais infrações, aplicando-lhes penas de reclusão e multa.

Além disso, a Lei n. 12.846/2013, conhecida como Lei Anticorrupção, estabelece "atos lesivos à Administração Pública", que podem ser perpetrados por pessoas jurídicas contra a administração pública nacional ou estrangeira. Essa Lei contempla, em seu artigo 5º, condutas que, embora sejam inicialmente tratadas no âmbito administrativo e civil, podem ter correlatos penais, especialmente quando envolvem fraudes em licitações, a obstrução de investigações ou a oferta de vantagens indevidas a agentes públicos.

Portanto, é evidente que uma série de infrações administrativas relacionadas a licitações e contratos administrativos possuem correspondentes criminais, sendo passíveis de sanções tanto no âmbito administrativo, quanto no penal, com o objetivo de coibir e punir práticas ilícitas que comprometam a integridade e a transparência dos procedimentos licitatórios e da execução contratual na administração pública.

O mesmo fenômeno observa-se, por exemplo, quanto às seguintes infrações de natureza administrativa e aos equivalentes crimes contra as relações de consumo, respectivamente: artigo 12, inciso II, do Decreto n. 2.181/1997 e o artigo 7º, inciso VI, da Lei n. 8.137/1990; artigo 12, inciso IX, do Decreto n. 2.181/1997 e o artigo 63 da Lei n. 8.078/1990 (CDC); e o artigo 13, inciso I, do Decreto n. 2.181/1997 e o artigo 66 do CDC.

Além desses, merecem destaque - porque incluem, em certa medida, a proteção de dados pessoais - a infração administrativa do artigo 13, inciso XIV, do Decreto n. 2.181/1997 - "Art. 13. Serão consideradas, ainda, práticas infrativas, na forma dos dispositivos da Lei nº 8.078, de 1990: [...] XIV - deixar de corrigir, imediata e gratuitamente, a inexatidão de dados e cadastros, quando solicitado pelo consumidor; [...]" -, a qual encontra seu correspondente penal no artigo 73 do CDC, *verbis*: "Art. 73. Deixar de corrigir

imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata: Pena Detenção de um a seis meses ou multa".

E não é só. Relativamente ao direito fundamental ao meio ambiente ecologicamente equilibrado, consagrado no *caput* do artigo 225 da CRFB/1988, denota-se que o próprio texto constitucional expressamente dispõe que os infratores ambientais se sujeitam a punições penais e administrativas, independentemente da reparação civil pelos danos provocados[7]. No campo infraconstitucional, esse duplo sancionamento pode ser observado na Lei n. 9.605/1998, que prevê responsabilização criminal e administrativa pela prática de condutas e atividades lesivas ao meio ambiente.

Por derradeiro, também a defesa das crianças e dos adolescentes é multidisciplinar, a exemplo da Lei n. 8.069/1990, que prevê, em seu Título VII, os crimes e as infrações administrativas puníveis no seu âmbito, sendo possível afirmar, por exemplo, que a infração administrativa disposta no artigo 249[8] encontra equivalentes nas infrações penais dos artigos 236[9] e 238[10].

5. TIPOS PENAIS QUE TRATAM DO DIREITO FUNDAMENTAL À PROTEÇÃO DOS DADOS PESSOAIS

Então, esse mesmo raciocínio precisa ser transplantado agora diante do surgimento desse novel desafio: a proteção dos dados pessoais como direito fundamental de cidadãos/titulares que, na sua grande maioria, nem

---

7. Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.
[...]
§ 3º As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados.

8. Art. 249. Descumprir, dolosa ou culposamente, os deveres inerentes ao poder familiar ou decorrente de tutela ou guarda, bem assim determinação da autoridade judiciária ou Conselho Tutelar:
Pena - multa de três a vinte salários de referência, aplicando-se o dobro em caso de reincidência.

9. Art. 236. Impedir ou embaraçar a ação de autoridade judiciária, membro do Conselho Tutelar ou representante do Ministério Público no exercício de função prevista nesta Lei:
Pena - detenção de seis meses a dois anos.

10. Art. 238. Prometer ou efetivar a entrega de filho ou pupilo a terceiro, mediante paga ou recompensa:
Pena - reclusão de um a quatro anos, e multa.
Parágrafo único. Incide nas mesmas penas quem oferece ou efetiva a paga ou recompensa.

sequer sabe da existência desse direito, dando azo, nesse cenário, a um ambiente propício a abusos e desrespeitos por parte daqueles que querem tirar vantagens dessa incapacidade.

Dados pessoais valem ouro, tem valor incomensurável e, reunidos, planilhados e perfilados -muito fácil e rapidamente pelo processo *big data*-, podem significar muito, alavancar um aplicativo, dar suporte milionário a um influenciador, mover a indústria farmacêutica, o mercado financeiro, demonstrar tendências, criar mundos paralelos e problemas de toda monta, dentre outras consequências.

É verdade que igualmente podem significar avanços excepcionais, muito bons mesmo, em várias áreas de inovação, pesquisa e desenvolvimento social. A tecnologia é sensacional, um marco inevitável, e é a grande propulsora do desenvolvimento mundial. Dessa afirmação não há qualquer dúvida. Sem falar que é um caminho sem volta, um fenômeno que jamais será revertido pelo ser humano. Nem é o caso de se almejar esse retrocesso.

Mas o questionamento é inevitável: será com a tecnologia que o ser humano viverá mais e cada vez melhor? Será? Oxalá que sim, todavia, não se tem essa certeza toda, pois, na mesma medida, com a tecnologia e avanços virtuais, levantam-se mazelas e problemas. É um caminho desconhecido da grande parte da população mundial.

Pois esse mundo novo pode ferir direitos, como o da privacidade, da intimidade, da dignidade, ou seja, os direitos mais básicos de cada cidadão. Discriminação, preconceito e dores são gerados. Na verdade, em alguns cenários, parece não existir mais limites aos abusos no tratamento ilegal, ilícito, desleal e perigoso dos dados pessoais dos cidadãos, em total descompasso com a eleição de tal proteção à categoria de direito fundamental.

Sim, a garantia fundamental à proteção de dados pessoais requer um regime jurídico robusto que contemple não apenas medidas preventivas e administrativas, mas também a previsão de sanções penais para as violações mais graves. A tipificação de crimes relacionados à violação de dados pessoais serve como um mecanismo de dissuasão eficaz contra condutas que possam comprometer a segurança e a privacidade dos dados, reforçando o compromisso do Estado na proteção desse direito fundamental e permitindo uma maior ingerência do Ministério Público na conservação desse direito, porque, repita-se, é o titular exclusivo da ação penal pública.

Atualmente, destaque-se, há um rol de condutas violadoras da proteção dos dados pessoais que podem ser corriqueiramente detectadas e que infelizmente são usuais do dia a dia na sociedade. Práticas que são verificadas na interação com o mundo virtual ou até mesmo com o mundo real. Nesse sentido, entre tantas outras, merecem atenção: falta de consentimento; falta de segurança da informação; retenção excessiva de dados pessoais; monitoramento excessivo; transferência e compartilhamento ilegal de dados pessoais; uso inadequado de dados pessoais sensíveis; *marketing* não

solicitado[11]; perfilamento social, financeiro, político, sexual e religioso a partir de acesso indiscriminado e indevido a dados pessoais sensíveis; e falta de acesso e retificação a bancos de dados com informações pessoais.

Sem dúvida, situações como essas acontecem diariamente nas relações interpessoais e interorganizacionais. A Comunidade Europeia, sabe-se, possui uma estrutura administrativa avançada e muito bem organizada, que se debruça sobre tais questões na esfera administrativa, possuindo experiência na capacitação, fiscalização e no combate de tais abusos. Aplica multas e determina ações de correção e de proteção, no lídimo exercício de atribuições de suas autoridades administrativas constituídas[12]. Em casos mais graves, a conduta pode desbordar até para uma atuação na esfera criminal, já que se está diante de um direito fundamental que precisa ser protegido.

Muito a propósito, entre outras condutas violadoras ao direito à proteção dos dados pessoais, o Código Penal alemão[13] prevê os crimes de "disseminação perigosa de dados pessoais" (Seção 126a), de "violação da privacidade da palavra falada" (Seção 201), de "violação da privacidade íntima e dos direitos da personalidade ao tirar fotografias ou outras imagens" (Seção 201a) e de "espionagem de dados" (Seção 202a), este último assim traduzido por Decomain (2014, p. 269):

> Seção 202a. Espionagem de dados. (1) Quem, de modo não autorizado, mediante suplantação da segurança de acesso, obtém para si ou para outrem dados, que não lhe são destinados e que são especialmente contra acesso não autorizado, é punido com pena privativa de liberdade de até três anos ou com pena pecuniária.
>
> (2) Dados, no sentido da alínea 1, são apenas aqueles que são armazenados ou transmitidos eletrônica ou magneticamente, ou de outra forma não imediatamente acessível.

O Código Penal suíço[14] igualmente traz previsões protetivas ao direito do titular dos dados pessoais, a exemplo dos crimes de "ouvir e gravar as conversas de outras pessoas", de "gravação não autorizada de conversas", de "obtenção de dados pessoais sem autorização", dispostos no artigo 179. Além desses, vale destacar o artigo 321 do Códex Criminal helvético, *verbis*:

---

11. Quem nunca recebeu uma propagando, via e-mail ou aplicativo de mensagem, a partir de remetente desconhecido, não autorizado?

12. Maiores informações podem ser verificadas no sítio de internet da Autoridade Europeia para a Proteção de Dados (<https://www.edps.europa.eu/_en>), que recentemente completou 20 anos.

13. Disponível em: <https://www.gesetze-im-internet.de/englisch_stgb/>. Tradução livre.

14. Disponível em: <https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en>. Tradução livre.

> Violação do sigilo postal ou de telecomunicações
> Artigo 321
> 1 Qualquer pessoa que, na qualidade de funcionário público, empregado ou auxiliar de uma organização prestadora de serviços postais ou de telecomunicações, revele a terceiros detalhes de correspondência, pagamentos ou telecomunicações de clientes, abra correspondência lacrada ou tente descobrir o seu conteúdo, ou permite a um terceiro a possibilidade de praticar tal ato será punido com pena privativa de liberdade não superior a três anos ou com pena pecuniária.
> 2 As penas anteriores aplicam-se também a quem, por engano, fizer com que uma pessoa vinculada ao dever de confidencialidade nos termos do n.º 1 viole a sua obrigação de sigilo.
> 3 A violação do segredo postal ou de telecomunicações continua a constituir infracção mesmo após a cessação da relação de trabalho como funcionário público, empregado ou auxiliar de organização prestadora de serviços postais ou de telecomunicações.
> 4 A violação do sigilo postal ou de telecomunicações não é punível se for praticada para determinar a identidade do titular.
> 5 O artigo 179º é reservado, juntamente com as disposições federais e cantonais sobre as obrigações de prestar depoimento ou fornecer informações a uma autoridade pública (Suíça, [2024], tradução livre).

O que se propõe, então, aqui e agora, é exatamente essa provocação: no Brasil, há a necessidade de se refletir acerca de quais condutas, efetivamente, precisariam - ou poderiam - ser guindadas à categoria de infrações penais para que a tutela penal tenha maior força de ação, para que o efeito pedagógico do risco de ser descoberto e de receber sanção por isso tenha algum efeito prático na inibição de condutas que desrespeitam o direito fundamental da proteção dos dados pessoais.

A incriminação de comportamentos danosos ao organismo social, limitadora - de certa forma - da liberdade das pessoas (Capez, 2009), justificar-se-á na proporcionalidade de tal medida, já que tal ônus será compensado pela vantagem na proteção do bem jurídico valoroso que se está a ressaltar: a proteção dos dados pessoais de cada cidadão. Na conta entre custos e benefícios sociais, a incriminação de condutas desse jaez - que atentam contra esse direito fundamental indispensável - será a melhor opção.

Discussão que precisa ser feita com cuidado, é certo, com muito debate, reflexão e ponderação, na medida em que o tamanho da ofensa a esse direito fundamental é que deve servir de baliza, por óbvio, à reação estatal penal. Como deve acontecer em qualquer tipificação penal de condutas sociais, insiste-se. Não há que se deixar influenciar por reclamos momentâneos de proteção penal, até porque, já se disse, não se está defendendo um direito penal de emergência ou simbólico. Ao contrário, o bem jurídico em evidência é por demais valioso, qual seja, a proteção dos dados pessoais do titular, ou, na essência, a sua própria existência como ser humano único.

Lembrando que, numa visão clássica, "crime é a conduta humana que lesa ou expõe a perigo um bem jurídico protegido pela lei penal. Sua essência é a ofensa ao bem jurídico, pois toda norma penal tem por finalidade sua tutela" (Noronha, 1987, p. 94).

Então, pergunta-se, uma vez mais: quais condutas, tipificadas como crimes, e quais sanções correspondentes, de fato contribuiriam para a efetividade da tutela desse direito fundamental?

Cabe ao legislador - em nome da sociedade e a partir dos valores abrigados na CRFB/88, como a liberdade, a segurança, o bem-estar-social, a propriedade, a igualdade, a justiça, a dignidade da pessoa humana, a privacidade, a intimidade, além dos princípios/pressupostos éticos, sociais, econômicos e políticos fundantes - fazer a seleção das ações humanas que merecem ser alçadas à categoria de infrações penais.

Nesse viés e não sem a necessária lapidação e reflexão política criminal, pode-se confeccionar um rol de condutas que, atualmente, já em prática, estão sem controle e sem a devida atenção do Estado. São ações altamente lesivas e que estão retirando direitos; no mínimo, a liberdade dos cidadãos e proprietários desses dados pessoais. Estão causando mal em nome de um progresso pouco palpável e, muitas das vezes, de uma inovação desmedida, descontrolada, sem ética e, portanto, proibida. Como já se afirmou, não é essa inovação que irá salvar e desenvolver a sociedade.

São condutas que estão acontecendo a todo momento e em todo lugar, cabendo destacar, por exemplo, aquelas consistente na ação, omissiva ou comissiva, de não proteger um banco de dados contendo dados pessoais sensíveis, de informações de saúde, biométricas, econômicas ou de tendências sociais, políticas, sexuais e íntimas de um titular; no compartilhamento indiscriminado e mediante paga, de um banco de dados pessoais, à sorrelfa dos titulares; no uso de inteligência algorítmica descontrolada; e na falsa informação sobre o tratamento de dados pessoais, deixando o titular falsamente seguro de que seus dados estariam protegidos, quando não estão.

Também, há a falta dolosa de investimento em sistemas de tratamento de dados desatualizados, por ganância ou risco injustificado; a coleta desmedida e sem finalidade absolutamente justificada, de dados pessoais sensíveis - como biometria facial ou dados da íris -, para fins de comercialização ou de confecção de um banco de dados valioso; a utilização, à sorrelfa, de dados pessoais colhidos indevidamente, para fins de comercialização/monetização e de perfilamento social, econômico, político, sexual ou financeiro de alguém ou de uma coletividade identificável; e a utilização de perfilamento pessoal, a partir de dados colhidos sem consentimento, para fins de direcionamento de marketing, inclusive com georreferenciamento.

Ainda, vê-se a utilização de perfilamento pessoal para fins de discriminação dolosa quanto à oferta de bens e serviços, ou de emprego, ou de serviços

públicos; coleta dolosa e ilícita de dados pessoais de crianças e adolescentes, em descompasso com a previsão e autorização legal, notadamente sem a ciência dos pais ou responsáveis; a utilização da *deepweb* e da *darkweb* para obtenção/compra espúria de bancos de dados pessoais; o emprego de programas de informática maliciosos (*malware*), capazes de subtrair dados pessoais, notadamente biométricos e sensíveis; a sonegação de informações corretas ou entrega de informações incompletas ou deturpadas, às autoridades competentes, quando devidamente requisitadas em procedimento próprio; o extravio de banco de dados por ação comissiva ou omissiva, com prejuízo aos beneficiados do serviço público respectivo; o compartilhamento de bancos de dados pessoais com grupos criminosos organizados, adeptos ao terrorismo ou outra forma de macro criminalidade violenta.

No Código Penal brasileiro, ainda no ano de 2012, foi inserido o artigo 154-A, incriminando a invasão de dispositivo informático. Sobre esse tipo penal, Santa Terra Júnior (2023) observa que precisa ser aperfeiçoado, corrigido, passando a prever a punição, por exemplo, pela simples visualização dos dados pessoais do proprietário do dispositivo invadido, independentemente de outra finalidade específica, na medida em que tal é suficiente para ofender, além da privacidade, o direito à proteção de dados pessoais, consagrado na Constituição Federal brasileira.

Nessa trilha, retomando as condutas observadas na atualidade, soa razoável também a criação de causas de aumento de pena se houver o uso de tecnologias mais avançadas na coleta irregular de dados pessoais para fins comerciais, por exemplo; ou quando envolverem dados pessoais sensíveis, notadamente de crianças, adolescentes e pessoas vulneráveis, de titulares em situação de risco e vulneráveis; com finalidades falsas, engodo ou manipulação. Além disso, previsão de crimes culposos, quando o desleixo no tratamento desses dados possa causar prejuízos e ofensas à liberdade ou à dignidade do titular, ou quando houver coleta desnecessária, ou a manutenção de erros no banco de dados; crimes vagos, de resultado cortado, sem que necessariamente se tenha condições de aferir prejuízos concretos ou de todos os indivíduos que tiveram seus dados pessoais desprotegidos.

Enfim, parecem ser muitas as possibilidades de se conjecturar sobre condutas abusivas e ilícitas, indevidas, intrusivas, desrespeitosas, perigosas, danosas e potencialmente lesivas aos titulares dos dados pessoais, em flagrante ofensa ao direito fundamental hoje consagrado na nossa Carta Magna (art. 5º, inciso LXXIX).

Talvez não sejam todas as condutas aqui exemplificadas que estejam merecendo uma tipificação penal. Mas o debate sobre elas é urgente e a escolha de algumas, também.

Ademais, é certo que junto com essa mudança legislativa e incrementação de condutas, o próprio Estado terá de se adequar e reunir condições de garantir a produção de provas robustas, principalmente periciais, no mundo virtual, capazes de materializar essa plêiade de novos crimes previstos,

quase sempre desafiando perícias e provas técnicas. Cuidados com a cadeia de custódia e com a licitude/ legitimidade dessas provas deverão ser preocupação estatal também, em homenagem à segurança e à garantia de todos os envolvidos. Até porque de nada adiantará um incremento legislativo penal, nessa seara, na busca da proteção desse direito fundamental tão caro, se o próprio Estado, daí, negligenciar a utilização dessa importante ferramenta.

A ideia, pois, é provocar a reflexão. É tirar da escuridão e trazer ao debate o uso abusivo - às vezes silencioso e à sorrelfa, vênia pela repetição - de informações e dados pessoais tão sensíveis. A ideia é lançar luzes sobre a existência de um direito fundamental atualmente desprestigiado, quiçá desconhecido, deixado de lado e que, talvez por isso, esteja sendo tão maltratado.

Muitas condutas aqui mencionadas, repita-se, por certo precisam ser mais discutidas e divulgadas, ressaltadas, para que o cidadão comece a despertar o seu interesse em relação a elas. A discussão sobre essas ações humanas e condutas escondidas, algumas inclusive praticadas, a mando, por robôs e algoritmos, precisa ser iniciada e deve ser acalorada.

Muitas precisam ser guindadas à condição de condutas administrativamente típicas, ensejando controle administrativo pelos órgãos competentes. Outras, porém, frise-se, bem selecionadas e cuidadosamente tipificadas, dentro de uma política criminal séria e eficaz, precisam se transformar em crimes e prever sanções correspondentes, eficazes, que possam fazer com que aqueles que tradicionalmente desrespeitam direitos fundamentais reflitam sobre a mantença de tais posturas e, se for o caso, recebam a retribuição penal-estatal cabível e necessária.

Até porque muitas das condutas em voga tangenciam, igualmente, outros bens jurídicos que lhes são inerentes, como a honra, a segurança, a dignidade - inclusive sexual - da pessoa humana, a liberdade. Ferem igualmente direitos de proteção ao consumidor, (de proteção integral) às crianças e aos adolescentes, à vulnerabilidade social, à privacidade, à intimidade, à inviolabilidade do lar e outros. Direitos fundamentais igualmente atingidos pela ofensa ao direito fundamental da proteção dos dados pessoais.

Talvez assim o Direito Penal possa cumprir a sua função social, de controle e pacificação social, numa sociedade cada vez mais distante, desrespeitosa, alheia, virtual e sem rumo certo.

6. CONCLUSÃO

A expansão do Direito Penal como reforço na proteção de direitos fundamentais é uma estratégia possível, importante para assegurar a efetiva tutela de bens jurídicos essenciais e valiosos, como é a proteção dos dados pessoais, inserida na CRFB/88 no seu art. 5°, inciso LXXIX.

Trata-se de uma importante opção de política criminal, não sendo o caso de se falar em um direito de emergência ou simbólico, na medida em que tal bem jurídico carece de efetiva tutela penal em prol da proteção dos cidadãos e titulares desse direito.

Por outro lado, a análise de infrações administrativas e crimes em licitações públicas e contratos administrativos, por exemplo, ou nas áreas do consumidor e das infrações de trânsito, ilustra como a tipificação de condutas ilícitas no âmbito penal pode complementar as sanções administrativas, em casos pontuais e importantes, contribuindo para um ambiente de maior efetividade na tutela de direitos fundamentais, notadamente quando essa postura legislativa tem como escopo a proteção social.

Atualmente, quanto ao direito em testilha, são muitas as condutas abusivas que estão sendo verificadas, notadamente no ambiente tecnológico, sem que os maiores interessados - que são os titulares dos dados pessoais - percebam que estão sendo vítimas de manipulação, perfilamentos e riscos desnecessários e ilegais. A identificação, o debate e a reflexão sobre a tutela penal de tais condutas exsurge como urgente e útil, à semelhança da legislação penal de outros países.

Assim, é essencial que o direito penal continue a evoluir para enfrentar os desafios impostos pela modernidade, especialmente para garantir a proteção efetiva de direitos fundamentais, em uma sociedade cada vez mais digital e interconectada, que está tratando com desdém a proteção dos dados pessoais.

E o fortalecimento da legislação penal em prol desse novel direito fundamental da proteção de dados pessoais exigirá, obviamente, o fortalecimento das instituições públicas responsáveis pelo combate à criminalidade, no caso em especial, o Ministério Público, como titular exclusivo da ação penal pública.

7. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Alemanha. Código Penal. [Berlim]: Ministério Federal da Justiça, [2021]. Disponível em: https://www.gesetze-im-internet.de/englisch_stgb/.

Artese, Gustavo. Compliance digital: proteção de dados pessoais. *In*: Carvalho, André C.; Bertoccelli, Rodrigo de P.; Alvim, Tiago C.; Venturini, Otávio (coord.). *Manual de compliance*. Rio de Janeiro: Forense, 2019.

Bioni, Bruno Ricardo. *Proteção de dados pessoais, a função e os limites do consentimento*. Rio de Janeiro: Forense, 2018.

Brasil. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Brasil. Decreto-lei nº 2.848, de 07 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

Brasil. Decreto nº 2.181, de 20 de março de 1997. Dispõe sobre a organização do Sistema Nacional de Defesa do Consumidor - SNDC, estabelece as normas gerais de aplicação das sanções administrativas previstas na Lei n. 8.078, de 11 de setembro de 1990, revoga o Decreto n. 861, de 9 julho de 1993, e dá outras providências. *Diário Oficial da União*, Brasília, 21 mar. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d2181.htm.

Brasil. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. *Diário Oficial da União*, Brasília, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm.

Brasil. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. *Diário Oficial da União*, Brasília, 16 jul. 1990. (retificado em 27 set. 1990). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

Brasil. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, Brasília, 12 set. 1990 (retificado em 10 jan. 2007). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

Brasil. Lei nº 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. *Diário Oficial da União*, Brasília, 28 dez. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8137.htm.

Brasil. Lei nº 8.666, de 21 de junho de 1993. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Brasília, DF: Presidência da República, [2021]. (revogada pela Lei nº 14.133, de 1º de abril de 2021). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8666cons.htm.

Brasil. Lei nº 9.605, de 12 de fevereiro de 1998. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. *Diário Oficial da União*, Brasília, 13 fev. 1998 (retificado em 17 fev. 1998). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9605.htm.

Brasil. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. *Diário Oficial da União*, Brasília, 2 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.

Brasil. Lei nº 14.133, de 1º de abril de 2021. Lei de licitações e contratos administrativos. *Diário Oficial da União*, Brasília, 1º abr. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm.

Capez, Fernando. *Curso de direito penal - parte geral*. 13. ed. São Paulo: Saraiva, 2009. 1 v.

Conselho Nacional do Ministério Público. *Resolução nº 281, de 12 de dezembro de 2023. Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público e dá outras providências*. Brasília, DF: CNMP, 2023. Disponível em: https://www.cnmp.mp.br/portal/atos-e-normas/norma/10515.

Cunha, Rogério Sanches. *Manual de direito penal - parte geral* (arts. 1º a 120). 12. ed. rev., atual. e ampl. São Paulo: JusPodivm, 2023.

Decomain, Pedro Roberto. *O código penal alemão: tradução, comparação e notas*. Porto Alegre: Núria Fabris, 2014.

Doneda, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

Dotti, René A. *Curso de direito penal - parte geral*. 6. ed. São Paulo: Revista dos Tribunais, 2018.

Frazão, Ana; **Carvalho**, Angelo Prata de; **Milanez**, Giovanna. *Curso de proteção de dados pessoais: fundamentos da LGPD*. 1. ed. Rio de Janeiro: Editora Forense, 2022.

Greco, Rogério. *Curso de direito penal - parte geral*. 13. ed. Rio de Janeiro: Impetus, 2011. 1 v.

Masson, Cleber. *Direito penal - parte geral* (arts. 1º a 120). 11. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2017. 1 v.

Noronha, Edgard Magalhaes .*Direito penal*. 1. ed. São Paulo: Saraiva, 1987. 1 v.

Nucci, Guilherme de Souza. *Manual de direito penal*. 19. ed. Rio de Janeiro: Forense, 2023.

Prado, Luiz Regis. *Curso de direito penal brasileiro*. 10. ed. São Paulo: Revista dos Tribunais, 2010. 1 v.

Santa Terra JR., João. Impactos das Tecnologias da Informação e da Comunicação (TIC) na política criminal brasileira. *In*: Vadell, Lorenzo M. B.; Veiga, Fábio da S.; Pierdoná, Zélia L. *Retos Del Horizonte Jurídico Iberoamericano*. 1. vol. Porto/Salamanca: IBEROJUR e Universidad de Salamanca, 2023.

Schiefler, Rui C. K.; **Oliveira**, Maria Fernanda T. B. A segurança institucional do Ministério Público brasileiro e a Lei Geral de Proteção de Dados (Lei n. 13.709/2018): impressões iniciais. *In*: BRASIL. *Conselho Nacional do Ministério Público. Estudos de segurança institucional e contrainteligência no âmbito do Ministério Público brasileiro*. Brasília: CNMP, 2019.

Suíça. Código Penal. Confederação Suíça: Fedlex, [2024]. Disponível em: https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en.

Suxberger, Antonio Henrique Graciano; **Gomes Filho**, Demerval Farias. Funcionalização e expansão do direito penal: o direito penal negocial. *Revista de Direito Internacional*, Brasília, v. 13, n. 1, 2016. DOI: 10.5102/rdi.v13i1.3976.

TUTELA (PENAL) COLETIVA DA PROTEÇÃO DE DADOS PESSOAIS PELO MINISTÉRIO PÚBLICO BRASILEIRO

Jorge Augusto Caetano de Farias[1]

Resumo: O presente estudo busca analisar a atividade de tutela coletiva de direitos fundamentais pelo Ministério Público brasileiro, sob a perspectiva penal e para a salvaguarda do direito à proteção de dados pessoais, objeto de recente reconhecimento e intensas transformações pelo ordenamento jurídico brasileiro. A partir de pesquisa bibliográfica, normativa e jurisprudencial, propõe-se uma nova compreensão da atividade de persecução penal pelo Ministério Público, sob o prisma coletivo, como forma de enfrentar com eficácia e resolutividade os desafios emergentes da tutela de bem jurídico essencialmente individual – os dados pessoais do cidadão brasileiro – mas que sofre exploração e ataque massivos mediante o uso das novas tecnologias da informação e da comunicação.

Palavras-chave: Dados pessoais. Proteção. Tutela coletiva penal e processual. Direitos fundamentais. Ministério Público.

Resumen: Este artículo busca estudiar la actividad de tutela colectiva de derechos fundamentales por las Fiscalías de Brasil, sobre todo desde una perspectiva penal y para la protección de datos personales, que han sido recién e intensamente transformados por el orden jurídico brasileño. A partir de una investigación bibliográfica, legislativa y jurisprudencial, se propone una nueva comprensión acerca de la actividad de persecución penal por el Ministerio Público, bajo un prisma colectivo, como una manera de actuar más eficiente y resolutiva los desafíos a la protección de bien jurídico esencialmente individual – los datos personales de los ciudadanos brasileños – pero masivamente atacado y explotado, sobre todo con el uso de las nuevas tecnologías de la información y de la comunicación.

---

1. Promotor de Justiça do Ministério Público Militar brasileiro. Mestre em Direito Penal pela UCB/ESMPU.

Palabras clave: Datos personales. Protección. Tutela colectiva penal y procesal. Derechos fundamentales. Ministerio Público.

Sumário: 1. Introdução. 2. A proteção de dados pessoais no Brasil. 2.1. Origens. 2.2. Lei Geral de Proteção de Dados Pessoais. 3. Proteção de dados pessoais como direito fundamental. 4. A tutela coletiva de direitos fundamentais. 4.1. Classificação dos direitos objetos de tutela coletiva. 4.2. Natureza do direito à proteção de dados pessoais. 4.3. Legitimação do Ministério Público. 4.4. Instrumentos. 5. Tutela penal coletiva da proteção de dados pessoais. 5.1. Vertentes preventiva e repressiva. 5.2. Aspectos materiais e processuais penais. 6. Conclusão. 7. Referências bibliográficas e documentação.

1. INTRODUÇÃO

A proteção de dados pessoais no Brasil pode ser considerada um fenômeno relativamente recente, sobretudo quando se constata que a Lei Geral de Proteção de Dados Pessoais – LGPD – veio a lume apenas em 2018 (Lei nº 13.709, de 14 de agosto daquele ano), embora o tema já fosse objeto de preocupação – e de normatização – há décadas na Europa e já se registrassem notáveis casos de violação – por vezes, massiva – à proteção de dados pessoais no país.

Conquanto ainda não contasse com previsão constitucional expressa – ao tempo de sua edição, a LGPD extraía seus fundamentos da Constituição Federal do art. 1º, inciso III (dignidade da pessoa humana) e do art. 5º, inciso X (intimidade, vida privada, honra, imagem) – sobreveio a Emenda Constitucional nº 115/2022, que acresceu, ao rol de direitos fundamentais do art. 5º, o inciso LXXIX ("é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais").

Como o próprio nome indica, o direito em tela ostenta natureza essencialmente individual, embora o tempo revele que a tutela mais eficiente se deva operar, tanto preventiva quanto repressivamente, a partir de uma dimensão coletiva, seja pelo manejo tradicional dos meios já disponíveis, seja por novas formas de utilização desses mesmos instrumentos, seja pela criação de novos métodos.

E isso porque se tem multiplicado os episódios de violação de bancos de dados pessoais contendo informações de centenas, milhares ou até mesmo milhões de titulares. Ademais, impossível não considerar o tratamento (por vezes carente de melhor esclarecimento do alcance e da finalidade) operado pelos detentores dos maiores bancos de dados disponíveis na atualidade, quais sejam, as companhias tecnológicas que oferecem os principais serviços utilizados na rede mundial de computadores ao redor do globo, realidade na qual o Brasil se insere de forma importante, ante a mais de centena de milhões de usuários da grande rede no país, em número que não para de

crescer. Não por acaso, a Constituição buscou proteger o referido direito "inclusive nos meios digitais".

Nesse contexto, em que o direito fundamental mais recentemente incorporado ao ordenamento constitucional se vê desafiado diuturnamente, sob as mais diversas formas, com o dinamismo próprio dos meios digitais e com o interesse (legítimo ou não) de diversos segmentos sociais e econômicos, exsurge a necessidade da atuação inovadora e multifacetária do Ministério Público brasileiro, vocacionado à tutela do regime democrático e dos direitos sociais e individuais indisponíveis, categoria na qual se insere a proteção de dados pessoais.

Entretanto, tão importante e constante a ameaça que paira sobre referido direito que o imperativo de vedação à proteção deficiente demanda que a tutela se opere de forma integral, ou seja, não apenas na esfera cível mas também criminal, tanto na dimensão preventiva quanto repressiva, buscando evitar a ocorrência do dano e, quando consumado, alcançar a devida reparação aos titulares e a responsabilização dos agentes, sejam pessoas físicas ou jurídicas.

Embora na seara cível a tutela coletiva de direitos fundamentais já seja tradicionalmente exercida pelo Ministério Público brasileiro, antes mesmo do advento da Constituição de 1988 (a Lei de Ação Civil Pública – Lei nº 7.347 – remonta ao ano de 1985), a mencionada dimensão integral da proteção de dados pessoais reacende as discussões acerca da possibilidade de uma tutela coletiva desse direito também na esfera criminal, que se insere na mais antiga vocação ministerial, qual seja, a de titular da ação penal pública (art. 129, inciso I, da CF/88).

Eis o objeto do presente estudo, que, valendo-se de pesquisa bibliográfica, legislativa e jurisprudencial, busca identificar as bases para uma tutela penal coletiva, pelo Ministério Público brasileiro, do direito fundamental à proteção de dados pessoais.

Para tanto, inicialmente se traça um panorama histórico e normativo da proteção de dados pessoais no Brasil, inclusive mediante o resgate de sua inspiração europeia para a edição da LGPD, além dos desafios para a adequação aos seus ditames e as implicações do seu reconhecimento constitucional como direito fundamental.

Em seguida, passa-se a analisar o complexo sistema brasileiro de tutela coletiva de direitos fundamentais, tanto preventivo quanto repressivo, seja judicial, seja extrajudicial, mas sempre considerando o protagonismo conferido ao Ministério Público pela Constituição e pela legislação de regência do tema.

Por fim, assentadas tais premissas, busca-se identificar as perspectivas para uma tutela penal coletiva do direito à proteção de dados pessoais, tanto no plano material quanto processual, com ênfase na atuação do Ministério Público.

2. A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Embora, como visto, já se pudesse extrair a proteção de dados como consectário de direitos fundamentais como a intimidade, a vida privada, a honra, a imagem, o sigilo das comunicações, ou mesmo o *habeas data* (Frazão, Carvalho e Milanez, 2022), o certo é que o patamar atual de conformação como direito fundamental autônomo e objeto de reconhecimento constitucional expresso levou algumas décadas para ser alcançado.

E a análise desse percurso deve passar, necessariamente, por destacar ao menos os elementos históricos mais importantes da matriz normativa e institucional europeia de proteção de dados, na medida em que foi o modelo que serviu de inspiração à elaboração da LGPD.

E, mesmo no Brasil, a positivação da proteção de dados de maneira expressa no rol de direitos fundamentais da Constituição Federal de 1988 passou antes pelo reconhecimento específico tanto do legislador ordinário quanto do Supremo Tribunal Federal, tudo conforme se analisará a seguir.

2.1. ORIGENS

Tendo a LGPD se inspirado, à toda evidência, no Regulamento Geral de Proteção de Dados (RGPD ou GDPR) da União Europeia[2], mister analisar, em linhas gerais, alguns aspectos históricos desse tema naquele continente.

Seguindo a tendência mundial no sentido da "constatação de um forte vínculo entre o progresso tecnológico e a tutela da privacidade" (Frazão *et al,* 2022, p. 19), a preocupação da União Europeia com a proteção de dados, no plano normativo (inicialmente como *soft law*), remonta ao início da década de 1980, com o advento da Convenção 108/1981 do Conselho da Europa.

Nessa mesma década (em 1983), houve importante precedente jurisprudencial do Tribunal Constitucional Federal alemão, o qual "reconheceu, a partir da dignidade humana e do direito geral ao livre desenvolvimento da personalidade, a existência de um direito de personalidade autônomo à proteção de dados pessoais" (Frazão *et al,* 2022, p. 20).

Na década seguinte, sobreveio a Diretiva 95/46/EC, a qual "determinou a adoção, até 1998, de um amplo conjunto de obrigações pessoais destinadas à proteção de direitos de privacidade, abrindo caminho para a posterior edição do RGPD, inclusive criando as bases do direito fundamental à proteção de dados pessoais" (Frazão *et al,* 2022, p. 20).

2. A propósito, confira-se a matéria jornalística sobre a aprovação do projeto de lei geral de proteção de dados pessoais no Senado Federal, que além de resumir o teor da nova lei, destacou a RGPD (disponível em https://www12.senado.leg.br/noticias/materias/2018/07/10/projeto-de-lei-geral-de-protecao-de-dados-pessoais-e-aprovado-no-senado).

Por fim, conquanto tenha seus fundamentos normativos em diplomas muito mais antigos, o Regulamento Geral de Proteção de Dados nº 2016/679[3] – já em caráter de *hard law,* vinculante dos Estados-membros – só entrou em vigor em 2018, mesmo ano de promulgação da LGPD brasileira.

2.2. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Embora a LGPD (Lei 13.709/2018) tenha sido editada somente três décadas após a Constituição Federal de 1988, a temática da proteção de dados foi objeto de preocupação pontual do legislador brasileiro em diplomas esparsos e com diversos outros escopos, destacando-se, especialmente, o Código de Defesa do Consumidor (Lei 8.078/90, cujo art. 43 preconiza o alerta escrito ao consumidor acerca da coleta de seus dados pessoais) e o Marco Civil da Internet – Lei 12.965/2014, cujo art. 7º, inciso VII, exige o consentimento livre, expresso e informado do usuário para a coleta, armazenamento e utilização de seus registros de conexão (Frazão *et al,* 2022).

E, como visto, apesar do longo lapso desde a nova ordem constitucional brasileira e os primeiros diplomas europeus, a LGPD veio a lume em momento muito próximo ao do RGPD, tendo sido objeto de extenso debate legislativo desde o início da década de 2010, sobretudo com o incremento da preocupação acerca da proteção de dados, especialmente nos meios digitais.

Ainda assim, a lei brasileira somente entrou em vigor em 2020, enquanto suas sanções (administrativas) tiveram o início da vigência prorrogado para 2021, quase um ano após o início das atividades da Autoridade Nacional de Proteção de Dados (ANPD), em novembro de 2020 (Frazão *et al,* 2022).

De todo modo, a LGPD veio ainda a tempo de se buscar "colocar um freio nas vicissitudes que possibilitaram a consolidação do estágio atual da economia movida a dados" e nos "problemas decorrentes do capitalismo de vigilância" (Frazão *et al,* 2022, p. 13), tendo seus objetivos e fundamentos elencados, respectivamente, em seus arts. 1º e 2º.[4]

---

3. A respeito do advento do RGPD, Frazão *et al* (2022, p. 20) destacam, ainda, que "seu objetivo é eliminar inconsistências em leis nacionais, ampliar o escopo de proteção da privacidade e proteção de dados e modernizar a legislação para desafios tecnológicos, econômicos e políticos atuais, a exemplo daqueles advindos do uso intensificado da internet".

4. A propósito, confira-se o teor de tais dispositivos: "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

Nesse contexto, apresentando-se como um instrumento para a realização e para a salvaguarda dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade, a LGPD ajudou a abrir caminho para o reconhecimento expresso e específico da proteção de dados pessoais como direito fundamental.

3. PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

A proteção de dados pessoais passou a ser reconhecida expressamente, e de maneira autônoma, como direito fundamental no Brasil, em dois momentos distintos: primeiramente, no plano jurisprudencial, por parte do Supremo Tribunal Federal (STF), ainda em 2020 (ano de entrada em vigor da LGPD); e, posteriormente, no plano constitucional, com o advento da Emenda nº 115/2022.

Ao analisar as Ações Diretas de Inconstitucionalidade propostas contra a Medida Provisória que determinava o compartilhamento de dados pessoais dos usuários de telefonia com o órgão estatal incumbido da realização do censo[5], o STF identificou um direito fundamental à proteção de dados pessoais a partir da interpretação sistemática da proteção constitucional à dignidade da pessoa humana, à intimidade, à vida privada, ao *habeas data,* como "instrumento de tutela processual do direito à autodeterminação informativa" (Frazão *et al,* 2022, p. 26/27).

Por fim, foi promulgada a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, no inciso LXXIX do art. 5º ("*é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais*").

4. A TUTELA COLETIVA DE DIREITOS FUNDAMENTAIS

Os direitos fundamentais, dentre os quais a proteção de dados pessoais, tem se revelado objeto de especial proteção da ordem jurídica, constitucional e infraconstitucional, na realidade brasileira, em todo o período da redemocratização.

Embora tenham uma dimensão majoritariamente individual (mesmo se tendo multiplicado os direitos fundamentais de titularidade coletiva), ainda antes de 1988, mas sobretudo com a Constituição Federal, verificou-se a preocupação em legitimar o Ministério Público para a busca da tutela

5. Medida Cautelar na ADI 6387, Relatora Ministra Rosa Weber, acórdão publicado em 12.11.2020. Disponível em https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf

coletiva de tais direitos, tanto judicial quanto extrajudicial, seja na vertente preventiva, seja na repressiva.

Com um perfil constitucional vocacionado à defesa dos direitos fundamentais, não apenas na esfera cível mas também criminal, a ordem normativa brasileira tem buscado dotar o Ministério Público de instrumentos jurídicos importantes para o adequado desempenho desse relevante mister.

Nesse contexto, o presente capítulo se propõe a analisar tais aspectos, com especial atenção ao direito fundamental à proteção de dados pessoais, antes de se passar a aprofundar a análise sobre a perspectiva penal da tutela coletiva pelo Ministério Público.

4.1. CLASSIFICAÇÃO DOS DIREITOS OBJETOS DE TUTELA COLETIVA

Tradicionalmente, são descritas três categorias de direitos passíveis de tutela ou defesa de forma coletiva, a partir da definição trazida pelo art. 81, parágrafo único, da Lei nº 8.078/90: interesses ou direitos difusos, coletivos ou individuais homogêneos.

Os difusos e coletivos são também classificados como transindividuais e de natureza indivisível. Enquanto os direitos difusos têm seus titulares indeterminados e indetermináveis, os coletivos são titularizados por grupo, categoria ou classe de pessoas ligadas por uma relação jurídica específica com o violador do direito[6].

Por seu turno, os direitos individuais homogêneos são divisíveis, uma vez que seus titulares são identificáveis e sua tutela pode ser buscada individualmente (embora também o possa ser de forma coletiva, na medida em que teriam ligação por um evento em comum).[7]

4.2. NATUREZA JURÍDICA DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Como visto, sobretudo com o advento da Emenda Constitucional nº 115/2022, não restam mais dúvidas acerca da natureza de direito fundamental atribuída à proteção de dados pessoais no Brasil, positivando

6. O Conselho Nacional do Ministério Público (CNMP) mantém, em seu sítio eletrônico, o Portal de Direitos Coletivos, por meio do qual se esclarece de forma didática em que consistem e como o Ministério Público atua em sua tutela. Disponível em https://www.cnmp.mp.br/direitoscoletivos/

7. O referido Portal de Direitos Coletivos do CNMP sustenta que a tutela coletiva dos direitos individuais homogêneos tem o "propósito de otimizar o acesso à justiça e a economia processual".

o reconhecimento já havido em sede jurisprudencial pelo Supremo Tribunal Federal.

Entretanto, em matéria de tutela coletiva, importante buscar identificar em qual espécie de direito transindividual melhor se adequa a proteção de dados pessoais, na medida em que guarda repercussões não apenas de índole material, mas sobretudo processual.

Em uma primeira análise, menos detida, pareceria até instintivo classificar o direito à proteção de dados pessoais como direito individual homogêneo, por se tratar de direito subjetivo divisível e individualizável, tendo titularidade determinada[8], ostentando seus titulares elo de ligação por circunstância de fato (por exemplo, as vítimas de um mesmo evento de violação decorrente de vazamento de uma base de dados pessoais)[9].

Entretanto, a proteção de dados pessoais, assim como outros direitos fundamentais precipuamente individuais, pode assumir feição coletiva, tanto de direitos difusos quanto coletivos em sentido estrito.

Pode envolver direitos difusos, a título exemplificativo, quando "se pretende corrigir algum tratamento inadequado de dados pessoais realizado por autoridades públicas, relativamente a todos os que vivem em certa localidade – tutela indivisível e sem (...) relação jurídica base prévia que delimite o grupo" (Roque, 2019).

Por outro lado, também pode-se vislumbrar sua dimensão coletiva, em sentido estrito, "na hipótese em que se pede a adequação do tratamento de dados pessoais realizado por uma empresa, relativamente a seus consumidores – tutela também indivisível, mas referente a uma relação jurídica de consumo base" (Roque, 2019).

Ocorre que, em qualquer caso, a fundamentalidade do direito à proteção de dados pessoais prepondera sobre tal classificação tripartite, de modo que o Ministério Público sempre se legitima à respectiva tutela coletiva, seja no âmbito cível, seja na esfera penal.

4.3. LEGITIMAÇÃO DO MINISTÉRIO PÚBLICO

A Constituição Federal, em seu art. 127, incumbe ao Ministério Público brasileiro a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, incumbência expressamente reafirmada

8. A esse respeito, Zavascki (2016) destaca, ainda: "Constituem, portanto, direitos subjetivos individuais na acepção tradicional, com titular identificado ou identificável e com determinação do seu conteúdo, bem como com adequado elo de ligação entre um e outro".

9. Segundo Roque (2019), "É necessário que haja preponderância das questões comuns em relação às individuais para que seja possível a proteção coletiva".

nas respectivas leis orgânicas (Lei Complementar nº 75/93 e Lei Federal nº 8.625/93, ambas em seu art. 1º, tamanha a relevância desses temas para as funções institucionais do MP).

Como visto, a mesma Carta Magna tratou de elencar, em seu rol de direitos fundamentais, a proteção de dados pessoais, inclusive em meios digitais, fazendo-o no inciso LXXIX do art. 5º.

Ademais, conforme expressamente reconhecido pelo Supremo tribunal Federal, antes mesmo da previsão constitucional específica, extrai-se a proteção de dados pessoais de outros valores fundantes da ordem jurídica brasileira, como a dignidade da pessoa humana, a intimidade, a privacidade, o *habeas data*.

Por oportuno, cabe ressaltar que a proteção de dados pessoais, em sentido amplo, encontra conexão inegável com o próprio regime democrático, uma vez que o tratamento indiscriminado de dados por agentes públicos e privados, com interesses políticos ou até econômicos, pode prejudicar o livre convencimento de eleitores e cidadãos na tomada de decisões individuais ou coletivas de interesse da sociedade (Frazão *et al*, 2022).

Além disso, tampouco se pode negar a ampla transversalidade do direito à proteção de dados pessoais na ordem jurídica, tanto nacional quanto internacional (a tutela normativa do tema iniciou-se de forma mais consistente na Europa, a partir das diretivas emanadas no âmbito da União Europeia), seja no plano material, seja na seara processual, de modo a que se possa cogitar, sem receios, de um verdadeiro microssistema de proteção de dados pessoais, que vai muito além da LGPD.

Por fim, cumpre destacar a missão constitucional (art. 129) do Ministério Público de 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 (inciso II).

De todo esse contexto, emerge a ampla legitimação do Ministério Público brasileiro para a tutela (sobretudo coletiva) do direito à proteção de dados pessoais.

Tanto que, recentemente, foi editada a Resolução nº 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público, para dispor sobre a política e o sistema de proteção de dados pessoais pelo Ministério Público, não apenas em sua atividade administrativa, mas especialmente em sua atuação finalística, com ênfase na tutela coletiva:

> Art. 14. A defesa dos interesses e dos direitos dos titulares de dados pessoais poderá ser exercida em juízo, individual ou coletivamente, nos termos legais e com o uso dos instrumentos de tutela individual e coletiva.
>
> Parágrafo único. Ao Ministério Público, por suas autoridades competentes, no exercício de sua atividade finalística, também caberá a defesa desse direito fundamental, de forma coletiva e com os instrumentos pertinentes.

4.4. INSTRUMENTOS

Considerando a já mencionada ampla legitimação conferida ao Ministério Público, tanto no plano constitucional quanto infraconstitucional, igualmente abrangente é o instrumental de que dispõe para o exercício desse mister, inclusive para a tutela do direito à proteção de dados pessoais.

Na esfera jurisdicional, extraem-se da Constituição as ações públicas, tanto a penal (inciso I) quanto a civil (inciso III, segunda parte), previsão reforçada pelas Leis Orgânicas do Ministério Público brasileiro (Lei Complementar nº 75/93 e Lei Federal nº 8.625/93), "no sentido irrestrito e mais amplo possível, em limites suficientes e necessários para a obtenção da tutela jurisdicional completa e compatível com a natureza e a magnitude da lesão ou da ameaça aos bens e valores tutelados" (Zavascki, 2016, p. 6.1)[10].

Por seu turno, destaca-se o protagonismo do Ministério Público para os procedimentos apuratórios respectivos (uma vez conduzidos na seara extrajudicial), tanto para o inquérito policial (inciso VIII), na condição de controlador, quanto para o inquérito civil (inciso III, primeira parte), na condição de presidente.

Ademais, ainda no plano extrajudicial e dentre os procedimentos investigatórios, salientam-se a notícia de fato, o procedimento investigatório criminal e o procedimento administrativo/preparatório, todos a serem adrede analisados.

Além disso, como resultado da atividade apuratória e alternativa à judicialização de demandas, merecem relevo a recomendação, o compromisso de ajustamento de conduta e o acordo de não persecução (penal e cível).

Tamanha a centralidade de tais instrumentos e sua importância para o desempenho das missões institucionais do Ministério Público, sobretudo em contexto de valorização da autocomposição, da proatividade e da resolutividade da atuação ministerial fora do cenário jurisdicional, que o Conselho Nacional do Ministério Público houve por bem disciplinar o tema por meio de uma série de resoluções específicas, de modo a conferir, mais que limites, segurança jurídica para os representantes ministeriais e para os cidadãos.

Dentre tais normas, regulamentadoras e uniformizadoras da utilização dos meios extrajudiciais de apuração e de tutela de direitos constitucionais a cargo do Ministério Público, destacam-se as Resoluções CNMP 23/2007 (instauração e tramitação do inquérito civil), 164/2017 (expedição de

10. Zavascki (2016) prossegue, ainda, no sentido de que "Inclui, portanto, legitimação para buscar tutela cognitiva, preventiva e reparatória, declaratória, constitutiva ou condenatória. Inclui também poderes para pleitear medidas de tutela provisória, de antecipação de tutela e cautelar. Estende-se a legitimação para as medidas de cumprimento das liminares e das sentenças, inclusive, quando for o caso, para a propositura da ação autônoma de execução".

recomendações) e 179/2017 (tomada do compromisso de ajustamento de conduta).

Nos termos da Resolução CNMP 23/2007[11], o inquérito civil tem "natureza unilateral e facultativa, será instaurado para apurar fato que possa autorizar a tutela dos interesses ou direitos a cargo do Ministério Público nos termos da legislação aplicável", além de servir "como preparação para o exercício das atribuições inerentes às suas funções institucionais".

Por seu turno, a Resolução CNMP 164/2017[12] define que a recomendação é ato formal de persuasão do destinatário, por meio de razões fáticas e jurídicas, "em benefício da melhoria dos serviços públicos e de relevância pública ou do respeito aos interesses, direitos e bens defendidos pela instituição", visando à prevenção de responsabilidades ou correção de condutas, muito embora não possua caráter coercitivo.

Enquanto a recomendação tem caráter unilateral, realidade diversa ocorre com o compromisso de ajustamento de conduta. Disciplinado pela Resolução CNMP 179/2017[13], tem natureza de negócio jurídico e eficácia de título executivo extrajudicial, buscando a adequação da conduta às exigências legais e constitucionais, como instrumento de garantia dos direitos e interesses cuja tutela cabe ao Ministério Público.

No plano investigativo, cabe ressaltar, ainda, a Notícia de Fato e o Procedimento Administrativo, ambos normatizados pela Resolução CNMP 174/2017[14].

A Notícia de Fato "é qualquer demanda dirigida aos órgãos da atividade-fim do Ministério Público (...) entendendo-se como tal a realização de atendimentos, bem como a entrada de notícias, documentos, requerimentos ou representações".

Já o Procedimento Administrativo destina-se a "acompanhar o cumprimento das cláusulas de termo de ajustamento de conduta celebrado; acompanhar e fiscalizar, de forma continuada, políticas públicas ou instituições; apurar fato que enseje a tutela de interesses individuais indisponíveis; embasar outras atividades não sujeitas a inquérito civil".

---

11. Disciplina, no âmbito do Ministério Público, a instauração e tramitação do inquérito civil. Inteiro teor disponível em https://www.cnmp.mp.br/portal/images/Normas/Resolucoes/Resoluo-0232.pdf

12. Disciplina a expedição de recomendações pelo Ministério Público brasileiro. Inteiro teor disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resolução-164.pdf

13. Disciplina, no âmbito do Ministério Público, a tomada do compromisso de ajustamento de conduta. Inteiro teor disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resolução-179.pdf

14. Disciplina, no âmbito do Ministério Público, a instauração e a tramitação da Notícia de Fato e do Procedimento Administrativo. Inteiro teor disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resoluo-174-2.pdf

Por fim, na esfera criminal, destaca-se a Resolução CNMP 181/2017[15], que disciplina o Procedimento Investigatório Criminal e o Acordo de Não Persecução Penal.

O Procedimento Investigatório Criminal é instrumento "sumário e desburocratizado de natureza administrativa e investigatória, instaurado e presidido pelo membro do Ministério Público com atribuição criminal", tendo como finalidade "apurar a ocorrência de infrações penais de iniciativa pública, servindo como preparação e embasamento para o juízo de propositura, ou não, da respectiva ação penal".

Por seu turno, o Acordo de Não Persecução Penal é o negócio jurídico celebrado entre o Ministério Público e o investigado que, além de confessar circunstanciadamente o crime com pena mínima inferior a quatro anos cometido sem violência ou grave ameaça, comprometer-se a reparar o dano ou pagar prestação pecuniária, renunciar ao produto do crime ou prestar serviços comunitários, dentre outras condições, conforme o caso.

Além disso, não se podem olvidar os instrumentos consensuais para as infrações de menor potencial ofensivo, como a transação penal e a suspensão condicional do processo.

Em suma, o Ministério Público brasileiro dispõe de uma série de instrumentos, investigatórios, negociais e de persuasão, tanto na seara cível quanto criminal, para a tutela dos bens ou interesses confiados pela Constituição e pelas leis, não apenas no plano judicial, mas também, e sobretudo, no âmbito extrajudicial, de modo a exercer sua vocação com resolutividade e proatividade, o que se revela com expressivo potencial diante do novo desafio representado pela proteção de dados pessoais.

5. TUTELA PENAL COLETIVA DA PROTEÇÃO DE DADOS PESSOAIS

Como visto, o expresso reconhecimento constitucional da proteção de dados pessoais, inclusive, nos meios digitais, como direito fundamental (art. 5º, inciso LXXIX), atrai a incidência de todo o regime jurídico aplicável à tutela dos bens jurídicos assim qualificados.

Ademais, considerando que a Constituição Federal, em seu art. 5º, § 1º, preceitua que "as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata", e que a proteção de dados pessoais já conta com legislação própria desde o advento da Lei 13.709/2018, tem-se o arcabouço normativo mínimo para a adoção das medidas institucionais necessárias à adequada tutela desse bem jurídico.

15. Dispõe sobre instauração e tramitação do procedimento investigatório criminal a cargo do Ministério Público. Inteiro teor disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resoluo-181-2-verso-compilada.pdf

Nesse contexto, ante o imperativo constitucional que veda a proteção deficiente de direitos fundamentais, faz-se mister conferir a interpretação mais abrangente para a proteção de dados pessoais, inclusive em homenagem ao princípio da máxima efetividade dos ditames da Constituição.

Portanto, considerando que a tutela de direitos fundamentais, para a consecução de tais objetivos constitucionais em sua máxima amplitude, exige o referido esforço interpretativo e institucional, defende-se que a atuação do Ministério Público, com todo o instrumental já analisado, deva ocorrer não apenas na esfera cível, mas também penal, tanto de forma preventiva quanto repressiva, buscando as soluções necessárias, sejam de índole material, sejam processuais.

Desse modo, entende-se que, também assim (preventiva ou repressivamente), se deve proceder em matéria de proteção de dados pessoais, conforme preceitua o Conselho Nacional do Ministério Público, em sua Resolução 281/2023:

> Art. 59. O Ministério Público, no âmbito de suas atribuições, deverá atuar para prevenir e coibir a violação das normas de proteção de dados pessoais e da autodeterminação informativa quando constatada lesão ou ameaça de lesão a direitos individuais indisponíveis, difusos, coletivos e individuais homogêneos (...)[16]

5.1. VERTENTES PREVENTIVA E REPRESSIVA

Considerando a normativa do CNMP, que preceitua a atuação do Ministério Público para prevenir e coibir violações à proteção de dados pessoais, tanto em caso de lesão quanto de ameaça ao referido direito, cumpre analisar de que forma se podem articular as iniciativas ministeriais, visando à consecução da tutela penal coletiva objeto do presente estudo.

Ademais, ante a assentada premissa de que a proteção de dados pessoais no Brasil tem se revelado um microssistema jurídico, dada a transversalidade de temas e de instrumentos de garantia previstos no ordenamento (à semelhança do que ocorre com o Direito do Consumidor e com o Direito Ambiental, por exemplo), entendemos necessária a articulação de iniciativas às quais usualmente se atribui natureza não penal, mas que são extremamente úteis, especialmente na vertente preventiva.

A esse respeito, cumpre relembrar o instituto da recomendação, legalmente previsto (art. 6°, inciso XX, da Lei Complementar n° 75/93) para

16. Note-se que referido artigo reforça o quanto adrede já defendido, no sentido de que a proteção de dados fundamentais pode assumir feição de difusos, coletivos ou individuais homogêneos, a depender do caso concreto, mas todos com a legitimidade do Ministério Público expressamente assegurada e sua atuação devidamente incentivada pelo seu órgão constitucional de controle externo, qual seja, o CNMP.

buscar a "melhoria dos serviços públicos e de relevância pública, bem como o respeito, aos interesses, direitos e bens cuja defesa lhe cabe promover, fixando prazo razoável para a adoção das providências cabíveis".

Embora expedido unilateralmente pelo Ministério Público e dependente da adesão voluntária por parte do destinatário, indubitável que representa um primeiro passo, em uma escala de uso progressivo da força, para evitar a ocorrência de violação à proteção de dados pessoais[17], inclusive com repercussão penal, uma vez que, nos termos da Resolução CNMP nº 164/2017, a recomendação serve "como instrumento de prevenção de responsabilidades ou correção de condutas".

Tanto que, o Ministério Público Militar, cuja atuação tem ocorrido precipuamente na esfera penal (ao menos se considerada a competência da Justiça Militar federal, especializada em matéria criminal), emprega largamente a recomendação com intento preventivo da ocorrência de crimes militares, a exemplo do que ocorre na atividade de fiscalização prisional, conforme FARIAS (2018, p. 92).

Da mesma forma, cabível o compromisso de ajustamento de conduta em matéria de proteção de dados pessoais[18], inclusive para evitar práticas penalmente relevantes, a exemplo de todas aquelas elencadas nos incisos do art. 59 da Resolução CNMP nº 281/2023[19] (em rol não exaustivo, vale ressaltar).

---

17. A esse respeito, mais uma vez cabe salientar iniciativa no âmbito do Ministério Público do Distrito Federal e Territórios, desta feita acerca da expedição de recomendação em matéria de proteção de dados pessoais, cujo inteiro teor encontra-se disponível em https://www.mpdft.mp.br/portal/pdf/recomendacoes/espec/recomendacao_espec_2020_002.pdf

18. A propósito, novamente merecem destaque, inclusive a título ilustrativo, os termos de ajustamento de conduta celebrados pelo Ministério Público do Distrito Federal e Territórios, tais como os disponíveis em https://www.mpdft.mp.br/portal/index.php/mpdft-acao/termos-de-ajustamento-de-conduta/10567-unidade-especial-de-protecao-de-dados-e-inteligencia-artificial-espec

19. A propósito, confiram-se as mencionadas hipóteses trazidas pela Resolução: "I - transferência de bancos de dados pessoais, inclusive com fins econômicos; II - disseminação de dados pessoais; III - tratamentos automatizados de dados pessoais, inclusive sensíveis; IV - uso de instrumentos de inteligência artificial; V - análises de perfis de titulares, inclusive por meio de agregações de dados históricos; VI - prejuízos à igualdade de oportunidades; VII - abuso de poder econômico; VIII - abuso do poder de direção em relações de trabalho em geral, inclusive no âmbito de grupos econômicos e em contratos de prestação de serviços; IX - ausência de interesses legítimos do controlador; X - ausência de base legal para o tratamento de dados pessoais sem consentimento do titular; XI - ausência de transparência algorítmica; XII - prejuízos ao exercício da cidadania em meios digitais; XIII - manutenção indevida de dados pessoais; XIV - deficiências em processos de anonimização ou pseudonimização de dados pessoais, sobretudo de dados pessoais sensíveis; XV - acesso indiscriminado a dados pessoais sensíveis de titulares, em relações como as de consumo e de trabalho; XVI - incidentes de segurança no tratamento de dados pessoais, notadamente de dados pessoais sensíveis; XVII - coleta de consentimento de forma genérica, ambígua, induzida, excessiva ou com abuso de poder

E isso porque, assim como a recomendação, o ajustamento de conduta depende da adesão voluntária do destinatário, mas, por se tratar de negócio jurídico celebrado pelo Ministério Público com o potencial violador das normas de proteção de dados pessoais, visando evitar a ocorrência de danos ou mesmo buscando a sua reparação, na medida em que tem natureza de título executivo passível de cobrança judicial, pode contribuir de maneira decisiva para a evitar a eclosão de ilícitos penais, inclusive aqueles de repercussão coletiva (ante a multiplicidade de ofendidos que usualmente se observa em tal contexto).

Prosseguindo na escala de força dos instrumentos jurídicos disponíveis ao Ministério Público, ainda na vertente preventiva da tutela (penal) coletiva da proteção de dados pessoais, cabe destacar a ação civil pública, uma vez que pode servir à cessação compulsória de práticas violadoras (mesmo que apenas potencialmente) desse direito fundamental, sobretudo quando alcançada a tutela jurisdicional em tempo hábil (ainda que a título cautelar), de modo a evitar a consumação de fatos típicos penais.

Por seu turno, em matéria repressiva, a tutela penal da proteção de dados pessoais, tanto em sua dimensão individual quanto coletiva, encontra diversos desafios, sobretudo ante a ainda incipiente produção normativa sobre o tema.

Além da já mencionada ação civil pública, para buscar a reparação compulsória dos danos eventualmente causados por eventual prática violadora das normas de proteção de dados pessoais, merecem destaque os instrumentos mais vocacionados à tutela penal, que também podem ser utilizados de forma eficaz em sua vertente coletiva.

Primeiramente, seguindo a mesma técnica de uso progressivo da força jurídica, salienta-se a possibilidade da celebração do acordo de não persecução penal (ANPP), legalmente previsto no art. 28-A do Código de Processo Penal e regulamentado, no âmbito do Ministério Público, pela Resolução CNMP nº 181/2017.

Trata-se de instrumento alternativo à propositura da ação penal, tendo natureza negocial, por meio do qual o agente confessa circunstanciada

econômico; XVIII - perda, modificação ou eliminação indevidas de dados pessoais; XIX - obtenção indevida de dados pessoais; XX - coleta de dados pessoais sem necessidade ou finalidade delimitadas; XXI - informações insuficientes sobre a finalidade do tratamento; XXII - falha em considerar direitos do titular de dados pessoais; XXIII - vinculação ou associação indevidas, direta ou indireta, de dados pessoais; XXIV - falha ou erro de processamento durante a execução de operações de tratamento; XXV - reidentificação indevida de dados pseudonimizados ou com anonimizações deficientes; XXVI - técnicas de engenharia social que acarretem o ilícito tratamento de dados pessoais, inclusive a indevida inclusão de dados pessoais inexatos; XXVII - fundamentação do tratamento em base legal equivocada ou com erro grosseiro; e XXVIII - quaisquer outras violações aos princípios e às normas protetivas de dados pessoais".

e voluntariamente a prática do ilícito criminal, comprometendo-se ao cumprimento de condições previstas na lei, sem prejuízo de outras pactuadas com o Ministério Público, sob pena de rescisão do acordo e consequente oferecimento de denúncia.

Considerando que, dentre referidas condições, encontram-se a reparação do dano e outras medidas que se revelem proporcionais e compatíveis com a infração penal imputada, verifica-se um campo fértil para a tutela coletiva do direito fundamental à proteção de dados pessoais, uma vez que passível de mensuração e adequação ao caso concreto, especialmente quanto à extensão do dano e aos titulares eventualmente atingidos.

Ocorre que, apesar do grande potencial de emprego do ANPP para os casos de violação da proteção de dados pessoais, referido instrumento também guarda suas limitações e hipóteses de não cabimento, tanto objetivas (crimes cuja pena mínima não ultrapasse os quatro anos, já consideradas as causas de aumento ou de diminuição aplicáveis) quanto subjetivas (reincidência ou ter tido o mesmo benefício há menos de cinco anos), de modo que não se pode desconsiderar a possibilidade da persecução por meio da investigação e do processo penal convencionais.

Entretanto, conforme se analisará a seguir, sobretudo quando se considera a partir de um contexto de tutela coletiva, ainda são grandes os desafios para a proteção de dados pessoais em matéria penal e processual penal.

5.2. ASPECTOS MATERIAIS E PROCESSUAIS PENAIS

Na seara da tutela penal do direito à proteção de dados pessoais, a primeira grande deficiência que se extrai da legislação de regência é a ausência da previsão legal de tipos penais específicos para o tema.

Embora a LGPD conte com seção alusiva às sanções administrativas, não traz definição de crimes nem de penas em matéria de proteção de dados, limitando-se a, em seu art. 52, § 2º, assegurar a aplicação das sanções penais previstas no Código de Defesa do Consumidor e em legislação específica.

Ou seja, transcorridos seis anos da edição da LGPD, ainda se faz necessário subsumir os casos concretos dessa especial temática aos tipos penais concebidos para a proteção de bens jurídicos apenas transversais ou mediatos à proteção de dados pessoais, a revelar a violação ao princípio constitucional da vedação à proteção deficiente, na vertente penal.

Desse modo, visando mitigar tal deficiência, ainda verificada na tutela penal da proteção de dados pessoais, faz-se necessário um grande esforço institucional e interpretativo para adequação das estruturas e dos instrumentos jurídicos existentes, para o que se revela essencial o engajamento do Ministério Público brasileiro como um todo nessa temática, aspecto evidenciado pela Resolução CNMP nº 281/2023.

No plano interpretativo dos elementos normativos já existentes, faz-se imperiosa a "releitura da noção de bem jurídico penal" (Almeida e Costa, 2022, p. 30), de modo a se incluir em tal categoria os bens coletivos, alcançando até mesmo aqueles "por ficção jurídica", ou "artificialmente coletivos" ou "processualmente coletivos" (Almeida e Costa, 2022, p. 30), já objetos de tutela na área não penal, inclusive do direito à proteção de dados pessoais.

Ocorre que, apesar desse esforço, logo se nota que "a proteção dos bens jurídico-penais coletivos não se ajusta ao Direito Penal clássico" (Almeida e Costa, 2022, p. 31), sendo necessários, ainda, outros expedientes de adequação jurídica do tratamento do tema em matéria criminal, a exemplo dos "quatro princípios básicos (...) na tutela penal dos interesses difusos"[20].

Por fim, outra importante medida que se deve incorporar em matéria de tutela penal coletiva, especialmente na temática da proteção de dados pessoais, guarda relação com a ideia de que "condutas que lesionam ou expõem a risco bens e interesses difusos também podem causar danos imateriais, que também devem ser objeto da relação processual com vistas à sua integral reparação" (Turessi e Ponte, 2022, p. 343-374).

Além de tais considerações acerca da tutela penal da proteção de dados em sua dimensão material ou substantiva, imperioso analisar as implicações processuais inerentes, sobretudo na vertente coletiva.

Primeiramente, destaca-se a necessidade de uma nova "sistematização dos princípios, das garantias e das regras processuais", de tal modo que "implique em reconhecer a necessidade de uma investigação criminal, de uma persecução e, enfim, de um processo penal coletivo" (Moraes e Costa, 2019, p. 1609-1648).

A esse respeito, considerando que, em matéria de proteção de dados pessoais, as violações mais expressivas ocorrem predominantemente em meio cibernético, e que a proteção constitucional a esse direito, conforme art. 5º, inciso LXXIX, alcança os meios digitais, inescapável a constatação de que "as novas formas criminosas não podem ser demonstradas pelos meios clássicos de prova disciplinados no Código de Processo Penal", sendo necessários "novos meios de prova e obtenção de prova" (Turessi e Ponte, 2022, p. 343-374), inclusive "provas por estatísticas e provas por amostragem" (Almeida e Costa, 2022, p. 264).

20. Sobre o tema, Almeida e Costa (2020) propõem: "1) a responsabilidade penal da pessoa jurídica; 2) a responsabilidade pessoal do representante da pessoa jurídica, seja de direito público, seja de direito privado; 3) a possibilidade de transação penal coletiva, de suspensão condicional do processo coletiva e de celebração de acordo de não-persecução penal coletivo; e 4) a aplicação de sanções penais alternativas" e, ainda, "modificações substanciais na compreensão de bem jurídico, o abandono da concepção individualista de conduta, a possibilidade de ampla responsabilização da pessoa jurídica, a aplicação da imputação objetiva, a delimitação dos contornos da teoria do domínio do fato, a adoção de novas técnicas de combate à criminalidade organizada, (...) e a devida delimitação dos deveres de cuidado".

Outro mecanismo que ganha em importância para a investigação e o processo penal em matéria de proteção de dados é a cooperação internacional, uma vez que, no mais das vezes, as violações perpetradas de forma criminosa prestam-se a abastecer bases de dados clandestinas hospedadas em serviços informáticos de países diversos, até mesmo como estratégia para dificultar a responsabilização dos envolvidos[21].

Ainda em matéria processual, essencial a revisão, proposta por Almeida e Costa (2022), da compreensão da causa de pedir e do pedido nas ações penais de natureza coletiva, assim como do alcance da cognição judicial para temas de natureza multidisciplinar, fazendo incidir o "princípio da máxima amplitude, de modo que são cabíveis todas as medidas necessárias à reparação e à prevenção, inclusive no que concerne à concessão de tutela inibitória para evitar a prática, a repetição ou a continuidade do ilícito penal" (Almeida e Costa, 2020).

Outra releitura que se sugere, e que se mostra de especial valia para a tutela do direito à proteção de dados pessoais, refere-se à prevalência da "vítima difusa e da reparação dos danos" (Turessi e Ponte, 2022), a evidenciar a necessidade de se ampliar o emprego "da via consensual para a solução de conflitos penais e, consequentemente, com o paulatino enfraquecimento do princípio da obrigatoriedade da ação penal" (Turessi e Ponte, 2022, p. 343-374).

Por oportuno, Almeida e Costa (2022) sustentam o cabimento da colaboração premiada coletiva, especialmente interessante para a tutela penal coletiva da proteção de dados pessoais.

Portanto, evidencia-se que a proteção de dados pessoais exige que se supere a tradicional visão do processo penal adversarial como via principal para a tutela penal, sobretudo na sua dimensão coletiva, o que demanda, inevitavelmente, que o Ministério Público adapte sua atuação a essa nova realidade, potencializando o emprego e o alcance dos diversos instrumentos extrajudiciais, preventivos e consensuais, para que se alcance "uma proteção

21. A ampliação dos meios de prova e da cooperação internacional integram uma série de diretrizes propostas para o processo penal coletivo, sugeridas por Almeida e Costa (2020), plenamente aplicáveis à tutela da proteção de dados pessoais: "a) a adoção de medidas para garantir a prevalência da atuação preventiva; b) a estruturação estatal pessoal e com novas tecnologias para fortalecer os meios de investigação criminal; c) a ampla interação e integração entre as esferas de atuação na defesa da tutela coletiva: penal e não penal; d) a ampliação da causa de pedir e do pedido na Ação Penal Coletiva, tendo em vista a sua natural complexidade e as garantais constitucionais coletivas de tutela dos bens jurídico-penais coletivos fundamentais para a dignidade social e a efetivação do Estado Democrático de Direito como Estado de Justiça Material (art. 3º da CR/1988); e) a utilização de novos meios de provas, inclusive provas por estatísticas e provas por amostragem; f) o alargamento no plano da cognição judicial em uma perspectiva multidisciplinar; g) a aplicação do sistema de coisa julgada coletiva *secundum eventum litis* e *secundum eventum probationis* no Sistema do Direito Processual Penal Coletivo; h) a ampliação e o fortalecimento dos mecanismos de cooperação nacional e internacional; i) a observância dos princípios da máxima amplitude e da máxima utilidade da tutela jurisdicional penal coletiva.

suficiente e eficiente dos interesses transindividuais" (Moraes e Costa, 2019, p. 1609-1648).

6. CONCLUSÃO

A proteção de dados pessoais, objeto de normatização e de jurisprudência no âmbito europeu desde cerca de quatro décadas, foi expressamente prevista no ordenamento brasileiro apenas recentemente, tanto no plano constitucional (art. 5º, LXXIX, da CF/88, incluído pela EC 115/2022) quanto infraconstitucional (Lei 13.709/2018), revelando-se o mais novo microssistema jurídico do país, dada a transversalidade do tema nos mais diversos ramos do Direito e a necessidade de uma abordagem especializada.

Nesse contexto, com uma normativa ainda incipiente e carente de uma série de previsões para a adequada tutela do direito fundamental à proteção de dados pessoais, resta pela frente um longo desafio, administrativo, cível e criminal, para os quais já se destacam, cada qual em sua missão institucional, a Autoridade Nacional de Proteção de Dados (ANPD) e o Ministério Público, constitucionalmente vocacionado à defesa dos direitos fundamentais.

Embora saudável e necessária a inspiração e a interação com os modelos mais consolidados em matéria de proteção de dados[22], faz-se ainda maior o desafio na realidade brasileira, com uma enorme massa de dados pessoais (basta considerar que o Brasil conta com mais de duzentos milhões de habitantes) e cujos titulares são, majoritariamente, hipossuficientes na temática.

Em boa hora, pois, editada a Resolução nº 281 do Conselho Nacional do Ministério Público, como marco jurídico orientador da atividade administrativa e finalística do Ministério Público brasileiro para essa hercúlea tarefa de tutela do direito fundamental à proteção de dados pessoais, sobretudo para fomentar as mudanças institucionais necessárias.

Além do esforço institucional, faz-se mister buscar toda a criatividade interpretativa, seja sobre o emprego dos métodos tradicionais, seja para a adoção de novas estratégias e instrumentos, inclusive legislativos, para a almejada tutela integral do direito fundamental à proteção de dados pessoais, com enfoque na prevenção e na consensualidade, a reforçar a vocação extrajudicial do moderno Ministério Público brasileiro.

22. A esse respeito, louvável a parceria entre o Colégio de Encarregados pelo Tratamento de Dados Pessoais nos Ministérios Públicos (CEDAMP) do Brasil e o Centro de Estudos de Seguridade (CESEG) da Universidade de Santiago de Compostela (USC) da Espanha, que promoveram a "Formación de Alto Nivel en Protección de Datos", durante o primeiro semestre de 2024, curso que contou com a participação de integrantes dos diversos ramos do Ministério Público brasileiro e do Conselho Nacional do Ministério Público com atuação na temática.

Portanto, a criação de estruturas especializadas (promotorias, procuradorias, centros de apoio) no Ministério Público revela-se medida importante e necessária para a articulação de todas as vertentes de atribuição ministerial, devendo ser integradas por membros e servidores com conhecimento especializado e com perfil proativo para atuar tanto na área penal quanto não penal, preferencialmente na vertente coletiva da proteção de dados pessoais.

Somente assim, com transversalidade, proatividade e criatividade, articulando-se instrumentos usualmente empregados na esfera cível aos já adotados na esfera penal, buscando a prevenção, a consensualidade e a resolutividade típicas do moderno Ministério Público brasileiro, faz-se viável a tutela penal coletiva do direito fundamental à proteção de dados pessoais, vertente que se revela a mais adequada em contexto de violação massiva, sobretudo a que se verifica diuturnamente nos meios digitais.

7. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Almeida, G. A. de., e **Costa**, R. de O. (2020). Direito Processual Penal Coletivo e a Tutela dos Bens-Jurídicos Penais Coletivos Fundamentais: Direitos ou Interesses Difusos, Coletivos e Individuais Homogêneos. *In* É. Milaré (coord.), *Ação Civil Pública*. São Paulo: Editora Revista dos Tribunais.

Brasil. Conselho Nacional do Ministério Público. (2007). Resolução nº 23, de 17 de agosto de 2007. Disciplina, no âmbito do Ministério Público, a instauração e tramitação do inquérito civil. Disponível em https://www.cnmp.mp.br/portal/images/Normas/Resolucoes/Resoluo-0232.pdf

Brasil. Conselho Nacional do Ministério Público. (2017a). Resolução nº 164, de 28 de março de 2017. Disciplina a expedição de recomendações pelo Ministério Público brasileiro. Disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resolução-164.pdf

Brasil. Conselho Nacional do Ministério Público. (2017b). Resolução nº 174, de 4 de julho de 2017. Disciplina, no âmbito do Ministério Público, a instauração e a tramitação da Notícia de Fato e do Procedimento Administrativo. Disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resoluo-174-2.pdf

Brasil. Conselho Nacional do Ministério Público. (2017c). Resolução nº 179, de 26 de julho de 2017. Disciplina, no âmbito do Ministério Público, a tomada do compromisso de ajustamento de conduta. Disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resolução-179.pdf

Brasil. Conselho Nacional do Ministério Público. (2017d). Resolução nº 181, de 7 de agosto de 2017. Dispõe sobre instauração e tramitação do

procedimento investigatório criminal a cargo do Ministério Público. Disponível em https://www.cnmp.mp.br/portal/images/Resolucoes/Resoluo-181-2-verso-compilada.pdf

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Brasil. Supremo Tribunal Federal. (2020). Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6387/DF. Relatora Ministra Rosa Weber. Acórdão publicado em 12.11.2020. Disponível em https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf

Farias, J. A. C. de. (2018). *Sistema prisional militar e fiscalização pelo Ministério Público: contributos para o exercício pleno da atribuição*. Disponível em https://bdtd.ucb.br:8443/jspui/bitstream/tede/2481/2/JorgeAugustoCaetanodeFariasDissertacao2018.pdf

Frazão, A., **Carvalho**, A. P., e **Milanez**, G. (2022). *Curso de proteção de dados pessoais: fundamentos da LGPD* (1ª ed.). Rio de Janeiro: Forense.

Moraes, A. R. A., e **Costa**, R. de O. (2019). O Processo Coletivo: primeiras impressões para a construção de uma nova dogmática processual. *Revista Brasileira de Direito Processual Penal*, 5(3), 1609-1648.

Roque, A. (2019). A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). *Revista Eletrônica de Direito Processual – REDP*, 20(2), 1-19.

Turessi, F., e **Ponte**, A. (2022). Tutela penal de interesses difusos, justiça penal negociada e os novos desafios do Ministério Público. *Argumenta Journal Law*, 36, 343-374.

Zavascki, T. A. (2016). *Processo coletivo: tutela de direitos coletivos e tutela coletiva de direitos* (6ª ed.). São Paulo: Editora Revista dos Tribunais.

OS DESAFIOS DO MINISTÉRIO PÚBLICO COMO GARANTIDOR DOS DIREITOS DE PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA FRENTE ÀS NOVAS TECNOLOGIAS

Cláudia Pessoa Marques da Rocha Seabra[1]
Andrea Cristina de Sousa Fialho[2]

Resumo: O artigo analisa a evolução da proteção de dados e da autodeterminação informativa na era digital, enfatizando o papel fundamental do Ministério Público como garantidor desses direitos essenciais. O texto traça o desenvolvimento do conceito de privacidade até a noção mais ampla de proteção de dados impulsionados pelos avanços tecnológicos. Discute-se o surgimento de legislações específicas, como o GDPR, na Europa, e a LGPD, no Brasil, que buscam regular o tratamento de dados pessoais. O conceito de autodeterminação informativa é explorado, destacando sua importância no contexto digital atual. Em seguida, examina-se o papel constitucional do Ministério Público na defesa dos direitos fundamentais, incluindo a proteção de dados. São apresentadas perspectivas futuras para a atuação do Ministério Público, como a criação de estruturas especializadas, capacitação contínua, cooperação interinstitucional, ações educativas para a sociedade e o uso de tecnologias inovadoras nas investigações. O texto conclui ressaltando a importância de uma atuação proativa do Ministério Público na defesa dos direitos digitais dos cidadãos, enfatizando a necessidade de constante atualização e adaptação às mudanças tecnológicas para garantir a efetiva proteção de dados e autodeterminação informativa na era digital.

Palavras-chave: Proteção de Dados. Autodeterminação Informativa. Ministério Público. Era Digital. Direitos Fundamentais. Tute Coletiva. Novas Tecnologias. LGPD.

Resumen: El artículo analiza la evolución de la protección de datos y la autodeterminación informativa en la era digital, enfatizando el papel

1. Procuradora-Geral de Justiça do Ministério Público do Estado do Piauí. Pós-graduada em Direito Administrativo pela UFCE. Especialista em Proteção de Dados Pessoais pela FMP.

2. Mestre em Políticas Públicas pela Universidade Federal do Piauí/UFPI.

fundamental del Ministerio Público como garante de estos derechos esenciales. El texto traza el desarrollo del concepto de privacidad hasta la noción más amplia de protección de datos, impulsado por los avances tecnológicos. Se discute el surgimiento de legislaciones específicas, como el RGPD en Europa y la LGPD en Brasil, que buscan regular el tratamiento de datos personales. Se explora el concepto de autodeterminación informativa, destacando su importancia en el contexto digital actual. A continuación, se examina el papel constitucional del Ministerio Público en la defensa de los derechos fundamentales, incluyendo la protección de datos. Se presentan perspectivas futuras para la actuación del Ministerio Público, como la creación de estructuras especializadas, capacitación continua, cooperación interinstitucional, acciones educativas para la sociedad y el uso de tecnologías innovadoras en las investigaciones. El texto concluye resaltando la importancia de una actuación proactiva del Ministerio Público en la defensa de los derechos digitales de los ciudadanos, enfatizando la necesidad de constante actualización y adaptación a los cambios tecnológicos para garantizar la efectiva protección de datos y autodeterminación informativa en la era digital.

Palabras clave: Protección de Datos. Autodeterminación Informativa. Ministerio Público. Era Digital. Derechos Fundamentales. Tutela Colectiva. Nuevas Tecnologías. LGPD.

1. INTRODUÇÃO

A revolução tecnológica do século XXI, marcada por sua velocidade e abrangência inéditas, vem transformando a maneira como as informações individuais são manipuladas e compartilhadas na esfera digital, segundo Zuboff (2019), impulsionada pela captura, análise e distribuição de dados pessoais no panorama cibernético mundial.

Neste cenário, caracterizado pela presença de dispositivos conectados e sistemas de inteligência artificial cada vez mais sofisticados, como destaca Véliz (2020), a interação humana com o mundo digital tornou-se uma fonte contínua de dados. Em cada interação online, voluntária ou não, os indivíduos deixam rastros digitais que podem ser coletados, analisados e utilizados de maneiras nem sempre transparentes ou éticas.

As implicações dessa nova realidade se estendem para além da esfera individual, afetando a sociedade como um todo. O tratamento de dados em larga escala pode influenciar desde decisões de consumo até processos democráticos, como demonstrado por recentes escândalos envolvendo o uso indevido de informações pessoais em campanhas políticas.

A proteção de dados e a autodeterminação informativa no mundo digital representam, portanto, não apenas um desafio técnico ou legal, segundo Doneda (2019), mas também uma questão ética e social de primeira ordem. O equilíbrio entre inovação tecnológica e preservação dos direitos individuais será um dos grandes desafios das próximas décadas, conforme Véliz (2020), demandando um esforço conjunto de governos, empresas e sociedade civil para construir um futuro digital mais seguro, ético e respeitoso com a privacidade dos indivíduos, o que torna imperativo o desenvolvimento de marcos regulatórios robustos e atualizados, capazes de acompanhar o ritmo acelerado da inovação tecnológica. Legislações como o Regulamento Geral de Proteção de Dados (GDPR), na União Europeia, e a Lei Geral de Proteção de Dados (LGPD), no Brasil, são passos importantes nessa direção, mas é necessário um esforço contínuo de atualização e fiscalização.

Frente a esta realidade, é fundamental que haja uma atuação efetiva por parte do Ministério Público para garantir que os direitos à proteção de dados e à autodeterminação informativa sejam respeitados. O objetivo deste artigo é analisar o papel do Ministério Público nesse contexto e discutir as medidas que podem ser adotadas para enfrentar os desafios impostos pelas novas tecnologias. A pergunta norteadora que guiará nossa análise é: Como o Ministério Público pode garantir a proteção de dados e a autodeterminação informativa diante dos desafios impostos pelas novas tecnologias?

Para responder à referida pergunta, o presente artigo foi estruturado para, inicialmente, trazer a conceituação necessária para o seu desenvolvimento e, posteriormente, adentrar nos pontos de análise específica. A primeira parte aborda a evolução do direito de privacidade e a sua limitação na era da sociedade de informação, o que levou ao surgimento do direito à proteção de dados. A segunda parte destaca a normatização do direito à proteção de dados tanto em outros países quanto no Brasil. A terceira parte destaca a importância da autodeterminação informativa nesta nova cena. Por fim, a quarta parte aborda a evolução do Ministério Público como garantidor dos direitos fundamentais individuais e coletivo, sobretudo, a proteção de dados e a autodeterminação informativa.

2. DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS

O conceito de privacidade começou a ganhar forma, na lição de Zuboff (2019), com a Revolução Industrial e o crescimento das cidades, que levaram

a uma maior proximidade e interação entre as pessoas. A necessidade de proteger a vida privada e familiar dos olhares e intromissões alheios tornou-se cada vez mais evidente.

O artigo de Samuel Warren e Louis Brandeis, como assinala Bessa (2020), publicado na Harvard Law Review, em 15 de dezembro de 1890, é considerado um marco na história do direito à privacidade. Os autores defenderam a existência de um direito em ser deixado em paz, protegendo a vida privada e a intimidade das pessoas.

O artigo 12 da Declaração Universal dos Direitos Humanos (Assembleia Geral da ONU, 1948) reconhece o direito à privacidade como um direito humano universal, estabelecendo que "ninguém será sujeito a interferências na sua vida privada, família, domicílio ou correspondência, nem a ataques à sua honra e reputação", esse teor foi, mais adiante, reiterado no artigo 8º da Convenção Europeia sobre Proteção dos Direitos Humanos e das Liberdades Fundamentais, assinada em Roma, em novembro de 1950, e no artigo 17 do Pacto Internacional de Direitos Civis e Políticos proclamado pela Assembleia Geral das Nações Unidas em dezembro de 1966.

O desenvolvimento de novas tecnologias, como a fotografia, o telefone e a vigilância eletrônica, de acordo com Doneda (2019), intensificou a preocupação com a privacidade. Diversos países passaram a incorporar o direito à privacidade em suas constituições e leis, reconhecendo-o como um direito fundamental. (Colocar artigo da CRFB/88 que fala sobre a proteção à privacidade)

Para Bioni (2021), a privacidade tem sido historicamente articulada com base na dicotomia entre as esferas pública e privada, sendo sua lógica centrada na liberdade negativa de o indivíduo não sofrer interferências alheias, um direito estático, à espera de que seu titular delimite quais fatos de sua vida devem ser excluídos do domínio público.

Nesse contexto, a privacidade está vinculada ao direito à intimidade, ao anonimato e à liberdade de se resguardar de intromissões. O objetivo é proteger a vida privada e pessoal dos indivíduos contra invasões, seja pelas mãos do Estado ou de outros cidadãos.

Com a ascensão da Ciência da Computação e, posteriormente, da internet, o conceito de privacidade começou a se transformar. A digitalização das interações sociais e profissionais, bem como a proliferação de tecnologias de informação e comunicação, segundo Bioni (2019), reinventaram os meios pelas quais informações pessoais são coletadas, armazenadas, processadas e transmitidas. As ameaças à privacidade se multiplicaram, indo muito além das invasões físicas ou observacionais. A questão central passou a ser a proteção dos dados, não apenas a privacidade.

Isto se dá porque, cada vez mais, a atividade de tratamento de dados impacta a vida das pessoas, como enfatiza Zuboff (2019), em particular,

quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados tutela a própria dimensão relacional da pessoa humana, em especial, para que tais decisões não ocasionem práticas discriminatórias, o que extrapola o âmbito da tutela do direito à privacidade.

A proteção dos dados pessoais como um novo direito da personalidade, segundo Bioni (2019), abrange todo e qualquer dado que denote o prolongamento de um sujeito. Dados pessoais não se limitam, portanto, a um tipo de projeção imediata, mas também a um referencial mediato que pode ter ingerência na esfera de uma pessoa.

O direito à proteção de dados, no entendimento de Bioni (2019), opera fora da lógica binária do público e do privado, bastando que a informação esteja atrelada a uma pessoa para deflagrá-lo. Diante disso, a proteção de dados se apresenta como um direito fundamental, essencial para a construção de uma sociedade mais justa, livre e democrática. Ao garantir o controle sobre suas informações pessoais, de acordo com Mendes (2020), os indivíduos podem exercer sua autonomia e podem participar plenamente da vida social e política. A evolução da legislação e a conscientização da sociedade são passos importantes para a construção de um futuro em que a privacidade e a autodeterminação informativa sejam valores inegociáveis.

2.1. DAS LEGISLAÇÕES DE PRIVACIDADE DE DADOS

De acordo com Doneda (2019), ao se analisar o progresso geracional dos normativos de proteção de dados, percebe-se que a primeira geração de leis tem como preocupação o processamento massivo dos dados na esfera governamental, tendo como estratégia regulatória concentrar, na figura do Estado, o poder de criar e licenciar o funcionamento de todos os bancos de dados.

Já a segunda geração, para Doneda (2019), caracteriza-se por transferir, ao próprio titular de dados, a responsabilidade de gerir o seu fluxo de dados por meio do consentimento, estabelecendo as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais.

A amplitude desse papel de protagonismo do indivíduo na proteção dos dados pessoais, no entendimento de Mendes (2020), é o divisor de águas para a terceira geração de leis. As normas de proteção de dados nesse estágio procuram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais da coleta ao compartilhamento, além de criarem deveres para aqueles que coletam e processam dados pessoais.

A grande inovação trazida pelas normas de quarta geração em face das anteriores, como destaca Bioni (2019), foi a disseminação de autoridades independentes para a aplicação das leis de proteção de dados pessoais.

A União Europeia (UE) tem desempenhado um papel importante na evolução da proteção de dados, como assinala Teffé e Medon (2020). A Diretiva 95/46/CE, também conhecida como Diretiva de Proteção de Dados, foi uma das primeiras tentativas significativas para harmonizar as normas de proteção de dados pessoais entre os Estados Membros da UE. Porém, foi com o Regulamento Geral sobre a Proteção de Dados (GDPR), implementado em 25 de maio de 2018, que a UE estabeleceu um padrão robusto e globalmente influente para a proteção de dados.

O GDPR, substituindo a Diretiva 95/46/CE, não apenas harmonizou as leis de proteção de dados na União Europeia, mas também, segundo Mendes (2020), estabeleceu novos direitos para os indivíduos e responsabilidades mais rigorosas para as organizações. Entre os direitos assegurados pelo GDPR estão o direito ao esquecimento, o direito à portabilidade dos dados e o direito de ser informado sobre violações de dados que possam impactar a privacidade individual. A regulamentação também introduziu penalidades substantivas para o não cumprimento, incentivando as organizações a adotarem práticas robustas de proteção de dados.

Além da Europa, outros países e regiões têm adotado legislações inspiradas no GDPR ou desenvolvido marcos legais próprios para a proteção de dados, como Japão, Canadá, Austrália e Brasil.

Ao fortalecer as leis de proteção de dados, reconheceu-se que a privacidade é um aspecto intrínseco à dignidade pessoal e um pilar essencial para o exercício pleno da democracia. Proteger os dados pessoais é, portanto, mais do que uma questão de privacidade, trata-se de garantir liberdade, segurança e justiça na sociedade digital.

2.2. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Até a aprovação da LGPD, o Brasil contava somente com leis setoriais de proteção de dados, como destacam Bioni, Zanatta, Rielli e Vergili (2021), que não cobriam setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Dentre as referidas leis setoriais, pode-se destacar:

- O Código de Defesa do Consumidor, que disciplinou, em seu art. 43, os bancos de dados e cadastros de consumidores, trouxe a exigência de que o consumidor seja notificado da abertura de um banco de dados por ele não solicitado, permitindo que o consumidor acompanhe o fluxo de seus dados e seja garantido o seu acesso, a exatidão das informações, que o banco de dados se restrinja a finalidades claras e verdadeiras e que se observe o limite de cinco anos para o armazenamento de informações negativas. Isso se configura nos direitos de acesso, retificação e cancelamento.

– A Lei do Cadastro Positivo, Lei 12.414/11, trouxe, de forma mais sistematizada, a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los. A lei passou a exigir o consentimento do titular dos dados pessoais em instrumento específico ou em cláusula apartada, inclusive para os casos de compartilhamento da base de dados com terceiros. O referido diploma estabelece, ainda, o dever do gestor da base de dados de não coletar informações excessivas e sensíveis para fins de análise de crédito, bem como de não as utilizar para outra finalidade que não a creditícia.
– O Marco Civil da Internet, Lei 12.965/14, inaugurou uma norma específica para os direitos e garantias do cidadão nas relações travadas na internet. Dentre os direitos previstos, encontram-se a proteção da privacidade e dos dados pessoais, tais como: consentimento expresso para coleta, uso, armazenamento e tratamento de dados pessoais; direito de acesso aos dados coletados; direito de retificação e exclusão dos dados; e direito à portabilidade dos dados.

2.3. A LEI GERAL DE PROTEÇÃO DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/18, marca um momento histórico na proteção de dados pessoais no Brasil. A LGPD regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O escopo da LGPD abrange organizações públicas e privadas, nacionais e internacionais, que tratam dados de indivíduos no Brasil. Essa abrangência reflete a natureza global do fluxo de dados na era digital e a necessidade de uma proteção que transcenda fronteiras nacionais.

A lei apresenta dez princípios essenciais, cada um deles crucial para a construção de um ecossistema de dados ético e responsável, notadamente os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Além disso, a LGPD introduz bases legais específicas e taxativas para o tratamento de dados, incluindo o consentimento do titular, o cumprimento de obrigação legal ou regulatória, a execução de políticas públicas, a realização de estudos por órgãos de pesquisa, a execução de contratos, o exercício regular de direitos em processos, a proteção da vida ou da incolumidade física, a tutela da saúde, o atendimento aos interesses legítimos do controlador e a proteção do crédito.

A lei apresenta a definição de dado pessoal e estabelece categorias especiais de dados, como informações sensíveis (dados 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) e dados de crianças e adolescentes, que exigem proteções adicionais e específicas.

A LGPD fortalece significativamente os direitos dos titulares de dados, conferindo-lhes um conjunto robusto de prerrogativas. Os indivíduos, agora, têm o direito de acessar facilmente seus dados, corrigir informações incompletas ou inexatas, solicitar a exclusão de dados tratados com base no consentimento, portar seus dados para outro fornecedor de serviço ou produto e revogar o consentimento a qualquer momento. Esses direitos empoderam os cidadãos, dando-lhes controle efetivo sobre suas informações pessoais.

A lei também aborda questões complexas, como as transferências internacionais de dados, estabelecendo critérios rigorosos para garantir que os dados dos brasileiros sejam adequadamente protegidos quando transferidos para outros países. Isso inclui a exigência de um nível de proteção de dados adequado por parte do país ou organismo internacional de destino, ou o fornecimento de garantias específicas pelo controlador.

Em essência, a LGPD representa não apenas um salto qualitativo na proteção de dados pessoais no Brasil, mas também uma mudança de paradigma na forma como dados pessoais são valorizados e tratados. Sua implementação bem-sucedida exige um esforço conjunto e contínuo de organizações, indivíduos e autoridades reguladoras.

Esta nova realidade, embora desafiadora, promete criar um ambiente digital mais seguro, transparente e respeitoso aos direitos fundamentais dos cidadãos brasileiros. Além disso, a LGPD posiciona o Brasil como um *player* relevante no cenário internacional de proteção de dados, potencialmente influenciando práticas globais e contribuindo para o desenvolvimento de um ecossistema digital mais ético e centrado no ser humano.

3. AUTODETERMINAÇÃO INFORMATIVA

A autodeterminação informativa está ligada à ideia de transparência e consentimento informado, na lição de Mendes (2020), requerendo que as entidades que coletam e processam dados forneçam informações completas sobre suas práticas de coleta e uso de dados. Isso garante que a participação do indivíduo no processo de coleta de dados seja voluntária, consciente e baseada em uma compreensão plena de como, onde e por que seus dados serão utilizados.

Segundo Bessa (2020), já em 1967, em sua clássica obra *Privacy and Freedom* (Nova Iorque: Atheneum), Alan Westin advertia que, para manter a privacidade na era moderna, o indivíduo precisava ter a possibilidade de definir quando, como e quais informações pessoais poderiam ser comunicadas a terceiros.

Mas o termo "autodeterminação informativa", conforme Mendes (2020), ganhou destaque a partir do julgamento do Tribunal Constitucional Federal Alemão, em 1983, no caso conhecido como "Censo". Por meio da decisão, o tratamento não transparente de dados pessoais foi repudiado a partir da ideia da dignidade da pessoa humana e do livre desenvolvimento da personalidade. Naquela oportunidade, a Corte Constitucional alemã entendeu que, principalmente pela quantidade de informações coletadas, a iniciativa de recenseamento poderia possibilitar a criação de perfis completos da personalidade dos cidadãos, comprometendo a própria autonomia das pessoas. Então, esclareceu-se que o tratamento de dados deve ocorrer somente quando há uma justificativa legal a partir da finalidade do processamento.

As primeiras definições da autodeterminação informativa nasceram na Europa juntamente com a preocupação com a regulamentação dos bancos de dados pessoais. O primeiro passo em direção à proteção desses bancos de informações, de acordo com Navarro (2012), foi a edição da Resolução nº 428 pela Assembleia Consultiva do Conselho da Europa, em 1970, ou seja, muito antes da poderosa ferramenta da internet ganhar popularidade. Esta resolução vedava o acúmulo de informações sobre o indivíduo que pudesse torná-lo 'exposto e transparente', determinando que o Estado deveria apenas armazenar informações pessoais mínimas para fins de prestação de serviços públicos a que essas informações fossem destinadas, seja qual fosse o tipo de serviço, além de prever sanções nos casos de violação desse direito.

No âmago da autodeterminação informativa está o reconhecimento de que os dados pessoais não são meramente informações que podem ser livremente utilizadas por terceiros, como destaca Mendes (2020), mas constituem uma extensão da personalidade de cada indivíduo. Assim, a proteção desses dados é essencial para preservar a autonomia, a privacidade e a liberdade de expressão de cada pessoa.

O direito à autodeterminação informativa é de natureza material, oponível em face do Estado. No exercício da autodeterminação informativa, para Teffé e Medon (2020), o indivíduo pode exercer controle sobre a legitimidade do recolhimento, da divulgação e da utilização de seus dados pessoais, controle esse que é limitado apenas pela lei, diante de manifesto interesse público e atendido o princípio da proporcionalidade.

A partir dessa decisão, como explicita Navarro (2012), ocorreu uma convergência de legislações voltadas à proteção de dados pessoais nos Estados-membros da, então, Comunidade Europeia, de modo que o direito à autodeterminação informativa passou a receber proteção jurídica eficiente no espaço da atual União Europeia. As sucessivas diretivas da Comunidade Europeia e legislações nacionais criaram instrumentos apropriados para lidar com a proteção de dados pessoais, fazendo com que o direito à autodeterminação informativa se identificasse com o direito à proteção de dados pessoais.

A legislação em diversos países e regiões tem buscado responder a esses desafios. O GDPR consagra explicitamente o direito à autodeterminação informativa ao exigir consentimento explícito, o direito de acesso e retificação dos dados, e, até mesmo, o direito ao esquecimento.

No Brasil, a autodeterminação informativa é um dos fundamentos da disciplina de proteção de dados pessoais, de acordo com o art. 2º, inciso II, da Lei Geral de Proteção de Dados (Lei nº 13.709/18 – LGPD).

É, ainda, importante destacar, conforme Maria e Picolo (2021), que a autodeterminação informativa foi um dos pontos amplamente debatidos nas Ações Diretas de Inconstitucionalidade nº 6387, 6388, 6389, 6390, 6393. No acórdão referente, os julgadores definiram que a privacidade só poderá ser mitigada diante de uma justificativa legítima. Além disso, o Ministro Luiz Fux entendeu que "a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada" (Maria & Picolo, 2021, p. 1). Dessa forma, a jurisprudência brasileira reconheceu a autodeterminação informativa como direito fundamental, ressaltando que não existem dados insignificantes no contexto atual de automatização de processos.

Manter e defender a autodeterminação informativa é, portanto, na visão de Teffé e Medon (2020), não apenas uma questão de proteger a privacidade, mas também de salvaguardar a autonomia individual, a dignidade e os direitos fundamentais em uma sociedade cada vez mais mediada pela tecnologia.

A autodeterminação informativa também é crucial no contexto da inteligência artificial e da big data. Algoritmos e sistemas de inteligência artificial dependem enormemente de grandes volumes de dados para funcionar eficazmente. No entanto, o uso desenfreado dessas tecnologias, sem as devidas salvaguardas, pode levar a práticas invasivas e à discriminação algorítmica. Por isso, é essencial que os princípios de autodeterminação informativa sejam incorporados desde o desenvolvimento até a implementação e operação dessas tecnologias.

4. O PAPEL DO MINISTÉRIO PÚBLICO BRASILEIRO COMO GARANTIDOR DOS DIREITOS FUNDAMENTAIS

A Constituição Federal de 1988, de acordo com Goulart (2018), ampliou a atuação do Ministério Público (MP), estabelecendo, dentre suas funções institucionais, a condução do inquérito civil e da ação civil pública. Esses instrumentos visam proteger o patrimônio público e social, o meio ambiente e outros interesses difusos e coletivos. Além disso, o Ministério Público foi investido do poder de expedir notificações em procedimentos administrativos de sua competência, requisitando informações e documentos necessários à sua instrução.

Para Neves (2020), a interpretação do texto constitucional evidencia a íntima relação do Ministério Público com o interesse público, tanto primário quanto secundário. No entanto, a defesa do interesse público secundário só ocorre quando este se alinha com o interesse público primário, uma vez que o Ministério Público pode litigar contra o próprio Estado, independentemente da esfera federativa. Assim, cabe ao órgão ministerial salvaguardar os direitos difusos e coletivos, bem como os individuais indisponíveis, atuando como parte ou como fiscal da ordem jurídica.

É importante ressaltar que o rol de matérias de atuação do Ministério Público na defesa dos direitos, conforme estabelecido na Constituição, é meramente exemplificativo. A legislação infraconstitucional pode ampliar essa atuação sempre que necessário para preservar o interesse público. Exemplos dessa expansão incluem a atuação do Ministério Público, conforme Mazzilli (2019), em áreas como a defesa dos direitos das pessoas com deficiência, a proteção dos investidores no mercado de valores mobiliários, a tutela dos direitos da criança e do adolescente, a defesa do consumidor, a proteção do patrimônio público e a salvaguarda da ordem econômica e da livre concorrência.

O avanço da sociedade e o rápido progresso tecnológico impuseram novos desafios ao Ministério Público na manutenção de sua fidelidade aos propósitos institucionais estabelecidos pela Constituição Federal de 1988. Entre essas novas fronteiras de atuação, destaca-se a proteção de dados pessoais alçada à categoria de direito fundamental pela EC 115/22.

Essa evolução na atuação do Ministério Público, segundo Garcia (2021), reflete a natureza dinâmica de suas funções constitucionais, que se expandem para abranger novas áreas de interesse público à medida que a sociedade se transforma. Essa nova abordagem não apenas mantém o Ministério Público alinhado com suas funções constitucionais originais, mas também o posiciona na vanguarda da defesa dos direitos fundamentais em um mundo cada vez mais digitalizado e interconectado.

5. PERSPECTIVAS FUTURAS DA ATUAÇÃO DO MINISTÉRIO PÚBLICO BRASILEIRO COMO GARANTIDOR DO DIREITO À PROTEÇÃO DE DADOS E DA AUTODERMINAÇÃO INFORMATIVA

A revolução digital do final do século XX transformou profundamente a sociedade, colocando a informação e o conhecimento no centro do desenvolvimento econômico. Essa mudança, já mencionada anteriormente, na visão de Véliz (2020), trouxe consigo novos desafios e riscos, especialmente no que diz respeito à proteção de dados pessoais e à autodeterminação informativa.

Diante desses novos desafios, a abordagem individualista tradicional da proteção de dados mostrou-se insuficiente. Assim, de acordo com Mendes (2019), como ocorreu com os direitos de terceira geração (ambientais, do consumidor, etc.), surgiu a necessidade de uma tutela coletiva para a proteção de dados pessoais.

O Brasil, com sua tradição de tutela coletiva, conforme Mulholland (2022), incorporou essa abordagem na Lei Geral de Proteção de Dados Pessoais (LGPD). A lei prevê expressamente a possibilidade de defesa coletiva dos direitos dos titulares de dados e a reparação por danos coletivos:

> Art. 22 da LGPD: A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Nesse contexto, o Ministério Público e outros órgãos legitimados ganham um papel crucial na proteção coletiva de dados pessoais. Podem atuar administrativa ou judicialmente para coibir práticas abusivas, aplicar sanções e buscar reparação por danos coletivos.

As perspectivas futuras para a atuação do Ministério Público na proteção de dados e na autodeterminação informativa são promissoras e desafiadoras na mesma medida. À medida que se avança na era digital, o Ministério Público deve assumir um papel proativo e inovador nas estratégias de proteção dos direitos digitais dos cidadãos.

Diante disso, foi publicada, em dezembro de 2023, a Resolução 2023 do CNMP, que instituiu a Política Nacional e o Sistema Nacional de Proteção de Dados Pessoais do Ministério Público. Entre seus objetivos, está o de fixar premissas programáticas para que o Ministério Público concretize a tutela do direito fundamental à proteção de dados pessoais por meio de seus órgãos de execução nas hipóteses de lesão ou ameaça de lesão ocasionadas por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, de sua sede ou do país onde estejam localizados os dados pessoais, consoante a legislação vigente.

Assim, faz-se necessário, em conformidade com o artigo 56 da referida resolução, que os ramos e as unidades do Ministério Público promovam a estruturação de suas promotorias e procuradorias para atuação na defesa da ordem jurídica e da dimensão coletiva do direito à proteção de dados pessoais diante de violações à legislação por pessoas físicas ou jurídicas, de direito público ou privado.

Os membros do Ministério Público, ainda em conformidade com a Resolução 281/23 do CNMP, poderão requisitar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) com a descrição dos processos de tratamento que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais de forma a promover medidas, salvaguardas e mecanismos de mitigação e eliminação de riscos e danos.

A Resolução traz, ainda, a importância da promoção da capacitação continuada de membros e servidores do Ministério Público voltada para a proteção de dados, segurança da informação e uso ético de tecnologias emergentes para manter o órgão atualizado com as práticas e tendências atuais, bem como com os riscos associados à era digital.

Além disso, deve-se investir em ações educativas para a sociedade, conscientizando a população sobre os riscos e os direitos no ambiente digital. Parcerias com escolas, universidades e outras instituições de ensino podem ser um caminho eficaz para integrar o aprendizado sobre proteção de dados e privacidade ao currículo educacional, preparando cidadãos mais conscientes e capacitados para protegerem suas informações.

Para acompanhar a evolução tecnológica, o Ministério Público pode utilizar ferramentas inovadoras em suas operações, como a inteligência artificial, para análise de dados e automação de processos. Isso pode aumentar a eficiência nas investigações e na análise de casos complexos que envolvam grandes volumes de informações.

Por último, a construção de parcerias com empresas, organizações da sociedade civil e a comunidade acadêmica é fundamental para a promoção e a defesa da proteção de dados e da autodeterminação informativa. A colaboração pode facilitar o desenvolvimento de tecnologias e práticas que respeitem os direitos dos cidadãos e fomentem um ambiente digital ético e seguro.

6. CONCLUSÃO

O Ministério Público, sem dúvida alguma, apresenta-se como um pilar essencial na salvaguarda dos direitos fundamentais à proteção de dados e à autodeterminação informativa. A trajetória institucional do órgão, desde sua redefinição pela Constituição Federal de 1988 até a implementação da Resolução 281/23 do CNMP, evidencia uma evolução consciente e necessária frente aos desafios impostos pela revolução tecnológica e informacional do século XXI.

A atuação do Ministério Público neste novo panorama demanda uma abordagem holística e multidisciplinar. Esta deve abranger desde a rigorosa fiscalização e aplicação das normas de proteção de dados até o desenvolvimento de iniciativas educativas inovadoras, visando à conscientização e ao empoderamento da sociedade civil. É imperativo que o órgão não apenas acompanhe, mas se antecipe às transformações tecnológicas, mantendo-se na vanguarda do conhecimento técnico-jurídico e da aplicação ética e responsável das tecnologias emergentes em suas próprias operações.

Para concretizar essa visão, é fundamental o fortalecimento da estrutura interna do Ministério Público com a criação de núcleos especializados em proteção de dados e tecnologia. Paralelamente, a implementação de

programas robustos de capacitação contínua para membros e servidores é crucial para manter a instituição alinhada com as mais recentes tendências e desafios do mundo digital. O estabelecimento de parcerias estratégicas com a academia, o setor privado e organizações da sociedade civil potencializará a eficácia das ações do MP, promovendo um ecossistema colaborativo na defesa dos direitos digitais.

Ademais, o Ministério Público deve assumir um papel de liderança na promoção de uma cultura de proteção de dados e privacidade. Isso implica não apenas ações reativas, mas também iniciativas proativas que fomentem a conscientização pública, a educação digital e o desenvolvimento de práticas éticas no uso de tecnologias. A formação de cidadãos digitalmente conscientes e críticos é essencial para a construção de uma sociedade mais resiliente aos riscos cibernéticos e mais apta a usufruir dos benefícios da era digital de forma segura e responsável.

Por fim, o papel do Ministério Público na proteção de dados e na garantia da autodeterminação informativa transcende a tradicional aplicação da lei, exigindo uma postura inovadora, colaborativa e profundamente engajada com os desafios contemporâneos. A instituição deve reinventar-se continuamente, equilibrando a preservação de seus valores fundamentais com a adaptabilidade necessária para enfrentar as complexidades do mundo digital. Somente por meio desse compromisso será possível assegurar que o progresso tecnológico ocorra em harmonia com os direitos fundamentais, preservando a dignidade, a liberdade e a autonomia dos indivíduos no intrincado ecossistema digital do século XXI.

7. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Assembleia Geral da ONU. (1948). *Declaração Universal dos Direitos Humanos* (217 [III] A). Paris. Disponível em http://www.un.org/en/universal-declaration-human-rights/

Bessa, L. R. (2020). LGPD e o direito à autodeterminação informativa. *Consultor Jurídico*. Disponível em https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa

Bioni, B. R. (2021). *Proteção de dados pessoais: A função e os limites do consentimento* (3ª ed.). Forense.

Bioni, B. R., **Zanatta**, R. A. F., **Rielli**, M., & **Vergili**, G. (2021). *Proteção de dados pessoais na LGPD: Uma análise setorial*. Thomson Reuters Brasil.

Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Conselho Nacional do Ministério Público. (2023). *Resolução nº 281, de 12 de dezembro de 2023*. Disponível em https://www.cnmp.mp.br/portal/atos-e-normas/norma/10515/

Doneda, D. (2019). *Da privacidade à proteção de dados pessoais: Elementos da formação da Lei geral de proteção de dados* (2ª ed.). Thomson Reuters Brasil.

Doneda, D., **Mendes**, L. S., **Cunha**, M. V., & **Moreira**, T. M. (2022). *Tratado de proteção de dados pessoais*. Forense.

Garcia, E. (2021). *Ministério Público: Organização, atribuições e regime jurídico* (7ª ed.). Saraiva.

Goulart, M. P. (2018). *Ministério Público e democracia: Teoria e práxis*. Editora Lumen Juris.

Maria, I., & **Picolo**, C. (2021). *Autodeterminação informativa: Como esse direito surgiu e como ele me afeta?* LAPIN. Disponível em https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/

Mazzilli, H. N. (2019). *Regime jurídico do Ministério Público* (9ª ed.). Saraiva.

Mendes, L. S. (2019). *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. Saraiva.

Mendes, L. S. F. (2020). Autodeterminação informativa: a história de um conceito. *Pensar - Revista de Ciências Jurídicas, 25(4)*, 1-18. Disponível em https://periodicos.unifor.br/rpen/article/view/10828/pdf

Monteiro, R. L. (2018). *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil*? Instituto Igarapé, Artigo Estratégico 39.

Mulholland, C. (2022). Dados pessoais sensíveis e a tutela de direitos fundamentais: Uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direito do Consumidor, 139*, 179-206.

Navarro, A. M. N. P. (2012). *O direito fundamental à autodeterminação informativa*. In: XXI Congreso Nacional do CONPEDI, Direitos Fundamentais e Democracia II (pp. 410-438), Florianópolis. Disponível em http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c

Neves, D. A. A. (2020). *Manual de processo coletivo* (4ª ed.). Editora JusPodivm.

Teffé, C. S., & **Medon**, F. (2020). Proteção de dados pessoais e direito à autodeterminação informativa: A emergência de um novo direito fundamental na era tecnológica. *Pensar - Revista de Ciências Jurídicas, 25(4)*, 1-14.

Véliz, C. (2020). *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. Bantam Press.

Zanatta, R. A. F. (2019). A tutela coletiva na proteção de dados pessoais: Uma análise da efetividade da LGPD. *Revista de Direito e as Novas Tecnologias, 5*, 1-23.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

A LGPD E O TRATAMENTO DE DADOS: DESAFIOS E APLICAÇÕES NO MINISTÉRIO PÚBLICO

Francisco de Carvalho Neto[1]

Resumo: Este artigo analisa a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Ministério Público brasileiro, identificando suas especificidades em comparação com o setor privado. O estudo apresenta uma descrição geral da LGPD, examinando suas bases legais e princípios fundamentais, além das particularidades do tratamento de dados pessoais realizado pelo Ministério Público. São explorados os desafios enfrentados pela instituição, especialmente relacionados ao equilíbrio entre confidencialidade, transparência e proteção de dados pessoais sensíveis. Também é examinada a Resolução nº 281/2023, do Conselho Nacional do Ministério Público (CNMP), destacando sua relevância como marco regulatório interno. Por fim, são discutidas as bases jurídicas mais adequadas para legitimar o tratamento de dados pessoais no contexto ministerial, propondo uma reflexão crítica sobre os mecanismos necessários para garantir o cumprimento da LGPD e a proteção dos direitos fundamentais.

Palavras-chave: Lei Geral de Proteção de Dados. Ministério Público. Tratamento de Dados Pessoais. Resolução 281/2023 CNMP. Compliance. Privacidade. Segurança da Informação.

Resumen: Este artículo analiza la aplicación de la Ley General de Protección de Datos Personales (LGPD) en el ámbito del Ministerio Público brasileño, identificando sus especificidades en comparación con el sector privado. El estudio presenta una descripción general de la LGPD, examinando sus bases legales y principios fundamentales, además de las particularidades del tratamiento de datos personales realizado por el Ministerio Público. Se exploran los desafíos enfrentados por la institución, especialmente relacionados con el equilibrio entre confidencialidad, transparencia y protección de datos

1. Promotor de Justiça do Ministério Público do Estado do Paraná. Pós-graduado em Direito Civil pela FADISP (2009) e graduado em Direito pela Universidade Presbiteriana Mackenzie (2006). Ex-professor de Direito Penal e Processo Penal na graduação da FAG -Toledo e professor de pós-graduação na FAG - Cascavel.

personales sensibles. También se examina la Resolución n° 281/2023, del Consejo Nacional del Ministerio Público (CNMP), destacando su relevancia como marco regulatorio interno. Finalmente, se discuten las bases legales más apropiadas para legitimar el tratamiento de datos personales en el contexto ministerial, proponiendo una reflexión crítica sobre los mecanismos necesarios para asegurar la conformidad con la LGPD y la protección de los derechos fundamentales.

Palabras clave: Ley General de Protección de Datos. Ministerio Público. Tratamiento de Datos Personales. Resolución 281/2023 CNMP. Conformidad. Privacidad. Seguridad de la Información.

1. INTRODUÇÃO

A proteção de dados pessoais tornou-se um tema central no cenário jurídico contemporâneo, impulsionada pelo avanço tecnológico e pelo crescente fluxo de informações no mundo digital. No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, representa um marco normativo fundamental para regulamentar o tratamento de dados pessoais tanto no setor público quanto no privado. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD tem como principal objetivo assegurar a privacidade e a proteção dos dados dos indivíduos, promovendo transparência e responsabilidade no tratamento dessas informações.

O tratamento de dados, conforme definido pela LGPD em seu art. 5º, inciso X, abrange uma ampla gama de operações, que incluem a coleta, armazenamento, processamento, transferência, entre outros. A lei estabelece bases legais específicas para que o tratamento de dados seja considerado lícito, ressaltando a importância da conformidade legal como um dos pilares do tratamento regular. Entre essas bases, destacam-se o consentimento do titular, o cumprimento de obrigação legal, a execução de políticas públicas e a tutela da saúde.

A aplicação da LGPD transcende as esferas do setor privado, estendendo-se ao poder público e, em especial, ao Ministério Público. No setor privado, a principal finalidade do tratamento está vinculada aos interesses comerciais, visando à personalização de produtos e serviços e à otimização da experiência do cliente. Em contrapartida, o Ministério Público, como instituição pública de características únicas, enfrenta complexidades decorrentes de suas atribuições constitucionais, como a defesa dos direitos fundamentais e a

promoção da justiça. Essas responsabilidades frequentemente implicam no tratamento de dados sensíveis e no equilíbrio entre sigilo e transparência.

Diante desse cenário, o presente artigo se propõe a investigar as especificidades do tratamento de dados no Ministério Público em comparação com o setor privado, examinando as bases legais previstas na LGPD e seus reflexos na atividade ministerial. O trabalho será desenvolvido em três partes principais: a primeira apresentará uma visão geral da LGPD e seu impacto na regulamentação do tratamento de dados; em seguida, discutir-se-á as características do tratamento de dados no setor privado, analisando suas finalidades e desafios; ao final, buscar-se-á analisar as bases legais aplicáveis ao tratamento de dados no MP, explorando as particularidades e os desafios enfrentados pelo órgão ministerial.

A pesquisa pretende contribuir para o debate sobre a aplicação da LGPD nas atividades do Ministério Público, esclarecendo como as bases legais podem orientar o tratamento de dados e promover uma reflexão crítica sobre os mecanismos de proteção e conformidade adotados pela instituição.

2. A LEI GERAL DE PROTEÇÃO DE DADOS E O TRATAMENTO DE DADOS

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), conhecida como LGPD, estabelece um novo patamar de governança sobre a privacidade no Brasil, marcando um divisor de águas na regulamentação do tratamento de informações pessoais e reforçando a importância da segurança e da transparência no uso de dados. Inspirada em legislações internacionais, notadamente o Regulamento Geral sobre a Proteção de Dados (GDPR[2]) da União Europeia, a LGPD tem como objetivo principal assegurar a privacidade e a proteção de dados, incrementando transparência no tratamento de dados e estabelecendo responsabilidades aos agentes que manipulam tais informações. A legislação visa equilibrar o desenvolvimento econômico com a proteção dos direitos fundamentais de liberdade e privacidade, diante de um contexto de crescimento exponencial do fluxo de informações e das frequentes violações de privacidade que atingem tanto o setor público quanto o privado (MARTINS, 2020, p.18).

À luz dessas considerações, é importante destacar que a LGPD estabelece diretrizes claras para o tratamento de dados pessoais. Especificamente, em seu art. 5º, inciso X, a lei apresenta uma definição abrangente do conceito de

2. União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados - RGPD). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 14 de set de 2024.

tratamento de dados, essencial para a correta compreensão e aplicação das normas. Segundo o citado dispositivo, tratamento de dados é:

> toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018).

Observe-se que a técnica legislativa implementada para conceituar tratamento de dados é notavelmente ampla. A definição legal vigente abrange o tratamento de dados como uma atividade que engloba diversas condutas, todas elas sujeitas às hipóteses legais que condicionam seu exercício regular. Dessa forma, a conformidade do tratamento com as hipóteses estabelecidas em lei é condição indispensável para sua licitude, integrando, assim, a noção jurídica de "tratamento regular". Por outro lado, a violação, desde o início, das hipóteses que autorizam o tratamento de dados caracteriza-o como ilícito ou irregular, sujeitando o responsável às sanções previstas na legislação (Martins, 2024, p. 72).

Nessa linha, o tratamento de dados deve ser realizado com base em alguma das hipóteses legais previstas no art. 7°, destacando-se, entre elas, o consentimento, o cumprimento de obrigação legal, a execução de contrato, a proteção da vida, a tutela da saúde, entre outros. Tratando-se de dados pessoais sensíveis, o tratamento deve observar o art. 11 da Lei que cria uma camada extra de proteção, uma vez que o impacto do seu vazamento é ainda mais grave e a fiscalização é mais rigorosa. Por evidente, essas hipóteses devem ser interpretadas em conformidade com princípios orientadores da norma protetiva dos dados.

Denota-se, assim, que a Lei Geral de Proteção de Dados fundamenta sua estrutura em dois pilares: a) estabelecimento de hipóteses legais pré-definidas, que validam a conformidade legal do tratamento de dados pessoais; e b) a tutela dos direitos do titular dos dados. As hipóteses legais para o tratamento de dados, nesse contexto, são delineadas a partir do reconhecimento da conexão intrínseca entre a proteção dos dados pessoais e os direitos fundamentais de seus titulares.

Registre-se que a técnica adotada pelo legislador brasileiro é muito similar aquela utilizada no art. 6° do Regulamento Geral de Proteção de Dados, estabelecendo hipóteses abrangentes, mas exaustivas, que autorizam o tratamento de dados pessoais.

A lei, portanto, além de conferir aos titulares de dados pessoais uma série de direitos que visam garantir o controle sobre suas informações pessoais, também estabelece diversas obrigações aos controladores e operadores de dados para assegurar que o tratamento de dados pessoais ocorra de maneira legal, justa e transparente.

A implementação de medidas de segurança e a necessidade de controladores e operadores manterem registros das operações de tratamento de dados pessoais, especialmente quando baseadas no legítimo interesse, contribuem para formar um complexo sistema protetivo dos direitos do titular.

3. VISÃO GERAL DO TRATAMENTO DE DADOS NO SETOR PRIVADO E SUAS CARACTERÍSTICAS

O tratamento de dados no setor privado, sob a égide da Lei Geral de Proteção de Dados (LGPD), é delineado por características específicas que refletem as particularidades e os objetivos das empresas.

A finalidade principal desse tratamento geralmente está vinculada a interesses comerciais, que visam gerar valor econômico e proporcionar vantagens competitivas, como a melhoria da experiência do cliente, a personalização de produtos e serviços, além do desenvolvimento de estratégias de marketing direcionadas. A título de exemplo, é fácil pensar que uma plataforma de comércio eletrônico pode coletar dados de navegação e histórico de compras para oferecer recomendações personalizadas. De igual modo, instituições financeiras utilizam dados detalhados de seus clientes para propor soluções de crédito alinhadas ao perfil de cada um.

A coleta desses dados tão importantes para o setor privado ocorre por meio de diversos canais, como formulários em websites, aplicativos móveis, interações em redes sociais, programas de fidelidade, e por meio de tecnologias como cookies e pixels, que monitoram o comportamento dos usuários na internet. A amplitude dos dados coletados pode ser extensa, variando de acordo com o objetivo da empresa. O rol desses dados pode se dar desde informações de contato básicas, como nome e endereço, até dados mais sensíveis, incluindo preferências de consumo, histórico de transações, geolocalização, e até informações de saúde, como ocorre com aplicativos de bem-estar.

Quanto ao armazenamento e processamento dos dados, as empresas podem utilizar servidores próprios ou contratar serviços de computação em nuvem oferecidos por terceiros. Embora a computação em nuvem ofereça vantagens de escalabilidade e flexibilidade, também impõe desafios adicionais relacionados à segurança da informação e à conformidade com a LGPD, especialmente no que tange à transferência internacional de dados. Contudo, a responsabilidade pelo tratamento adequado dos dados permanece com a empresa controladora, que deve garantir a segurança e a integridade das informações, independentemente da infraestrutura utilizada.

A segurança da informação desempenha um papel central no tratamento de dados pelo setor privado. Por esse motivo, a lei exige a adoção de medidas robustas de segurança, como criptografia, que protege os dados

tornando-os ilegíveis para usuários não autorizados; controles de acesso restritos, que garantem que apenas pessoas autorizadas possam manipular as informações; firewalls, que atuam como barreiras entre a rede interna e ameaças externas; backups regulares, que permitem a recuperação de dados em casos de falhas ou ataques; e um monitoramento contínuo para identificar e responder a incidentes de segurança, como tentativas de invasão ou vazamento de dados.

Além disso, a transparência é um princípio fundamental imposto pela LGPD ao setor privado. As empresas devem informar claramente aos titulares dos dados sobre a finalidade da coleta, as formas de utilização, os direitos dos titulares e como eles podem exercer o controle sobre suas informações pessoais, por meio de políticas de privacidade e avisos de uso de cookies. A lei também garante aos titulares o direito de acesso, retificação, portabilidade e, em certas circunstâncias, eliminação de seus dados.

O setor privado também está sujeito à supervisão da ANPD (Agência Nacional de Proteção de Dados) que tem a autoridade de aplicar sanções em casos de violação da lei, incluindo multas que podem alcançar até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, além de outras penalidades como advertências e a suspensão temporária das atividades de tratamento de dados. O cumprimento da LGPD é, portanto, essencial não apenas para evitar sanções, mas também para preservar a confiança dos consumidores e consolidar uma reputação positiva no mercado, evidenciando o compromisso da empresa com a privacidade e a proteção dos dados pessoais.

Em síntese, o tratamento de dados no setor privado é regido por uma série de características interconectadas, que envolvem a finalidade comercial, a necessidade de transparência, a segurança da informação e a observância dos direitos dos titulares. A lei reconhece nessas entidades a finalidade lucrativa. A conformidade com a LGPD é fundamental para que as empresas possam operar de maneira responsável e ética, equilibrando suas necessidades comerciais com a proteção dos direitos fundamentais dos indivíduos.

4. O TRATAMENTO DE DADOS NO MINISTÉRIO PÚBLICO: CARACTERÍSTICAS E DESAFIOS

O Ministério Público Brasileiro é uma instituição com características ímpares no cenário mundial. Por esse motivo, enfrenta uma série de especificidades e desafios no tratamento de dados pessoais, decorrentes de suas funções, complexidade e quantidade de dados que manipula. Essas dificuldades são agravadas diante do fato de que a LGPD pátria teve inspiração Europeia, e naquele continente a concepção de Ministério Público é totalmente diferente da brasileira. Essa diferença, logo de início, já impõe muitas situações que exigem adaptações a realidade específica do Brasil.

A regulamentação geral estabelecida pela LGPD (o art. 23) também aplica-se ao Ministério Público. A estratégia do legislador é criticada por parte da doutrina que afirma que seria um equívoco regulamentar, em um único ato, os setores público e privado. Para eles, a regulamentação do acesso administrativo aos dados estaria inserida dentro do âmbito normativo do direito administrativo de modo que a matéria deveria ser de competência exclusiva de cada ente federativo:

> A Lei 13.709/2018, contudo, disciplina o assunto como se ignorasse esse fato. O Legislador Federal arvora-se no direito de disciplinar o acesso a dados privados para a Administração estadual e municipal sem qualquer constrangimento. (MARTINS, 2020, p. 19-34).

Independentemente das críticas sobre a estratégia adotada pelo legislador, deve-se levar em conta que o tratamento de dados tem peculiaridades que merecem uma atenção especial do intérprete. Basta ponderar que a administração pública não pode simplesmente terceirizar seu serviço ou interromper suas atividades para se adequar à LGPD (Gomes e Zanatta, 2024).

Embora com características específicas, o tratamento de dados realizado pelo Ministério Público não é uma novidade. Alguns doutrinadores asseguram que o tratamento de dados sempre foi uma condição indispensável para o cumprimento de suas missões. O novo fator nessa relação é que graças ao desenvolvimento tecnológico o volume e capacidade de tratamento dos dados tratados é infinitamente maior. Nesse sentido, é natural a discussão sobre o formato desse tratamento, ainda mais considerando a assimetria entre cidadão e Poder Público.

O Ministério Público é instituição que desempenha um papel crucial no regime democrático de direito, sendo um dos principais responsáveis pela defesa dos direitos fundamentais e a promoção da justiça. Independente, tem a responsabilidade constitucional de defender a ordem jurídica, o regime democrático e os interesses sociais e individuais indisponíveis. Tal dever, imposto pela Constituição, constantemente implica o tratamento de dados pessoais em grande volume, sendo a maior parte deles sensíveis.

Apenas para ilustrar, dentre as principais funções exercidas pelo *Parquet* no tratamento de dados*, a* investigação civil e criminal exige a coleta, armazenamento e processamento de informações pessoais que são essenciais para a elucidação de ilícitos e responsabilização de infratores. A proteção dos direitos de determinados grupos vulneráveis é outra função relevante que incrementa a dificuldade no tratamento de dados. É o caso da defesa dos direitos de crianças, idosos e pessoas com deficiência.

É dentro desse contexto que surge a Resolução nº 281/2023 do CNMP (Conselho Nacional do Ministério Público). Importante marco regulamentar da atividade ministerial, a norma estabeleceu uma estrutura interna dedicada

à proteção de dados pessoais, incluindo a Autoridade de Proteção de Dados Pessoais no Ministério Público (APDP/MP) e o Sistema Nacional de Proteção de Dados Pessoais (SINPRODAP/MP), que coordenam e normatizam as atividades de tratamento de dados pessoais dentro da instituição. A medida busca colocar a Instituição como exemplo de aderências às normativas de proteção de dados.

Importante ponderar que o Ministério Público, ao mesmo tempo que deve observar rigorosamente deveres legais que a lei impõe, é responsável pela fiscalização e cumprimento da LGPD por outras entidades. Por esse motivo, deve ser exemplo de comprometimento com as normas mais rigorosas na proteção de dados.

Na busca para atingir essa adequação, muitos desafios são impostos. O primeiro obstáculo a ser enfrentado é a conciliação entre sigilo e transparência. É preciso equilibrar a necessidade de manter o sigilo das investigações com a exigência da LGPD de dar transparência à forma como os dados são tratados, assegurando que o acesso a informações sensíveis seja devidamente controlado. Além disso, o tratamento de dados sensíveis, como informações de saúde, requer cuidados adicionais para evitar discriminação e garantir a proteção adequada desses dados. Outro desafio constante é a capacitação dos membros e servidores do Ministério Público, de modo que compreendam a importância da proteção de dados e estejam preparados para cumprir a legislação.

A infraestrutura tecnológica também se mostra um grande obstáculo, pois manter sistemas de informação atualizados e seguros para prevenir vazamentos e acessos não autorizados é uma prioridade. Entretanto, essa tarefa representa um desafio técnico e orçamentário na realidade do Ministério Público. Ademais, a interpretação e aplicação da LGPD pelo *Parquet* precisa ser realizada em consonância com outras legislações específicas que regem sua atuação, o que pode gerar dúvidas e exigir uma harmonização normativa. Nesse sentido, a Resolução nº 281 do CNMP ganha grande importância, pois trata detalhadamente de diversos aspectos relacionados à atividade do Ministério Público.

Para enfrentar esses desafios, é essencial adotar medidas de segurança e governança. A Resolução nº 281 destaca a importância da implementação de políticas robustas de segurança da informação como forma de melhor preservar os dados tratados pela instituição.

Diante das especificidades e dos desafios enfrentados pelo Ministério Público no tratamento de dados pessoais, fica evidente a necessidade de um constante aperfeiçoamento das práticas adotadas pela instituição, o que demanda uma abordagem sistemática e uma rigorosa observância das normas legais. A conciliação entre sigilo e transparência, o cuidado no tratamento de dados sensíveis, a capacitação dos membros e servidores, a atualização tecnológica e a interpretação adequada da LGPD são elementos essenciais para o cumprimento desse objetivo.

Nesse cenário, a Resolução nº 281/2023 do CNMP revela-se como um marco crucial, ao estabelecer diretrizes claras para o cumprimento da LGPD no âmbito do Ministério Público, reafirmando o papel da instituição como agente promotor da proteção de dados. A efetividade dessas diretrizes, no entanto, depende do devido enquadramento das atividades do órgão ministerial nas bases legais do tratamento de dados previstas pela LGPD. É sobre essas bases legais e sua aplicação no âmbito do Ministério Público que se debruçará o próximo capítulo, analisando como cada uma delas orienta e sustenta as atividades do *Parquet* em consonância com a legislação vigente.

5. BASES LEGAIS DO TRATAMENTO DE DADOS NO MINISTÉRIO PÚBLICO

O tratamento de dados pelo Ministério Público, assim como no setor privado, deve estar fundamentado em uma das hipóteses legais previstas na Lei Geral de Proteção de Dados. No entanto, há peculiaridades em sua aplicação no âmbito público, especialmente em razão das funções constitucionais desempenhadas pelo *Parquet*, que vão além do simples cumprimento de obrigações contratuais ou do consentimento dos titulares dos dados. O MP é responsável pela defesa dos direitos fundamentais e pela fiscalização da ordem jurídica, e tais atribuições exigem uma análise criteriosa das bases legais aplicáveis ao tratamento de dados pessoais.

Uma das medidas primordiais a serem adotadas antes do início do tratamento de dados é a identificação da base legal aplicável. No entanto, e aqui surge a primeira diferença, o tratamento de dados pelo Ministério Público, além de estar amparado nas hipóteses dos art. 7º e 11 da LGPD, deve também seguir os critérios adicionais estabelecidos no art. 23. Esses critérios complementam e orientam a interpretação e a aplicação prática das bases legais no contexto das atividades do Poder Público o que, em síntese, estabelece que o tratamento de dados pessoais por órgãos públicos deve ter uma finalidade pública e atender aos princípios da administração pública.[3]

Nesse contexto, o artigo 7º da LGPD estabelece dez bases legais para o tratamento de dados pessoais, sendo suficiente que o tratamento esteja amparado em ao menos uma dessas hipóteses para ser considerado legítimo. Caso o tratamento de dados pessoais se enquadre em mais de uma base legal simultaneamente, é recomendável que se escolha a base mais segura e

3. Agência Nacional de Proteção de Dados (Brasil). Guia orientativo para o tratamento de dados pessoais pelo poder público. Versão final. Brasília, DF: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 31 ago. 2024.

apropriada ao contexto específico, de modo a garantir a conformidade legal e a minimização de riscos.[4]

Aprofundando o estudo sobre as bases legais de tratamento de dados, a seguir serão detalhadas as hipóteses autorizadoras previstas no artigo 7º da LGPD.

a) Consentimento do titular (art. 7º, I):

O consentimento é um negócio jurídico que deve respeitar as formalidades estabelecidas no Código Civil para tal ato. Além disso, para que o consentimento seja válido e em conformidade com a LGPD e a Resolução nº 281/2023 do CNMP, ele deve ser livre, informado e inequívoco, dado para uma finalidade específica, e expresso por uma manifestação clara do titular. O controlador deve documentar o consentimento e garantir que o titular possa revogá-lo facilmente a qualquer momento. Em situações que envolvam dados sensíveis ou a transferência internacional de dados, o consentimento deve ser ainda mais explícito.

Apesar da louvável iniciativa da LGPD de tentar uniformizar a proteção de dados pessoais, é crucial reconhecer que a relação entre o poder público e o cidadão é muito diferente da relação entre o setor privado e os indivíduos. O poder público trata os dados, na maioria das situações, como decorrência dos seus deveres constitucionais e legais. Consequentemente, tais circunstâncias não podem depender do consentimento dos seus titulares.

Exatamente em razão dessa assimetria das relações entre poder público e administrado, é que muitos doutrinadores criticam a utilização do consentimento como base legal para o tratamento. É fácil imaginar a situação de um cidadão sentir-se inseguro quanto à possibilidade de negar o consentimento e como consequência ter o serviço não prestado pelo poder público. É exatamente por causa desse receio, que se justifica essa base legal ter aplicação limitada na esfera pública.

Por outro lado, a existência de outras bases legais distintas do consentimento para o poder público é igualmente necessária para evitar o abuso de direito por parte do titular (exercício indevido de uma posição jurídica), o que poderia inviabilizar as atividades públicas. Apenas a título de exemplo, imagine-se a situação em que o Ministério Público necessitasse do consentimento para tratar dados pessoais dentro de uma investigação criminal, o que teria por consequência a frustração de toda a função de persecução penal da instituição.

Nessa linha, a Resolução nº 281/2023 do CNMP (art. 16) reforça que o Ministério Público possui a prerrogativa de realizar o tratamento de dados

4. "(...) Entende-se que, ainda que seja possível utilizar mais de uma base legal para determinado tratamento de dados, é preciso buscar a base mais adequada e segura para a situação concreta". (Doneda, Danilo (*et al*.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.133).

pessoais sem a necessidade de consentimento dos titulares, quando se trata de defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis. Essa competência inclui o acesso direto a bancos de dados de caráter público e a possibilidade de requisitar informações a instituições privadas, assegurando que tais atividades estejam em conformidade com os princípios e diretrizes estabelecidos na LGPD e nas normas internas da Instituição.

b) Cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II):

Possibilidade também prevista no caso de dados sensíveis (art. 11, inciso II, "a" LGPD), essa segunda hipótese está relacionada ao dever imposto ao controlador. Neste caso, é a própria lei que obriga o tratamento dos dados, ou é o tratamento um meio pelo qual se dará atendimento ao dever legal. Este conceito engloba não só a lei em sentido estrito, como outros tipos de atos normativos (normas regulatórias e regulamentos em geral).

Essa hipótese é especialmente aplicável ao Ministério Público, pois muitas de suas atividades-fim, como a investigação criminal e a fiscalização do cumprimento das leis, são realizadas para cumprir obrigações legais. Em diversas ocasiões, essas atividades exigem a formação de um cadastro pessoal, reforçando a impossibilidade de depender do consentimento do titular.

É imperativo lembrar que o poder do Ministério Público de tratar dados se valendo de exigências legais e regulatórias deve ser exercido de maneira proporcional aos direitos dos titulares e estar sujeito ao crivo da análise de constitucionalidade da norma que impõe tal exigência. Na ausência de observância desses requisitos, ou havendo uma origem irregular no tratamento, pode-se cogitar em desvio ou abuso do poder.[5]

Finalmente, uma vez que a lei determina o tratamento, não cabe ao membro do *Parquet* discricionariedade quanto ao cumprimento ou não desse dever. Ao agente responsável pelo tratamento de dados, não se confere a opção de recusar o tratamento, pois a norma cogente impõe essa obrigação, enquanto a LGPD autoriza o tratamento, completando o ciclo jurídico.

c) Execução de políticas públicas previstas em leis ou regulamentos (art. 7º, III):

O Ministério Público, em sua função de fiscal da lei e defensor dos interesses sociais, possui a competência para tratar dados pessoais para a execução de políticas públicas, especialmente aquelas direcionadas à proteção de direitos fundamentais, como a proteção de crianças, idosos e outros grupos vulneráveis.

5. STF, RE 1.055.941/SP, Rel. Min. Dias Toffoli, j. 28/11/2019, DJe 11/12/2019.

A hipótese de tratamento prevista no inciso III está intrinsecamente relacionada aos outros dois requisitos mencionados no art. 23 da mesma lei, que são, "atendimento de sua finalidade pública, na persecução do interesse público" e "com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público" (ROSSO, 2024).

A redação do inciso utiliza-se de expressões amplas, cujo significado não é precisamente definido. "Políticas Públicas", por exemplo, "é uma espécie de curinga para designar tudo aquilo que se supõe ser bom, belo e justo"(MARCACINI, 2020, p. 149). O direito à privacidade e à intimidade, em grande parte, existe justamente para restringir os poderes do Estado, de forma que nunca é demais recordar que o extermínio de judeus, por exemplo, foi uma política pública implementada pela Alemanha nazista. A amplitude do conceito também abrange a formalidade do ato, já que a parte final da redação fala em "instrumentos congêneres", dando grande amplitude de atos autorizativos que poderiam "criar" uma política pública que autorizaria o tratamento dos dados.

Diante desses aspectos, o Ministério Público, ao se utilizar dessa hipótese para realizar o tratamento de dados, deve agir com cautela, escolhendo com rigor o tipo de política pública a ser aplicada, priorizando aquelas que estejam previstas em atos normativos formais, como a Constituição ou leis federais.

Pensando no exemplo em que o tratamento de dados é realizado como condição para a execução e monitoramento dos serviços públicos de saúde, observa-se que, mesmo quando o tratamento de dados é fundamentado pelo interesse público, ele deve se subordinar ao princípio da proporcionalidade. Esse princípio visa garantir que o tratamento seja conduzido da maneira menos invasiva possível, minimizando os riscos ao titular dos dados (MARTINS, 2024, p. 81).

Conclui-se, portanto, que a utilização dessa base legal pelo Ministério Público deve ser cuidadosamente ponderada, priorizando a segurança jurídica e a proteção dos direitos fundamentais dos indivíduos, a fim de assegurar que o tratamento de dados esteja em estrita conformidade com os princípios da LGPD e com as atribuições legais da instituição.

d) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7°, IV):

Embora essa hipótese seja mais diretamente aplicável a atividades de pesquisa, não são incomuns os casos em que o Ministério Público utiliza os resultados dessas pesquisas para fundamentar suas posições ou para conduzir e monitorar políticas públicas sob sua responsabilidade.

A legislação exige que essa atividade seja exercida com cautela, especialmente no que diz respeito à necessidade de anonimização das informações pesquisadas. Por anonimização, entende-se a técnica que utiliza

meios "razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"[6]. Vale destacar que a expressão "sempre que possível" deve ser interpretada com a devida consideração ao fato de que a anonimização não será obrigatória se prejudicar o processo ou o resultado almejado com a pesquisa. Isso remete, essencialmente, ao princípio da necessidade.

e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art. 7°, V):

A hipótese prevista no inciso V do art. 7° é raramente utilizada no âmbito da atividade-fim do Ministério Público. Esse dispositivo legal, que autoriza o tratamento de dados pessoais "para a execução de contratos ou procedimentos preliminares relacionados a contrato do qual seja parte o titular", encontra aplicação mais relevante nas atividades-meio da instituição. É pertinente destacar, no entanto, que o Ministério Público pode recorrer a essa hipótese sempre que estiver celebrando contratos com particulares, sejam eles pessoas físicas ou jurídicas.

Nesse contexto, o tratamento de dados pessoais é autorizado quando necessário para o cumprimento das obrigações contratuais ou para a condução de procedimentos preliminares à formalização de um contrato. Portanto, a utilização do inciso V pelo Ministério Público deve observar rigorosamente a finalidade contratual e a necessidade do tratamento de dados, garantindo que a coleta e o uso das informações pessoais estejam estritamente vinculados à execução do contrato em questão.

f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n° 9.307/96 (art. 7°, VI):

O Ministério Público, em sua atuação, frequentemente necessita tratar dados pessoais para assegurar o exercício regular de seus direitos e deveres institucionais em processos judiciais e administrativos. Basta pensar no exemplo de uma investigação criminal em que o Ministério Público pode precisar coletar e analisar dados pessoais para fundamentar uma denúncia ou para defender os interesses de vítimas em processos cíveis. Da mesma forma, no âmbito de processos administrativos, o *Parquet* pode tratar dados pessoais ao fiscalizar o cumprimento de leis, como as que garantem a proteção de consumidores ou o respeito ao meio ambiente.

O inciso VI oferece uma base legal robusta que permite ao Ministério Público realizar o tratamento de dados e mais uma vez dispensa a necessidade de consentimento do titular. Tal tratamento, no entanto, deve ser necessário e proporcional para o exercício de direitos no contexto de um processo judicial, administrativo ou arbitral. Isso inclui a coleta de provas, a gestão de

6. Art. 5°, inciso XI, da Lei 13.709/2018.

informações relevantes para a defesa de direitos, e a atuação em nome do interesse público ou coletivo, sejam eles trazidos ou não para os autos da ação judicial.

Evidentemente, o tratamento de dados amparado nessa hipótese deve sempre se pautar pelos princípios gerais da LGPD, como a necessidade, a minimização e a adequação, garantindo que os dados pessoais tratados sejam estritamente necessários para o objetivo processual. Ao se basear no inciso VI, o Ministério Público atua com respaldo jurídico claro, podendo, assim, desempenhar suas funções de forma eficaz e conforme as diretrizes legais de proteção de dados pessoais.

g) Proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7°, VII):

Esta hipótese é aplicável em situações em que o Ministério Público precisa tratar dados pessoais para proteger a vida ou a integridade física de pessoas, como em ações voltadas à proteção de vítimas de violência ou de crimes. Trata-se de uma hipótese que contempla casos em que a urgência do contexto torna inviável a obtenção do consentimento do titular.

No entanto, sua utilização deve ser considerada subsidiária, uma vez que a hipótese prevista no inciso II (cumprimento de obrigação legal) já impõe ao Ministério Público o dever de tratar os dados no exercício de suas atividades constitucionalmente estabelecidas, que incluem a proteção da vida e da integridade física dos indivíduos. O inciso VII deve ser invocado apenas em situações onde a aplicação do inciso II não seja suficiente ou onde o caráter emergencial do tratamento requeira uma base legal específica.

h) Tutela da saúde, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7°, VIII):

A previsão contida no inciso VIII é predominantemente direcionada ao setor de saúde. No âmbito do Ministério Público, pode encontrar aplicação em contextos de ações relacionadas à proteção da saúde pública, como em investigações envolvendo surtos ou epidemias. Contudo, mesmo nesses casos, os incisos anteriormente analisados já autorizam o tratamento de dados, o que torna o uso dessa hipótese relativamente raro no contexto das atividades ministeriais.

i) Atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7°, IX):

O interesse legítimo pode ser invocado pelo Ministério Público em situações nas quais o tratamento de dados seja necessário para o desempenho de suas funções institucionais. Todavia, o seu conceito demasiadamente amplo dá margem as mesmas críticas que analisamos no estudo do art. 7°, inciso III, da LGPD (políticas públicas).

A interpretação sistemática e baseada em princípios da LGPD sugere que a aplicação desse inciso pelo Poder Público seja excepcional. Tal circunstância impõe à autoridade pública um elevado ônus de fundamentação, bem como a necessidade de cumprir rigorosamente todas as salvaguardas procedimentais. Em nenhuma circunstância é permitido às autoridades públicas realizar o tratamento de dados simplesmente em virtude de sua posição funcional, nem recorrer a invocações genéricas de interesse público como justificativa para o tratamento de dados pessoais (Frazão, 2022, p. 220).

j) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, IX):

O último inciso do art. 7º encontra aplicação mais relevante nas atividades dos particulares, sendo praticamente irrelevante para as atividades ministeriais.

A análise de todos os incisos do art. 7º demonstra que o tratamento de dados pessoais, mesmo diante da complexidade das atribuições do Ministério Público, deve ser cuidadosamente fundamentado em uma base legal adequada e sempre pautado pelos princípios da LGPD, tais como pelas disposições da Resolução nº 281/2023 do CNMP. Os incisos do art. 7º da legislação não apenas fornecem legitimidade ao tratamento de dados, mas também garantem que os direitos fundamentais dos titulares de dados sejam preservados, mesmo quando o tratamento é realizado por uma instituição pública, com o papel de fiscalizar e promover a justiça. A correta aplicação das bases legais permite que o Ministério Público exerça suas funções de maneira eficaz e em conformidade com a legislação vigente, equilibrando suas responsabilidades institucionais com a proteção dos direitos individuais.

6. CONCLUSÃO

A Lei Geral de Proteção de Dados (LGPD) trouxe uma mudança significativa na forma como o tratamento de dados pessoais é conduzido no Brasil, se consolidando como um marco normativo fundamental tanto para o setor privado quanto para o poder público. A análise realizada neste artigo evidencia que, por ter sido inspirada em legislações internacionais, a LGPD precisou ser adaptada à realidade brasileira, enfrentando desafios inerentes à estrutura das instituições nacionais, em especial o Ministério Público.

No setor privado, a LGPD estabelece diretrizes claras para o tratamento de dados, destacando a importância da finalidade comercial, da transparência e da segurança da informação. As empresas, impulsionadas por interesses econômicos, encontram na conformidade com a LGPD não apenas um imperativo legal, mas também um meio de construir confiança com seus consumidores e consolidar uma reputação de responsabilidade no mercado.

O cenário se torna mais complexo quando o tratamento de dados é analisado no âmbito do Ministério Público, pois, possui funções constitucionais que vão além do simples cumprimento de obrigações contratuais ou da obtenção do consentimento dos titulares dos dados. A complexidade do tratamento de dados pelo *Parquet* reside em suas atribuições de fiscal da ordem jurídica, defensor dos direitos fundamentais e promotor da justiça. Nesse contexto, a Resolução nº 281/2023, do CNMP, surge como um marco regulamentar crucial, exigindo e direcionando o Ministério Público a estabelecer mecanismos internos de proteção de dados e a se adequar às exigências da LGPD.

A análise das bases legais para o tratamento de dados no Ministério Público revela que o consentimento é, em geral, uma base pouco utilizada devido à assimetria das relações entre o poder público e o cidadão. As hipóteses de tratamento mais relevantes para o *Parquet* residem no cumprimento de obrigações legais, na execução de políticas públicas e no exercício regular de direitos em processos judiciais, administrativos ou arbitrais. Essas bases legais conferem legitimidade ao tratamento de dados, mas sua aplicação também demanda uma atenção cuidadosa e em consonância com os princípios da LGPD, como necessidade, proporcionalidade e adequação.

O tratamento de dados no Ministério Público, embora regido pelos mesmos princípios fundamentais da LGPD aplicáveis ao setor privado, requer uma abordagem específica e criteriosa. A submissão da atividade ministerial ao regramento contido na LGPD deve ser vista não apenas como uma obrigação legal, mas também como uma expressão de seu compromisso com a proteção dos direitos individuais e com a promoção da justiça. A Resolução nº 281/2023 do CNMP, ao fornecer diretrizes para a atuação do Ministério Público, reafirma seu papel como agente de proteção de dados e, ao mesmo tempo, evidencia os desafios e responsabilidades que lhe são inerentes.

Reforça-se a importância de uma contínua reflexão e aprimoramento das práticas de tratamento de dados no âmbito do Ministério Público. Ao observar rigorosamente as bases legais e princípios estabelecidos pela LGPD, o *Parquet* pode equilibrar sua atuação institucional com a garantia dos direitos fundamentais dos titulares de dados pessoais, cumprindo sua missão constitucional de forma eficaz e conforme a legislação vigente.

7. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Brasil. Agência Nacional de Proteção de Dados. *Guia orientativo para o tratamento de dados pessoais pelo poder público*. Versão final. Brasília, DF: ANPD, 2023.Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf.

Brasil. Supremo Tribunal Federal. RE 1.055.941/SP, Rel. Min. Dias Toffoli, j. 28/11/2019, DJe 11/12/2019.

Brasil. [Constituição (1998)]. *Constituição da República Federativa do Brasil: promulgada em 05 de outubro de 1998*. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Brasil. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, 15 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Brasil. Conselho Nacional do Ministério Público. Resolução CNMP nº 281, de 9 de julho de 2019. Dispõe sobre a proteção de dados pessoais no âmbito do Ministério Público. *Diário Oficial da União*: Seção 1, Brasília, DF, 11 jul. 2019. Disponível em: https://www.cnmp.mp.br.

Doneda, Danilo; *et al*. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

Frazão, Ana; **Carvalho**, Angelo Prata de; **Milanez**, Giovanna. *Curso de proteção de dados pessoais: fundamentos da LGPD*. 1. ed. Rio de Janeiro: Forense, 2022.

Gomes, Rodrigo Dias de Pinho; **Zanatta**, Rafael A. F. *Notas sobre o encarregado de dados no setor público*. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/348961/notas-sobre-o-encarregado-de-dados-no-setor-publico.

Marcacini, Augusto Tavares Rosa. Regras aplicadas ao tratamento de dados pessoais. In: LIMA, Cíntia Rosa Pereira de (Coord.). *Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019*. São Paulo: Almedina, 2020.

Martins, Guilherme Magalhães; **Longhi**, João Victor Rozatti; **Faleiros Júnior**, José Luiz de Moura (Coord.). *Comentários à Lei Geral de Proteção de Dados Pessoais*. 2. ed. Indaiatuba, SP: Editora Foco, 2024.

Martins, Ricardo Marcondes. Lei Geral de Proteção de Dados Pessoais e direito administrativo: questões polêmicas. In: Dal Pozzo, Augusto Neves; Martins, Ricardo Marcondes (Org.). *LGPD & administração pública: uma análise ampla dos impactos*. São Paulo: Revista dos Tribunais, 2020.

União Europeia. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados - RGPD). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679.

Rosso, Angela Maria. *LGPD e setor público: aspectos gerais e desafios*. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios.

O REGISTRO DE OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS (ROPA) NA ATIVIDADE-FIM DO MINISTÉRIO PÚBLICO BRASILEIRO

Lauro Francisco da Silva Freitas Júnior[1]
Leonardo Andrade Macedo[2]

Resumo: O trabalho aborda o tema do registro de operações de tratamento de dados pessoais (RoPA) no âmbito da atividade-fim do Ministério Público brasileiro. Inicialmente, são expostas as finalidades institucionais do órgão e descrito, de forma geral, como se dá o tratamento de dados pessoais na sua atividade finalística. Em seguida, explica-se o que é o inventário de dados pessoais, seu fundamento, finalidades e benefícios, conforme a LGPD, e discute-se sua aplicação na atividade-fim do Ministério Público, segundo a Resolução CNMP 281/2023. Ao final, são apresentadas diretrizes para elaboração do RoPA em relação às operações de tratamento de dados pessoais na atividade-fim do Ministério Público.

Palavras-chaves: Ministério Público brasileiro. Proteção de dados pessoais. Lei Geral de Proteção de Dados (LGPD). Inventário de dados. Registro de operações de tratamento de dados pessoais (RoPA).

Resumen: El trabajo aborda el tema del registro de actividades de procesamiento de datos personales (RoPA) en el ámbito de la actividad principal del Ministerio Público brasileño. Inicialmente se explican las finalidades institucionales del Ministerio Público y hay una descripción general de cómo se tratan los datos personales en su actividad final. A continuación, se explica qué es el inventario de datos personales, su fundamento, finalidades y beneficios, según la Ley General de Proteccion de Datos de Brasil (LGPD), y se analiza su aplicación en la actividad principal del Ministerio Público, según la Resolución CNMP 281/2023. Al final se presentan lineamientos para la elaboración del RoPA en relación con las operaciones de tratamiento de datos personales en la actividad principal del Ministerio Público.

---

1. Promotor de Justiça do Ministério Público do Estado do Pará. Mestre em Direito pela Universidade da Amazônia e Doutor em Psicologia pela Universidade Federal do Pará.

2. Procurador da República. Mestre em Direito pela Universidade Federal de Minas Gerais.

Palabras clave: Ministério Público de Brasil. Protección de datos personales. Ley General de Protección de Datos de Brasil (LGPD). Inventario de datos. Registros de actividades de procesamiento de datos personales (RoPA).

Sumário: 1. Introdução: as finalidades institucionais do Ministério Público brasileiro. 2. O tratamento de dados pessoais na atividade-fim do Ministério Público. 3. O registro de operações de tratamento de dados pessoais. 4. A Resolução CNMP 281/2023 e sua aplicação à atividade-fim do Ministério Público. 5. Diretrizes para o registro de operações de tratamento de dados pessoais na atividade-fim do Ministério Público. 6. Conclusão. 7. Referências bibliográficas e documentação.

1. INTRODUÇÃO: AS FINALIDADES INSTITUCIONAIS DO MINISTÉRIO PÚBLICO BRASILEIRO

A Constituição Federal de 1988 do Brasil reverenciou o reconhecimento amplo e irrestrito de garantias e direitos fundamentais. A Constituição Cidadã foi extensa e abrangeu direitos individuais e coletivos, elencados ao longo de seu corpo.

Na mesma esteira, além de reconhecer direitos e garantias, o Constituinte percebeu a necessidade da implantação de mecanismos e instrumentos, bem como de órgãos que, de forma estruturada e independente, pudessem tornar realidade os princípios insertos na Constituição. Foi nesse cenário, respeitando os marcos norteadores da Carta de Curitiba[3], que surgiu o Ministério Público que conhecemos.

O Ministério Público, consoante o art. 127, *caput,* da Constituição Federal, é instituição permanente, essencial à função jurisdicional do Estado incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis. A finalidade da existência do Ministério Público, diz o próprio texto constitucional, é a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, isto é, a função de defesa da sociedade no regime democrático, instituída pela Carta de 1988.[4]

Merece destaque que a expressão permanente, acrescida da condição essencial, ou seja, indispensável à própria função jurisdicional do Estado, gera

3. Por ocasião dos trabalhos preparatórios à Constituição de 1988, o Ministério Público, representado por seus diversos segmentos, elaborou uma carta-proposta referente à disciplina da Instituição o que refletiria seus principais anseios. A proposta foi aprovada em 1986, na ocasião do 1.º Encontro Nacional de Procuradores Gerais de Justiça e Presidentes de Associações, realizado na capital do Estado do Paraná, no período de 20 a 22 de junho, tendo recebido a denominação de Carta de Curitiba.

4. JATAHY, Carlos Roberto de Castro. Curso de Princípios Institucionais do Ministério Público. 2. ed. Rio de Janeiro: Roma Victor, 2006. p. 31.

impedimento ao próprio Poder de Reforma da Constituição, caso existisse o interesse de retirar o Ministério Público do arcabouço constitucional.

Desta forma, partindo-se da própria natureza da atividade desenvolvida do Ministério Público, voltada ao bem-estar da sociedade, protegendo-a contra terceiros e, em especial, contra o Estado, a sua existência deve ser considerada incluída no rol dos direitos e garantias individuais, sendo vedada a apresentação de qualquer proposta de Emenda tendente a aboli-la (art. 61, §4.°, V da CF-88). Assim, devemos considerar o Ministério Público como cláusula pétrea.[5]

Nesse sentido leciona Emerson Garcia:

> Por ser inócua a previsão de direitos sem a correspondente disponibilidade 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 isto, inviabilizando a sua atuação, que é elemento indicativo de sua própria existência).[6]

Por outro lado, a Constituição Federal também dispôs que o Ministério Público é instituição essencial à função jurisdicional do Estado. Desta forma, unindo o substantivo instituição com o adjetivo essencial, conclui-se que somente o Ministério Público pode desempenhar atividades outorgadas pelo legislador constitucional e infraconstitucional, imprescindíveis para a consecução final da justiça.[7]

A essencialidade, na prática, também pode ser visualizada quando, em determinada relação processual, a intervenção do Ministério Público for imprescindível.[8]

Portanto, dentro da nova arquitetura da Constituição Brasileira, específica e própria do Estado Democrático do Direito, o Ministério Público foi erigido

---

5. Cf. Ministro Carlos Ayres Brito, em palestra proferida da sede do Ministério Público Fluminense em 04.06.2004, citada por Carlos Roberto C. Jatahy, 2006, *op. cit*., p. 32.

6. Garcia, Emerson. Ministério Público, Organização, Atribuições e Regime Jurídico. 2. ed. Rio de Janeiro: Lumen Juris, 2005. p. 48.

7. *Ibid*, p. 48.

8. Cabe frisar a decisão do STF (agravo de instrumento 172.244/RS, Rel. Min. Celso de Melo, DJ. 13.11.1995, p. 38611), onde ficou determinado que ato processual (audiência) em que membro do Ministério Público tenha sido previamente intimado pode ocorrer com sua ausência, vez que esta falta não pode ser imputada ao aparelho judiciário.

à condição de Instituição permanente e independente a qualquer Poder do Estado. Dessa forma, o Ministério Público Brasileiro ganhou feição peculiar e sem similitude no mundo, com atribuições específicas para uma sociedade carente de democracia e de justiça social, como é a brasileira.[9]

Agora, diante deste panorama, é importante traçar um posicionamento do Ministério Público na Constituição brasileira, em especial, perante a teoria da separação de poderes. Para isso, se faz necessário uma pequena digressão a essa teoria.

A princípio, é correto afirmar que o poder representa um inconteste fenômeno social que, em último grau, se exterioriza pelos elementos concretos da força, em suas várias acepções: econômica, militar e política. Em termos mais amplos dentro da teoria estatal, no entanto, o poder, em sua noção teórica, traduz o veículo instrumental pelo qual se alcança uma ordem social que, representando uma ideia conceitual de direito, tem como finalidade o bem comum.[10]

A teoria da "separação de poderes" pressupõe a tripartição das funções do Estado, distinguindo-as em legislativa, administrativa (ou executiva) e jurisdicional.

Aristóteles, já na antiguidade, em sua *Política,* lançou aquela que seria a base de uma teoria acerca da separação das funções do Estado. Na concepção aristotélica o governo dividia-se em três partes: a que deliberava acerca dos negócios públicos; a que exercia a magistratura (uma espécie de função executiva) e a que administrava a Justiça.

John Locke (*Ensayo sobre el gobierno civil)* e Rosseau (*Du contrat social*) também contribuíram para a construção da "separação de poderes", tendo a mesma sido realmente definida e divulgada por Montesquieu em seu *De l'esprit des lois*, transformando-se, assim, numa das mais importantes doutrinas políticas de todos os tempos, alçada à categoria de princípio fundamental da organização política liberal.

A primeira Constituição escrita que adotou na íntegra a doutrina de Montesquieu foi a da Virgínia, em 1776, seguida pelas Constituições de Massachussetts, Maryland, New Hampshire e pela própria Constituição Federal Americana de 1787. Nessa época, os constitucionalistas norte-americanos afirmaram, de modo categórico, que a concentração dos três poderes num só órgão de governo representava a verdadeira definição de tirania.[11] Assim, o

9. Ritt, Eduardo, O Ministério Público como Instrumento de Democracia e Garantia Constitucional. Porto Alegre: Livraria do Advogado, 2002, p. 137.

10. De um modo amplo, busca-se associar a expressão bem comum à ideia de justiça (como valor axiológico), forjando a concepção segundo a qual o bem comum seria a medida da justiça ou a própria finalidade da mesma, em uma acepção ampla de direito.

11. Caetano, Marcello. Manual de Ciência Política e Direito Constitucional. Coimbra: Almedina, 1996. Tomo I. p. 191.

princípio de Montesquieu, ratificado e adaptado por Hamilton, Madison e May, foi a base da doutrina exposta no Federalista, de contenção do poder pelo poder, que os norte-americanos chamaram de sistema de freios e contrapesos (*checks and balances*).

Da mesma forma, a Revolução Francesa proclamou o princípio nos seguintes termos: "Toda sociedade na qual a garantia dos direitos não estiver assegurada nem determinada a separação de poderes, não tem Constituição" (Declaração dos Direitos do Homem, art. 16).

Não obstante ter o princípio da "separação de poderes" sido uma constante no ordenamento constitucional brasileiro segundo a fórmula preconizada por Montesquieu, a Constituição do Império, excepcionalmente, adotou a separação quatripartita: poderes Moderador, Legislativo, Executivo e Judiciário.

O princípio da separação e independência de poderes, malgrado constituir um dos signos distintivos fundamentais do Estado de Direito, não possui fórmula universal apriorística. Tão importante quanto essa divisão funcional básica é o equilíbrio entre os poderes, mediante um jogo recíproco dos freios e contrapesos.

Por outro lado, nos dias de hoje, não só o princípio da separação de poderes, como a própria tripartição de poderes, ou seja, a forma das funções do Estado é algo anacrônico, de mera constituição ideológica, não científica[12]. Assim, deve a separação de poderes, ser vista de forma relativizada, mitigada.

Dalmo de Abreu Dallari escreveu sobre o tema:

> A primeira crítica feita ao sistema de separação de poderes é no sentido de que ele é meramente formalista, jamais tendo sido praticado. A análise do comportamento dos órgãos do Estado, mesmo onde a Constituição consagra efetivamente a separação de poderes, demonstra que sempre houve uma intensa interpenetração. Ou o órgão de dos poderes pratica atos que, a rigor seriam do outro, ou se verifica a influência de fatores extralegais, fazendo que algum dos poderes predomine sobre os demais, guardando-se apenas a aparência de separação. [13]

Desta forma, uma divisão de funções e não uma separação de poderes rígida é, todavia, importante para possibilitar a eficiência do Estado e a independência de seus órgãos.

Diante de tudo que foi exposto, o Ministério Público não poderia ser um Poder de Estado, mas a realidade atual é outra. Um dos pilares da teoria da separação de poderes foi a forma de contenção do poder pelo poder.

---

12. Nesse sentido Ritt, *op. cit.*, p. 142-143.

13. Dallari, Dalmo de A. Elementos da Teoria Geral do Estado. 25. ed. São Paulo: Saraiva, 2005. p. 221.

Nos dias de hoje, o Ministério Público, em decorrência das atribuições que a própria Carta Magna lhe conferiu, é um exímio órgão de contenção de arbítrios do Estado.

O Ministério Público propicia o acesso à justiça, "zela pelo efetivo respeito dos poderes públicos e dos serviços de relevância pública aos direitos assegurados nesta Constituição, promovendo as medidas necessárias a sua garantia", consoante determina art. 129, II da CF-88. E ainda mais, o *Parquet* fiscaliza os demais órgãos públicos e o próprio Poder Executivo.

Assim sendo, considerando a realidade e a ideologia da separação de poderes, a discussão acerca de o Ministério Público ser considerado um "Quarto Poder" é válida.[14] Não se trata de "frívola vaidade", como ressalta Emerson Garcia[15], entender o Ministério Público como Poder Estatal. O reconhecimento do Ministério Público como Poder, ao menos no campo ideológico, é o primeiro passo para uma verdadeira independência deste grande órgão em benefício do cumprimento de suas missões constitucionais.

A Constituição brasileira de 1988 teve como fundamento o Estado de Direito e este, por sua vez, está estritamente relacionado à ideia de democracia. Assim, o Estado defendido pela Carta Maior é aquele que exerce seus poderes nos limites postos pelo direito e em harmonia com parâmetros traçados por estes, sempre com direitos e garantias respeitados, no tocante aos indivíduos.

O art. 127, *caput*, da Constituição Federal confere ao Ministério Público, dentre outros fins, a defesa da ordem jurídica[16] e do regime democrático.

Assim, o novo perfil do Ministério Público pressupõe a aferição e fiscalização de todos os atos praticados pelos órgãos do Estado, podendo ajuizar as medidas necessárias ao combate de abusos ou ilegalidades, sempre com o intuito de manter o Estado no limite da Constituição e do direito. Logo, também é de se concluir que ao Ministério Público compete também a defesa da ordem constitucional, onde quer que esta se encontre ameaçada.[17]

---

14. RITT, *op. cit*., p. 145.

15. *Ibid*., p. 45.

16. Nesse sentido a ordem jurídica não guarda similitude com a Lei, mas sim, com o direito, sendo noção eminentemente mais ampla.

17. Nessa linha, asseverou Eduardo Ritt, *op. cit*., p. 157: A atuação do Ministério Público brasileiro, portanto, é orientada para a supremacia constitucional e para o ordenamento jurídico como um todo não seja agredido, ou por abusos de poder e por atos ilícitos de autoridades públicas (inclusive por atos de improbidade administrativa), ou por atos ilícitos do próprio cidadão. Para tanto, utiliza-se da ação penal, da ação civil pública, da ação direta de inconstitucionalidade e, até mesmo, da representação para fins de intervenção da União e dos Estados, entre outras medidas para manter a legalidade (por exemplo, na defesa do patrimônio público contra os desmandos do administrador público), nos termos do art. 129 da Carta constitucional de 1988.

Outra faceta do novo perfil do Ministério Público é a defesa do regime democrático.

A Constituição de 1988 estabeleceu no Brasil, de forma expressa, o Estado democrático de direito, quando definiu os fundamentos do sistema de separação de poderes, a soberania popular, a cidadania, a dignidade da pessoa humana, os valores sociais do trabalho e da livre iniciativa e ainda, o pluralismo político.

Agindo dessa forma, a Constituição fixou, de maneira absoluta, a democracia participativa, como norma jurídica constitucionalmente positivada. Assim, a defesa do regime democrático importa em salvaguardar todos os dispositivos formais da democracia representativa e do conteúdo material da própria Constituição, em especial, os direitos e garantias fundamentais. Essa é uma das funções do Ministério Publico Brasileiro.

Portanto, o Ministério Público é também instituição destinada à preservação dos valores fundamentais do Estado enquanto comunidade e, para tanto, recebeu a função de efetivar esses direitos. O Ministério Público é um dos instrumentos de efetivação de cidadania.[18]

Enfim, para que Ministério Público bem desempenhe a defesa do regime democrático, alguns princípios devem ser respeitados, a saber: a) a existência de mecanismos pelos quais a grande maioria do povo possa tomar decisões concretas, não apenas para a escolha de um governante ou um legislador periodicamente e, a partir daí, faça este o que bem entender mesmo contrariamente ao que prometeu antes de ser eleito, mas sim para que o povo possa decidir as grandes questões que digam respeito ao destino do país e possa controlar o exercício do mandato dos que foram eleitos, o que inclui necessariamente sua cassação, em caso de violação dos compromissos partidários (*recall*); b) o funcionamento de canais de manifestação (como criação, fusão, extinção de partidos; sufrágios frequentes, não só para investiduras dos governantes, como também para as grandes questões nacionais etc..); c) não sejam suprimidas pelo poder de emenda à Constituição as garantias fundamentais ao exercício da democracia; d) haja total liberdade no funcionamento desses canais de controle; e) sejam validamente apurados os resultados dessas manifestações (eleições, plebiscitos, referendos); f) sejam efetivamente cumpridas as decisões ali tomadas (dever positivo); g) seja combatido qualquer desvio de cumprimento das decisões ali tomadas (dever negativo); h) sejam prioritariamente defendidos "aqueles que se encontrem excluídos, os empobrecidos, os explorados, os oprimidos, aqueles que se encontrem à margem dos benefícios produzidos pela sociedade".[19]

---

18. Cf. Ritt, *op. cit.*, p. 162.

19. Mazzilli, Hugo Nigro. O Acesso à Justiça e o Ministério Público. 3. ed. São Paulo: Saraiva, 1988. p. 50-51.

A promoção social está no núcleo do novo perfil constitucional do Ministério Público. A defesa do regime democrático e dos interesses sociais reafirma o compromisso do Ministério Público com a transformação, com a justiça, da realidade social. (art. 127, *caput*, combinado com art. 1.º e 3.º da CF-88). Nesse sentido os objetivos elencados no art. 3.º da Constituição do Brasil vinculam o Ministério Público, ou seja, ele deve defender uma sociedade livre, justa, solidária, com pobreza erradicada e com desigualdades sociais diminuídas. Esta é a destinação de fundo do Ministério Público brasileiro.

Assim, para o Ministério Público cumprir sua destinação constitucional não mais se sustenta o modelo institucional antigo. É preciso avançar com planejamento funcional e em suas estratégias de atuação. A atuação individual e intuitiva dos membros do Ministério Público deve ser superada por um novo modelo, em que o compromisso com a transformação social, o planejamento estratégico e a eficiência passem a ser condições naturais em todos os âmbitos da atuação institucional, jurisdicional ou extra jurisdicional.[20]

Esta Instituição, ao longo da história, sempre esteve em mutação, daí também ser chamado de agente de transformação social.[21] No pano de fundo do leque de atribuições conferidas ao Ministério Público, existe o interesse maior e supremo, que é a defesa da sociedade. A razão de ser do Ministério Público é a comunidade, este quando age é em nome e em prol da sociedade.

A Constituição cidadã pugnou pela proteção dos direitos individuais e sociais, enfim, pela defesa da sociedade. Nesse diapasão, os pobres e os excluídos não tinham como se organizar ou buscar, ainda que individualmente, fazer valer seus direitos, de forma rápida e eficaz. Do mesmo modo, erradicar ou amenizar a pobreza com uma melhor forma de justiça não tinha como ser efetivada por pessoas que sequer tinham consciência de seus direitos.

2. O TRATAMENTO DE DADOS PESSOAIS NA ATIVIDADE-FIM DO MINISTÉRIO PÚBLICO

A privacidade é um direito fundamental inerente a todo indivíduo, estando vinculada à dignidade humana, autonomia e à liberdade de expressão. Com o avanço da tecnologia e da coleta de dados, surgiu a abordagem da proteção de dados pessoais como um aspecto importante da privacidade.

---

20. Almeida, Gregório Assagra de. O Ministério Público no neo-constitucionalismo: Perfil constitucional e alguns fatores de ampliação de sua legitimação social. In: Farias, Cristiano Chaves de; Alves, Leonardo Barreto Moreira; Rosenvald, Nelson Alves. Temas Atuais do Ministério Público: a atuação do *parquet* nos 20 anos da Constituição Federal. Rio de Janeiro: Lumen Juris, 2008. p. 48-49.

21. Nesse sentido Jatahy, 2007, *op. cit.*, p. 71.

Nesse contexto, a edição da Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, representou importante conquista para o ordenamento jurídico brasileiro, notadamente no que se refere à proteção de direitos constitucionalmente garantidos. Nesse ponto, cumpre destacar que o Judiciário, mais especificamente o Supremo Tribunal Federal no julgamento de ações constitucionais[22] propostas em face da Medida Provisória 954/2020[23], pela primeira vez, ampliou a proteção constitucional de dados pessoais, de sorte a deslocar, como bem observa Frazão, Carvalho e Milanez (2022, p. 27), "o eixo de proteção dos *tipos de dados* tratados [...] para a *forma e finalidade* do próprio tratamento[24]". Com isso, foram sedimentadas as bases para a compreensão da proteção de dados pessoais como direito fundamental autônomo e que, portanto, vai além da proteção da intimidade sob a dicotomia do público-privado, para também proteger valores básicos de um Estado Democrático de Direito: liberdade, igualdade, cidadania e democracia.

Com isso, observação uma alteração do centro gravitacional protetivo do direito à privacidade: do caráter individualista e vinculado a uma abordagem negativa de não intervenção, para o reconhecimento de um direito positivo e dinâmico do indivíduo de controle sobre o fluxo de seus dados pessoais, independentemente de a informação ser íntima ou privada, pública e notória.

Desta feita, ao superar a ideia de privacidade como mera liberdade negativa, para adotar a noção de proteção de dados pessoais como um direito positivo, conferiu-se o devido protagonismo decisório ao titular quanto ao fluxo informacional dos seus dados. E não só isso: a edição da LGPD contribuiu para fomentar o debate acerca da atualização de critérios de regulação da privacidade e, em especial, à proteção de dados no país, como também veio ao encontro da necessidade de ampliação normativa de proteção do titular e dos seus dados pessoais.

Por esta senda e ainda em observância aos preceitos então recém editados da LGDP, a matéria do direito à proteção de dados pessoais também foi objeto de apreciação pelo Poder Legislativo, por meio da proposição da Emenda à Constituição (PEC) 17/2019. A proposta resultou na edição da Emenda Constitucional 115/2022, que acrescentou, entre os direitos e

22. Ações Diretas de Inconstitucionalidade (ADIs) 6.387, 6.388, 6.389, 6.390 e 6.393

23. A MP 954, de 17/04/2020, tratava do compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

24. Frazão, Ana; Carvalho, Angelo Prata de; Milanez, Giovana. Curso de Proteção de dados pessoais: fundamentos da LGPD. 1ª edição. Rio de Janeiro: Forense, 2022.

garantias fundamentais, o inciso LXXIX ao artigo 5º da Constituição Federal, segundo o qual: *"é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".*

Ao dispor do tratamento de dados pessoais, a LGPD definiu, em seu art. 5º, I que dado pessoal é toda "*informação relacionada a pessoa natural identificada ou identificável".* O inciso II do mesmo dispositivo, por sua vez, definiu dado pessoal sensível, este recebendo tratamento mais cauteloso no viés legislativo. De igual forma, a LGPD definiu, no seu artigo 5º, X, que tratamento é "toda operação realizada com dados pessoais, como as 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".

Assim, a LGPD não proíbe a utilização dos dados pessoais, mas se propõe a regulamentar a forma de tratamento dos dados pessoais por uma pessoa física ou jurídica, de direito público ou privado. Nessa esteira,o Estado, em suas diversas acepções e em todos os níveis federativos, é relevante agente de tratamento de dados, seja em razão das atividades públicas que exerce, seja em virtude da vasta base de dados confiados a sua tutela. Isso porque, como bem observa Frazão, Carvalho e Milanez (2022), o acesso a dados é, a um só tempo, importante elemento para a realização de políticas públicas e otimização de serviços, como também é assunto delicado e preocupante do ponto de vista democrático.

Na LGPD, que possui capítulo próprio (Capítulo IV) disciplinando o tratamento de dados pessoais pelo Poder Público, e considerando, ainda, os fenômenos da descentralização e desconcentração, próprios da organização administrativa brasileira, o legislador optou por se referir à Lei de Acesso à Informação - LAI (Lei nº. 12.527/2011) para enquadramento dos entes públicos:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 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, desde que: [...]

Assim, diante da redação do parágrafo único do artigo 1º, da LAI, os entes públicos compreendidos na esfera de proteção relacionada ao tratamento de dados pelo Poder Público, e que, portanto, submetem-se à disciplina da LGPD são: I) os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II) as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Nota-se, com isso, que o escopo da Lei de Proteção de Dados é bem abrangente, de modo a reunir entidades dos três Poderes da República, seus respectivos órgãos, o Ministério Público e a Administração Pública Indireta.

Sobre o assunto, a Autoridade Nacional de Proteção de Dados – ANPD, autarquia especial vinculada ao Ministério da Justiça e Segurança Pública e responsável por zelar pela proteção dos dados pessoais, assim como orientar, regulamentar e fiscalizar o cumprimento da LGPD em todo o território nacional, emitiu, em junho de 2023, Guia Orientativo[25], reconhecendo as especificidades do tratamento de dados pelo Poder Público, assim como diversas questões controvertidas que têm sido levantadas, pelos próprios órgãos públicos, para adequação à novel legislação:

> (i) o âmbito de incidência da LGPD e a aplicação de seus conceitos básicos ao setor público; (ii) a adequada interpretação das bases legais que autorizam o tratamento de dados pessoais; (iii) os requisitos e as formalidades a serem observados nas hipóteses de uso compartilhado de dados pessoais; e (iv) a relação entre as normas de proteção de dados pessoais e o acesso à informação pública.

Assim, a Lei Geral de Proteção de Dados brasileira, embora tenha representado importante avanço na defesa de direitos constitucionalmente garantidos, ainda experimenta inúmeros desafios e controvérsias na sua interpretação e implementação, em especial por parte do Poder Público, como por exemplo: a) a adequação normativa da estrutura de órgãos desvinculados dos Poderes da República (Executivo, Legislativo e Judiciário); b) o âmbito de incidência da LGPD, em especial na conciliação dos fundamentos que lhes são próprios (art. 2º, I e IV) com o princípio da publicidade consagrado tanto no artigo 37, *caput*, da Constituição Federal quanto na Lei de Acesso à Informação; c) definição do controlador de dados pessoais tratados no Ministério Público[26], sem que a independência funcional de seus membros seja mitigada e sem que a autonomia ministerial seja invadida por entes ou órgãos de quaisquer dos Poderes da Federação; d) definição de políticas e procedimentos para incutir na cultura organizacional uma adequada prática de gestão e governança de dados, sem que isso importe em prejuízo à transparência dos atos administrativos ou o exercício de suas competências

25. Autoridade Nacional de Proteção de Dados - ANPD (Brasil). Guia Orientativo para Tratamento de dados pessoais pelo Poder Público. Brasília/DF, 2023.

26. De acordo com o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, elaborado pela ANPD, define-se que, em relação à Administração Pública Direta, são controladores para todos os efeitos legais, somente a União, Estados, Distrito Federal e Municípios: "29. Assim, em conclusão: nas operações de tratamento de dados pessoais conduzidas por órgãos públicos despersonalizados a pessoa jurídica de direito público a que os órgãos sejam vinculados é a controladora dos dados pessoais e, portanto, responsável pelo cumprimento da LGPD. 30. Contudo, em razão do princípio da desconcentração administrativa, o órgão público despersonalizado desempenhará funções típicas de controlador de dados, de acordo com as obrigações estabelecidas na LGPD".

constitucionais; e) limitações estruturais, financeiras e procedimentais, para assegurar o devido fortalecimento da área de segurança da informação em órgãos públicos.

Não há dúvidas de que, por anos, a Administração Pública coletou dados pessoais de maneira indiscriminada, muitas vezes sem se preocupar, segundo ressalta Xavier (2023), com princípios consagrados na LGPD, como o da finalidade, adequação, necessidade ou mesmo da segurança. Por essa razão e dada a importância estratégica e comercial dos dados, tido como as novas "commodities do século XXI", é importante que o setor público busque estar em conformidade com a novel legislação, sem comprometer a consecução de suas finalidades públicas[27].

O Ministério Público, em sua função constitucional, é responsável por assegurar a correta aplicação da lei, defendendo o interesse público e a coletividade. Isso significa que ele pode fiscalizar e, quando necessário, acionar o Poder Judiciário para garantir que o Estado e a iniciativa privada atuem dentro dos limites legais, respeitando suas competências e responsabilidades. Assim, levando em conta as diretrizes programáticas do Ministério Público e sua função fundamental de fiscalização e tutela dos direitos fundamentais, cabe ao órgão proteger os dados pessoais nas relações de consumo, nas relações de trabalho, nos serviços públicos e em outras interações jurídicas.

A busca do Ministério Público Brasileiro por adequação às exigências legais é um passo essencial para garantir a privacidade e a segurança dos dados pessoais em um cenário de crescente compartilhamento e uso de informações. O reconhecimento constitucional da proteção de dados pessoais, que visa a defesa dos cidadãos — agora considerados titulares de dados —, ressalta a importância desse direito e a necessidade de um tratamento responsável e ético dos dados, incluindo a atuação do Poder Público. Isso é fundamental para assegurar que a proteção dos dados pessoais seja tratada com a seriedade necessária, promovendo a confiança da sociedade nas instituições responsáveis por sua defesa.

Nesse contexto, há uma preocupação em garantir que não apenas a atividade administrativa dos órgãos e entidades esteja em conformidade com os preceitos da LGPD, mas também que suas atividades-fim, especialmente no contato com o público externo, estejam adequadas.

Como demonstrado, a atividade-fim do Ministério Público brasileiro consiste na defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis. Isso inclui promover a justiça e assegurar o

27. Xavier, Fabio Correa. Passos mínimos necessários para adequação à LGPD pelas Cortes de Contas brasileiras. In: LIMA, Edilberto Carlos Pontes (Coord.). Os Tribunais De Contas, a Pandemia e o Futuro do Controle. Belo Horizonte: Fórum, 2021. Disponível em: https://www.forumconhecimento.com.br/livro/L4291/E4487/32716.

cumprimento da lei, atuando como fiscal da legislação e defensor dos direitos fundamentais dos cidadãos. Considerando as diversas funções do Ministério Público, como propor ações penais públicas, proteger o patrimônio público e social, garantir a defesa dos direitos difusos e coletivos, fiscalizar a execução de leis e promover a tutela dos interesses de crianças, adolescentes, idosos e outros grupos vulneráveis, é fundamental que os direitos à proteção de dados e à privacidade sejam respeitados e resguardados conforme a Constituição. Dessa forma, todo o tratamento de dados pessoais realizado pelo órgão, no cumprimento de sua atividade-fim, deve seguir boas práticas, superando as exigências da legislação vigente.

Ao implementar essas medidas, as divisões responsáveis pela atividade-fim do Ministério Público não apenas protegem seus ativos e a privacidade das pessoas que tutelam, mas também garantem o cumprimento das regulamentações e normativas legais, como a LGPD e o direito constitucional à proteção de dados.

3. O REGISTRO DE OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS

O Registro de Operações de Tratamento de Dados Pessoais (ROTDP), mais conhecido pela sigla, em inglês, RoPA (*Record of Processing Activities*), consiste em um processo de inventário (ou mapeamento) de todas as operações de tratamento de dados pessoais realizadas pelo agente de tratamento.

O RoPA é exigido pelo art. 37 Lei Geral de Proteção de Dados brasileira (LGPD), inspirado no art. 30 do Regulamento Geral sobre a Proteção de Dados europeu (GDPR).[28] Essa obrigação decorre dos princípios da responsabilização e prestação de contas (*accountability*), previstos no art. 6º, inciso X, da LGPD (art. 5º, 2, do GDPR), segundo os quais o agente de tratamento é responsável pelo cumprimento das normas de proteção de dados pessoais e deve ser capaz de apresentar evidências de que adotou medidas eficazes para tanto.

A partir do mapeamento é possível visualizar e compreender, em uma perspectiva macro, o fluxo de dados pessoais dentro da organização, de que forma eles são coletados, como são processados, onde estão armazenados e com quem são compartilhados. Para isso, devem ser reunidas informações de cada área ou processo de trabalho sobre as finalidades do tratamento, a base legal que ampara a operação, as categorias de titulares e os tipos de dados

28. Diferentemente da LGPD, que apenas enuncia a obrigação do controlador e do operador de manter o ROTD, o GDPR detalha as informações mínimas que devem constar do ROTD, estabelece que o ROTD deve ser elaborado por escrito (inclusive em formato eletrônico) e prevê que os agentes de tratamento devem disponibilizar o ROPD à autoridade de proteção de dados, quando requisitado.

pessoais tratados, origem dos dados, meios de coleta e processamento, locais de armazenamento, informações sobre compartilhamento e transferência internacional, prazos para eliminação dos dados e medidas de segurança aplicáveis, além de informações sobre os agentes de tratamento (controlador e operador) e o encarregado. [29]

Essas informações podem ser obtidas por meio de entrevistas ou questionários aplicados aos integrantes de cada setor ou aos responsáveis pelos respectivos processos de trabalho, com o uso de planilhas ou sistemas especializados.[30] Como a confiabilidade das informações reunidas no inventário depende substancialmente das declarações prestadas por essas pessoas, é essencial que, antes ou durante o processo de mapeamento, sejam implementadas ações de conscientização e treinamento acerca da temática da proteção de dados pessoais, a importância e finalidade do RoPA e os principais conceitos envolvidos. O mapeamento prévio dos processos de trabalho (cadeia de valor), ativos (sistemas) e terceiros (fornecedores) e a existência de tabelas de temporalidade e destinação de documentos também facilitam a elaboração do inventário dos dados pessoais e contribuem para a qualidade do RoPA. No caso de dados eletrônicos, em complemento às declarações e como forma de corroboração das informações, também podem ser utilizadas ferramentas automatizadas de *data discovery* para identificação dos dados nos sistemas e aplicações utilizados – sem esquecer os bancos de dados pessoais em suporte físico, que também são objeto de proteção (LGPD, art. 5º, IV) e devem ser mapeados.

Ao final, o RoPA precisa ser conferido e validado pelo encarregado e pela equipe de privacidade. No caso do Poder Público, uma boa prática associada ao princípio da transparência (LGPD, art. 6º, VI) é a consolidação dos resultados do RoPA e a divulgação de estatísticas sobre o inventário, como a quantidade de processos mapeados, principais tipos de dados pessoais tratados e categorias de titulares, bases legais mais frequentes, etc.[31]

O inventário precisa ser mantido sempre atualizado. Para tanto, a política de privacidade da organização pode prever revisões periódicas do RoPA. Outra alternativa é a definição de certos eventos (gatilhos) que, por terem impacto sobre os dados pessoais tratados pela organização (como mudanças em processos de trabalho, sistemas ou fornecedores), devem desencadear um processo de ajuste no inventário.

---

29. Fonseca, Edson Pires da. Lei geral de proteção de dados pessoais – LGPD. Imprenta: Salvador, JusPODIVM, 2021, p. 150-151.

30. Densmore, Russel; *et al*. Privacy Program Management. 3ª ed. Portsmouth: International Association of Privacy Professionals - IAPP, 2021.

31. Nesse sentido, vale conferir os painéis de inventário divulgados pelo Conselho Nacional do Ministério Público (https://www.cnmp.mp.br/portal/relatoriosbi/inventario-de-bases-de-dados-do-cnmp-simplificado) e o Ministério Público Federal (https://www.mpf.mp.br/servicos/lgpd/inventario-de-dados).

Muito além de atender um requisito legal, o inventário dos dados pessoais é relevante para construção da estratégia de implementação do programa de privacidade da organização.[32] Ele permite identificar os setores, sistemas e processos de trabalho mais críticos em relação aos riscos associados ao tratamento de dados pessoais, seja pelo volume de dados pessoais tratados ou a quantidade de titulares, os tipos de dados pessoais envolvidos (com especial atenção a dados pessoais sensíveis) ou as categorias de titulares (especialmente se há dados pessoais de crianças e adolescentes e outros titulares vulneráveis, como idosos, pessoas com deficiência, refugiados, minorias, vítimas e testemunhas de crimes, etc). Com isso é possível definir as prioridades para adoção de medidas de governança e conformidade, conscientização e treinamento, avaliação de riscos, segurança da informação, entre outras ações.

Os resultados do RoPA também são úteis e podem ser aproveitados em diversas etapas do programa de privacidade, como a elaboração dos avisos de privacidade, a análise da conformidade legal dos processos de trabalho, a aferição de riscos no âmbito de relatórios de impacto à proteção de dados (RIPD), a pesquisa de dados pessoais para atendimento a requerimentos de titulares e na adoção de providências em casos de incidentes de segurança com dados pessoais (avaliação do incidente, comunicações às autoridades e titulares).

4. A RESOLUÇÃO CNMP 281/2023 E SUA APLICAÇÃO À ATIVIDADE-FIM DO MINISTÉRIO PÚBLICO

A Resolução n. 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP), institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público. Essa é a principal referência normativa, de natureza setorial, para guiar a atuação dos ramos e unidades do Ministério Público brasileiro em matéria de proteção de dados pessoais – além, evidentemente, da própria LGPD, que funciona como norma geral, de interesse nacional, aplicável a todos os entes federativos (art. 1°, parágrafo único).

A Resolução CNMP n. 281/2023 está estruturada em três grandes pilares. Em primeiro lugar, ela busca assegurar a autonomia funcional e administrativa do Ministério Público e a independência funcional de seus membros (art. 127, §§1° e 2° da Constituição Federal), ao conferir ao CNMP o papel de Autoridade de Proteção de Dados Pessoais no Ministério Público (APDP/MP), responsável por zelar, implementar e fiscalizar a proteção de dados pessoais, no âmbito do Ministério Público brasileiro, por meio da Unidade Especial de

32. Densmore, Russel; *et al*. Privacy Program Management. 3ª ed. Portsmouth: International Association of Privacy Professionals - IAPP, 2021.

Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público (CPAMP) (art. 4º, V). Na mesma linha, a resolução reafirma e resguarda as prerrogativas funcionais dos membros do Ministério Público, em atividades que envolvem o tratamento de dados pessoais, como o poder de requisição e acesso a bancos de dados (arts. 16 e 17, 72 a 75), uso de dados pessoais para produção do conhecimento (arts. 72 a 75), a gestão de bancos de dados e o compartilhamento interno e externo (arts. 18 e 19).

Em outra vertente, a Resolução CNMP n. 281/2023 promove e incentiva a atuação finalística do Ministério Público para defesa do direito fundamental à proteção de dados pessoais, por meio dos instrumentos de que dispõe, extrajudiciais e judiciais, cíveis e criminais, especialmente no âmbito coletivo (art. 14, 56 a 62). Nesse sentido, a norma prevê a estruturação de promotorias e procuradorias para atuação na defesa da ordem jurídica e da dimensão coletiva do direito à proteção aos dados pessoais, diante de violações à legislação por pessoas físicas ou jurídicas, de direito público ou privado, inclusive com a criação de órgãos especializados ou grupos especiais de atuação. A resolução estabelece, ainda, a necessidade de ações de capacitação de membros e servidores do Ministério Público para qualificar a atuação finalística na tutela do direito fundamental à proteção dos dados pessoais, inclusive nos cursos de ingresso e vitaliciamento, além de incentivo à produção científica. Além disso, é essencial que sejam desenvolvidas campanhas institucionais de comunicação voltadas à conscientização da sociedade sobre esse novo direito fundamental e o papel do Ministério Público na sua defesa.

O terceiro pilar da Resolução CNMP n. 281/2023 é voltado à conformidade interna das atividades dos ramos e unidades do Ministério Público. Afinal, para que o Ministério Público possa exigir dos outros o cumprimento da legislação de proteção de dados pessoais é preciso que ele seja exemplo e também adote as medidas pertinentes nesse campo. Assim, a resolução estabelece uma série de regras a serem observadas na atividade administrativa (art. 66), em setores como gestão de pessoas (art. 104 e seguintes), contratos (art. 68, 110, 171) e tecnologia da informação (art. 120 e seguintes). Há, ainda, disposições específicas sobre atendimento a requerimentos de titulares (art. 76), tratamento de dados pessoais sensíveis (art. 83 e 84), dados de crianças e adolescentes (art. 85 a 91), tratamento automatizado (art. 92), transferência e compartilhamento (art. 99 a 103) e, no que mais interessa aos fins deste trabalho, regras sobre mapeamento e custódia de dados pessoais (art. 80 a 82).

Porém, antes de abordar as disposições da Resolução CNMP n. 281/2023 sobre o mapeamento dos dados pessoais, questiona-se: esse ato normativo também se aplica à atividade-fim do Ministério Público? De forma mais específica, as operações de tratamento de dados pessoais realizadas nas atividades finalísticas do Ministério Público, em processos judiciais, investigações e outros procedimentos extrajudiciais, devem ser mapeadas e compor o inventário de dados pessoais (RoPA)?

A resposta a essa questão passa, inicialmente, pela análise do âmbito de aplicação da LGPD. O art. 3º da lei prevê que ela se aplica "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados", bastando que a operação seja realizada no território nacional, os titulares estejam no Brasil ou os dados tenham sido coletados no país. Por sua vez, o art. 4º estabelece as exceções a essa regra geral, ou seja, operações de tratamento de dados pessoais às quais a LGPD não se aplica. Nesse universo merecem destaque as hipóteses do inciso III: tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Segundo a LGPD, o tratamento de dados pessoais realizados nessas atividades, justamente por suas peculiaridades, criticidade e relevância para os interesses nacionais, "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (art. 4º, §1º).[33]

Na condição de titular exclusivo da ação penal pública, uma das principais atividades do Ministério Público é justamente a investigação e repressão de infrações penais, bem como o controle externo da atividade policial (Constituição Federal, art. 129, incisos I, VII e VIII). Porém, as finalidades institucionais do Ministério Público, conforme o perfil constitucional adotado no Brasil, vão muito além da atuação criminal e alcançam âmbitos diversos, como o sistema eleitoral, a defesa de direitos trabalhistas, a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos, em temas como saúde, educação, consumidor, idosos, pessoas com deficiência, crianças e adolescentes, populações indígenas e comunidades tradicionais. Portanto, boa parte da atividade finalística do Ministério Público escapa ao alcance das exceções do art. 4º da LGPD.

Por outro lado, o art. 23 da LGPD, que inaugura o capítulo sobre tratamento de dados pessoais pelo Poder Público, faz remissão ao art. 1º da Lei 12.527/2011, a Lei de Acesso à Informação (LAI), ao indicar as pessoas jurídicas de direito

33. O GDPR, da mesma forma, exclui de seu âmbito de aplicação material o tratamento de dados pessoais "efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" (artigo 2º, para. 2, "d"). Assim, no contexto europeu vigora a Diretiva (UE) 2016/680, acerca do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Já no Brasil, o projeto de lei da chamada "LGPD Penal" ainda está em tramitação no Congresso Nacional (PL 1515/2022), inexistindo, atualmente, legislação específica sobre o tema. Aras, V.B.; Mendonça, A.B.; Capanema, W.A.; Silva, C.B.F.; Costa, M.A.S. (Org.). Proteção de Dados Pessoais e Investigação Criminal. Brasília: ANPR, 2020.

público às quais se destina a norma. Já se afirmou que o regime jurídico da LAI não alcança as funções típicas do Judiciário e do Ministério Público, mas apenas a função administrativa (atípica) que esses órgãos exercem, uma vez que a publicidade dos atos jurisdicionais e ministeriais seria regida por normas específicas. E, com base nesse raciocínio, é possível defender que, de forma similar à LAI, apenas a atividade administrativa do Ministério Público e do Judiciário estaria sujeita, de modo geral, às normas da LGPD. As atividades finalísticas do Ministério Público seguiriam o regime mais limitado do art. 4º, §1º da LGPD (previsto expressamente apenas para as atividades de investigação e repressão de infrações penais).[34]

Porém, esse raciocínio parece expor mais uma questão de conflito entre normas, solucionado por métodos de interpretação (finalística, sistemática, etc) e pela técnica de prevalência da norma especial em relação à norma geral, do que propriamente de âmbito de aplicação da LAI e LGPD. A existência de regras específicas sobre publicidade dos atos jurisdicionais e ministeriais não afasta completamente a aplicação da LAI a esses atos. Tanto que as resoluções sobre portais de transparência do Judiciário e do Ministério Público, construídas a partir das normas sobre transparência ativa da LAI, incluem exigências de divulgação de estatísticas e íntegras de atos finalísticos,[35] sem prejuízo das regras sobre publicidade, sigilo e segredo de justiça, previstas nos diplomas processuais e resoluções do CNMP.

Da mesma forma, não é preciso excluir, de forma geral, a atividade finalística do Ministério Público do âmbito de aplicação da LGPD para defender que essa norma não obsta o pleno exercício do poder requisitório do Ministério Público. A requisição de diligências, informações, exames, perícias e documentos de autoridades da Administração Pública e de entidades privadas é uma prerrogativa dos órgãos do Ministério Público, prevista na Constituição (art. 129, VI e VIII) e nas leis orgânicas (Lei Complementar n. 75/1993, art. 7º e 8º, e Lei 8625/1993, art. 26). A legislação de proteção de dados pessoais, seja no âmbito constitucional ou infra, em nenhum momento impede o acesso a dados pessoais pelo Ministério Público em suas atividades finalísticas, nem o subordina à reserva de jurisdição, mas apenas impõe que sejam observadas certas condições para o tratamento de

34. Colégio dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público – CEDAMP, Estudo técnico: Lei Geral de Proteção de Dados Pessoais e o poder requisitório do Ministério Público. Novembro de 2023.

35. No âmbito do CNJ, há a Portaria nº 209, de 19/12/2019, que institui a política interna de dados abertos do CNJ, e a Resolução nº 333, de 21/09/2020, que determina a inclusão do campo Estatística na página principal dos sítios eletrônicos dos órgãos do Poder Judiciário, com vistas a reunir dados abertos, painéis de *business intelligence* e relatórios estatísticos referentes à atividade-fim do Poder Judiciário. No CNMP, a Resolução n. 89, de 28/08/2012, que regulamenta a Lei de Acesso à Informação no âmbito do Ministério Público, prevê a divulgação nos portais de transparência do Ministério Público de vários atos finalísticos, como recomendações, termos de ajustamento de conduta e audiências públicas, além de dados e estatísticas relativos à movimentação processual (art. 7º).

dados pessoais (enquadramento nas bases legais, respeito aos princípios de proteção de dados, adoção de medidas técnicas e administrativas de segurança, atendimento a requerimentos de titulares, registro das operações de tratamento, avaliação de riscos e implementação de medidas de mitigação, etc). Portanto, a solução de potencial conflito entre essas normas passa mais pelo emprego de métodos de interpretação do que pela limitação do âmbito de aplicação.

A Resolução CNMP n. 281/2023 parece caminhar no mesmo sentido. Ao invés de restringir o âmbito de aplicação da norma apenas à atividade administrativa do Ministério Público,[36] vários dispositivos da resolução buscam harmonizar a legislação de proteção de dados pessoais com o regime jurídico próprio do Ministério Público, resguardando suas prerrogativas e funções institucionais no exercício da atividade finalística.[37]

A única delimitação material do âmbito de aplicação da resolução é mesmo quanto às atividades de investigação e repressão de infrações penais, em consonância com o art. 4º, III, da LGPD (art. 1º, §§2º e 3º). No mais, prevalece a regra geral do art. 93 (em seção denominada "Do limite territorial e material") de que "a presente Resolução aplica-se em todo território nacional, nas hipóteses de tratamento de dados pessoais pelo Ministério Público brasileiro", inclusive na atividade finalística, havendo regras voltadas especificamente à proteção de dados pessoais nos atos praticados em procedimentos, investigações, inquéritos ou processos administrativos e judiciais.[38]

---

36. Na versão inicial do texto do projeto de resolução produzido pelo grupo de trabalho formado no CNMP constava do art. 66 que "a LGPD se aplica somente para o tratamento de dados pessoais que digam respeito à atividade administrativa do Ministério Público brasileiro". Porém, durante a tramitação do projeto, o conselheiro relator adotou a seguinte redação: "Art. 66. A atividade administrativa do Ministério Público será regida pelas disposições da LGPD que tratam das entidades públicas, ressalvado o exercício pleno de sua atividade finalística constitucionalmente outorgada à Instituição." Assim, ao invés da ideia de que a atividade finalística estaria excluída do âmbito de aplicação da LGPD, optou-se por uma fórmula voltada a resguardar as atividades destinadas ao atendimento das finalidades institucionais do Ministério Público.

37. Nesse sentido, vale conferir os seguintes dispositivos: art. 1º, §1º; art. 9º, §3º; art. 15, 16, 17, 23, 24, 72, 73 e 77. A título de exemplo, o art. 80, §3º, da Resolução CNMP n. 281/2023, ao tratar do inventário de dados pessoais, ressalva que a finalidade atribuída ao tratamento "não obsta que os dados pessoais sejam utilizados na execução de outras missões institucionais do Ministério Público, inclusive para efeitos de prevenção, investigação, detecção ou repressão de ilícitos ou execução de sanções, bem como para a produção de conhecimento necessária ao Ministério Público, para a salvaguarda e para a prevenção de ameaças à segurança pública e à segurança institucional."

38. Nesse sentido, em matéria de conformidade na atividade-fim, vale destacar o art. 79, que estabelece que, "a fim de assegurar a proteção aos dados pessoais das pessoas naturais no âmbito de procedimentos ou processos que tramitam no Ministério Público, poderá ser promovido o controle de acesso, a pseudonimização ou a decretação de sigilo dos autos ou de documentos específicos neles contidos, inclusive em relação às petições e

Portanto, ressalvadas as atividades de investigação e repressão de infrações penais, sujeitas a um regime mais limitado (art. 4º, III, §1º da LGPD), de modo geral, as operações de tratamento de dados pessoais realizadas na atividade-fim do Ministério Público estão abrangidas pelo âmbito de aplicação da LGPD e da Resolução CNMP n. 281/2023.

5. DIRETRIZES PARA O REGISTRO DE OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS NA ATIVIDADE-FIM DO MINISTÉRIO PÚBLICO

A Resolução CNMP n. 281/2023 estabelece que "os ramos e as unidades do Ministério Público deverão realizar o mapeamento ou o inventário das bases de dados, abrangendo todos os dados pessoais que estejam sob seu controle, incluindo aqueles que tenham sido compartilhados, independentemente do modo como se realizou a sua coleta."

Como se nota, a norma sobre o RoPA é bastante abrangente e menciona "todos" os dados pessoais sob controle do órgão, não fazendo qualquer distinção entre atividade administrativa ou finalística ou mesmo entre os tipos de atuação finalística (cível, criminal, trabalhista, eleitoral, judicial, extrajudicial, etc).

Em princípio, por estarem fora do âmbito de aplicação da LGPD e da resolução, não haveria obrigação de mapeamento das operações de tratamento de dados pessoais realizadas para fins exclusivos de investigação e repressão de infrações penais. Porém, mesmo nessas atividades, a LGPD estabelece que devem ser "observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (art. 4º, §1º).[39]

O RoPA é um instrumento importante para análise da conformidade com os princípios de proteção. Por meio dele verifica-se se não estão sendo tratados dados excessivos ou incompatíveis com a finalidade específica de cada processo de trabalho, em consonância com os princípios da

aos documentos juntados pelas partes envolvidas." Outra importante iniciativa voltada à conformidade da atividade finalística à legislação de proteção de dados pessoais é a Orientação n. 1, de 22/5/2024, da Unidade Especial de Proteção de Dados Pessoais do Conselho Nacional do Ministério Público (UEPDAP/CNMP), que prevê providências a serem adotadas por membros do Ministério Público no tocante a gravações audiovisuais para instrução de procedimentos em trâmite no Ministério Público e concretizadas em audiências judiciais e Plenários do Júri. Disponível em https://www.cnmp.mp.br/portal/institucional/uepdap/documentos-e-publicacoes.

39. Sobre o sentido dessa disposição, vide Aras, Vladimir. Aplicabilidade da LGPD às atividades de segurança pública e persecução penal. Jota, 30/04/2024 Disponível em https://www.jota.info/opiniao-e-analise/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal-30042024?non-beta=1#_ftn3.

finalidade, adequação e necessidade (LGPD, art. 6º, I, II e III). Também se apura no inventário se são adotadas medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais e prevenir incidentes de segurança, conforme os princípios da segurança e prevenção (LGPD, art. 6º, VII e VIII). Além disso, ao identificar os dados pessoais tratados, meios de coleta, formas de processamento, situações de compartilhamento e tempo de retenção, os resultados do inventário podem ser aproveitados para produção de avisos de privacidade, que concretizam o princípio da transparência (LGPD, art. 6º, VI). Da mesma forma, ao mapear os locais de armazenamento dos dados pessoais, o RoPA pode auxiliar na busca de dados visando atender requerimentos de acesso e outros direitos dos titulares (LGPD, art. 18).[40]

Assim, a despeito da exceção legal do art. 4º, III, da LGPD, a fim de atender os princípios gerais de proteção e os direitos do titular (§1º), o inventário também é recomendável para as operações de tratamento de dados pessoais realizados na atuação criminal do Ministério Público – observadas, evidentemente, as peculiaridades e necessidades próprias dessa área para resguardar a efetividade das funções institucionais, como, por exemplo, a limitação da publicidade do RoPA.

A Resolução CNMP n. 281/2023 prevê que cabe ao encarregado a atribuição de "elaborar e manter inventário de dados pessoais que documente como e por que o Ministério Público coleta, compartilha e usa esses dados" (art. 46, IV). É necessário, contudo, interpretar essa regra em conformidade com a LGPD para extrair o sentido mais adequado, uma vez que a obrigação de "manter registro das operações de tratamento de dados pessoais" é conferida pela LGPD aos agentes de tratamento (controlador e operador) (art. 37) e não ao encarregado, cujas atribuições estão descritas no art. 41, §2º.

Recentemente, a Autoridade Nacional de Proteção de Dados (ANPD), exercendo a competência de "estabelecer normas complementares sobre a definição e as atribuições do encarregado" (art. 41, §3º), editou o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais (Resolução CD/ANPD n. 18, de 16 de julho de 2024). Essa norma estabelece que cabe ao encarregado, uma vez solicitado, "prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme o caso, de (...) registro das operações de tratamento de dados pessoais" (art. 16, II). Essa atuação de "assistência e orientação" por parte do encarregado na elaboração do RoPA parece mais condizente com o que dispõe a LGPD (art. 41, §2º, III), mantendo com os agentes de tratamento a obrigação de elaborar o inventário (art. 37).

40. Nesse sentido, a Resolução CNMP n. 281/2023 prevê que "na realização do inventário de dados pessoais, deverão ser identificados os processos e mecanismos técnicos pelos quais serão colhidas as informações necessárias para o atendimento dos direitos dos titulares de dados pessoais" (art. 80, §2º).

Assim, por determinação do controlador, o encarregado até pode assumir o planejamento, a coordenação e a execução do trabalho de mapeamento dos dados pessoais, além da atualização regular do RoPA, tudo em conjunto com a equipe de apoio e os setores mapeados. Porém, como bem ressalva a Resolução CD/ANPD n. 18/2024, "o desempenho das atividades e das atribuições [designadas ao encarregado] não confere ao encarregado a responsabilidade (...) pela conformidade do tratamento dos dados pessoais realizado pelo controlador."

Para elaboração do RoPA, a Resolução CNMP n. 281/2023 estabelece que "as coleções de dados pessoais inventariadas deverão ser catalogadas conforme os processos de trabalho desenvolvidos institucionalmente, de maneira a permitir a identificação precisa da natureza e da finalidade de todo tratamento, das estruturas orgânicas que o realizam e da forma de coleta dos dados pessoais" (art. 80, §1º). Embora a resolução faça menção aos "processos de trabalho desenvolvidos institucionalmente", a partir da cadeia de valor da organização (mapeamento de processos), não se vislumbra óbice à adoção de outra estratégia para inventário dos dados pessoais, conforme a autonomia administrativa de cada ramo ou unidade do Ministério Público. Assim, o inventário pode ser realizado por áreas ou setores da instituição (gestão de pessoas, contratos, comunicação, tecnologia da informação, secretaria jurídica, órgãos da Administração Superior, órgãos de execução, órgãos auxiliares) ou a partir de cada um dos sistemas, plataformas, aplicativos, bases de dados e outras ferramentas de tecnologia da informação onde os dados são tratados, sem deixar de incluir também os dados em suporte físico.

Qualquer que seja a estratégia adotada para o mapeamento, o trabalho deve envolver os setores diretamente responsáveis pelo tratamento dos dados, pois são eles que conhecem a operação e podem fornecer informações sobre os tipos de dados pessoais tratados, o perfil dos titulares, a finalidade pretendida, a origem e meios de coleta, locais de armazenamento, formas de processamento, com quem são compartilhados e por quanto tempo são retidos. Além do envolvimento do encarregado e da equipe de privacidade, também pode ser necessário o apoio das áreas de tecnologia e segurança da informação para prestar informações sobre medidas de segurança adotadas, atuação de operadores e eventual transferência internacional (por exemplo, em serviços de computação em nuvem).

No caso da atividade-fim, diante da multiplicidade de órgãos de execução e havendo certa similitude de suas estruturas e processos de trabalho, para a realização do inventário pode-se pensar em reuni-los em grupos temáticos ou regionais, envolvendo na elaboração do RoPA apenas os representantes de cada área e os respectivos órgãos de coordenação e apoio (Câmaras de Coordenação e Revisão do Ministério Público da União e Centros de Apoio Operacional dos Ministérios Públicos Estaduais). Também devem participar do inventário os responsáveis por outros setores que, de alguma forma,

tratam dados pessoais destinados aos órgãos de execução da atividade-fim, como secretarias jurídicas, núcleos periciais, áreas de pesquisa e análise, centros de inteligência e produção de conhecimento, grupos de trabalho, forças-tarefa e grupos de atuação especial.

Concluído o inventário, a Resolução CNMP n. 281/2023 determina que ele seja "atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas dos processos de trabalho" (art. 80, §4º). Portanto, é recomendável que sejam instituídos mecanismos de monitoramento para identificar mudanças nos processos de trabalho e outras alterações em operações de tratamento de dados pessoais, a fim de garantir que o RoPA esteja sempre atualizado e reflita a realidade da organização.

Por fim, considerando que na atividade dos órgãos públicos a regra é a publicidade e o sigilo a exceção, a Resolução CNMP n. 281/2023 estabelece que "o inventário de bases de dados pessoais não importa nem autoriza o acesso ao seu conteúdo", especialmente aquelas classificadas como sigilosas e confidenciais (art. 82). A resolução também ressalva a possibilidade de se restringir, total ou parcialmente, a publicidade do RoPA. Com isso, busca-se preservar o acesso, tanto internamente como para o público interno, a informações estratégicas cujo sigilo é considerado imprescindível para o cumprimento das finalidades institucionais.

6. CONCLUSÃO

No Brasil, diferentemente da maioria dos países da Europa e das Américas, as finalidades institucionais do Ministério Público vão muito além da esfera criminal. Uma importante parte da atividade-fim do Ministério Público é voltada à defesa de direitos fundamentais, à tutela de direitos difusos e coletivos, à proteção do patrimônio público e social e à defesa da ordem jurídica e do regime democrático.

No desempenho de sua missão constitucional o Ministério Público realiza diversas operações de tratamento envolvendo os mais variados tipos de dados pessoais e uma multiplicidade de titulares. Assim, além de atuar para tutela desse novo direito fundamental, no exercício de suas atribuições finalísticas os órgãos do Ministério Público devem igualmente observar a legislação de proteção de dados pessoais.

Um relevante instrumento para demonstrar esse compromisso é o inventário de dados pessoais (RoPA), previsto no art. 37 da LGPD, que compreende o registro de todas as operações de tratamento de dados pessoais realizadas pela organização. O inventário deve abranger não só as atividades administrativas, mas também a atividade-fim, descrevendo os dados pessoais tratados, as categorias de titulares, a finalidade, base legal e todo o ciclo de vida dos dados, desde a coleta até a eliminação.

A Resolução CNMP n. 281/2023 apresenta diretrizes para realização do inventário de dados pessoais nos ramos e unidades do Ministério Público brasileiro. Esse trabalho de mapeamento deve envolver não só o encarregado e sua equipe de apoio, mas todos os setores responsáveis pelo tratamento de dados pessoais, que conhecem os processos de negócio e são capazes de fornecer informações mais fidedignas para o inventário.

Portanto, o inventário é uma etapa fundamental para compreensão do fluxo de dados pessoais na organização e a definição da estratégia a ser adotada na implementação do programa de governança em privacidade no Ministério Público.

7. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Almeida, Gregório Assagra de. O Ministério Público no neoconstitucionalismo: Perfil constitucional e alguns fatores de ampliação de sua legitimação social. In: Farias, Cristiano Chaves de; Alves, Leonardo Barreto Moreira; Rosenvald, Nelson Alves. *Temas Atuais do Ministério Público: a atuação do parquet nos 20 anos da Constituição Federal*. Rio de Janeiro: Lumen Juris, 2008. p. 48-49.

Aras, Vladimir. *Aplicabilidade da LGPD às atividades de segurança pública e persecução penal*. Jota, 30/04/2024 Disponível em https://www.jota.info/opiniao-e-analise/artigos/aplicabilidade-da-lgpd-as-atividades-de-seguranca-publica-e-persecucao-penal-30042024?non-beta=1#_ftn3.

Aras, V.B.; **Mendonça**, A.B.; **Capanema**, W.A.; **Silva**, C.B.F.; **Costa**, M.A.S. (Org.). *Proteção de Dados Pessoais e Investigação Criminal*. Brasília: ANPR, 2020.

Autoridade Nacional de Proteção de Dados - ANPD (Brasil). *Segunda versão do Guia Orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*. Brasília/DF, 2022.

Autoridade Nacional de Proteção de Dados - ANPD (Brasil). *Guia Orientativo para Tratamento de dados pessoais pelo Poder Público*. Brasília/DF, 2023.

Brasil. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidente da República, 2023.

Caetano, Marcello. *Manual de Ciência Política e Direito Constitucional*. Coimbra: Almedina, 1996. Tomo I.

Cedamp - Colégio dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público, *Estudo técnico: Lei Geral de Proteção de Dados Pessoais e o poder requisitório do Ministério Público*. Novembro de 2023.

Dallari, Dalmo de Abreu. *Elementos da Teoria Geral do Estado*. 25. ed. São Paulo: Saraiva, 2005.

Densmore, Russel; *et al*. *Privacy Program Management*. 3ª ed. Portsmouth: International Association of Privacy Professionals - IAPP, 2021.

Fonseca, Edson Pires da. *Lei geral de proteção de dados pessoais – LGPD*. Imprenta: Salvador, JusPODIVM, 2021.

Frazão, Ana, **Carvalho**, Angelo Prata de, **Milanez**, Giovana. *Curso de Proteção de dados pessoais: fundamentos da LGPD.* 1° edição. Rio de Janeiro: Forense, 2022.

Garcia, Emerson. *Ministério Público, Organização, Atribuições e Regime Jurídico*. 2. ed. Rio de Janeiro: Lumen Juris, 2005.

Jatahy, Carlos Roberto de C. *O Ministério Público e o Estado Democrático de Direito. Perspectivas Constitucionais de Atuação Institucional*. Rio de Janeiro: Lumen Juris, 2007.

Mazzilli, Hugo Nigro. *O Acesso à Justiça e o Ministério Público*. 3. ed. São Paulo: Saraiva, 1988.

Ritt, Eduardo. *O Ministério Público como Instrumento de Democracia e Garantia Constitucional*. Porto Alegre: Livraria do Advogado, 2002.

Xavier, Fabio Correa. Passos mínimos necessários para adequação à LGPD pelas Cortes de Contas brasileiras. In: LIMA, Edilberto Carlos Pontes (Coord.). *Os Tribunais De Contas, a Pandemia e o Futuro do Controle. Belo Horizonte: Fórum, 2021*. página inicial-página final. Disponível em: https://www.forumconhecimento.com.br/livro/L4291/E4487/32716.

A ATUAÇÃO DO MINISTÉRIO PÚBLICO FEDERAL EM FACE DO FACEBOOK E GOOGLE: BREVES NOTAS SOBRE A UTILIZAÇÃO DE PLATAFORMAS SUPOSTAMENTE GRATUITAS

Daniel Teixeira Bezerra[1]

Resumo: O acesso à internet é crucial para o exercício de direitos fundamentais, como a informação e a cidadania. Todavia isto não permite que empresas privadas ofereçam internet e serviços supostamente gratuitos em violação ao princípio da neutralidade da rede e a regra do consentimento informado. O artigo discute a atuação do Ministério Público Federal do Brasil em relação às práticas de coleta e uso de dados pessoais por parte das empresas Facebook (atualmente Meta) e Google, destacando os riscos associados ao uso de plataformas digitais supostamente gratuitas.

Palavras-chave: Internet. Direito a informação. Proteção de dados pessoais. Consentimento informado.

Resumen: El acceso a internet es crucial para el ejercicio de derechos fundamentales como la información y la ciudadanía. Sin embargo, esto no permite que empresas privadas ofrezcan internet y servicios supuestamente gratuitos, violando el principio de neutralidad de la red y la regla del consentimiento informado. El artículo analiza las acciones del Ministerio Público Federal de Brasil en relación con la recogida y uso de datos personales por parte de las empresas Facebook (ahora Meta) y Google, destacando los riesgos asociados al uso de plataformas digitales supuestamente gratuitas.

Palabras clave: Internet. Derecho a la información. Protección de datos personales. Consentimiento informado.

---

1. Doutorando em Direito Civil pela Universidade Estadual do Rio de Janeiro - UERJ (2026-2022). Mestre em Direito, Democracia e Mudanças Institucionais na Universidade Federal do Piauí - UFPI (2021). Servidor concursado do Ministério Público Federal (2006).

1. INTRODUÇÃO

Na contemporaneidade em que o acesso à internet tem sido instrumento para o exercício do direito fundamental à informação, plataformas digitais com serviços supostamente gratuitos têm se utilizado da estratégia de se monetizar com o tratamento de dados pessoais dos usuários, sem, contudo, informar devidamente acerca dos riscos envolvidos.

Ao não adotar medidas adequadas de segurança e não informar claramente sobre os propósitos do processamento de dados, a privacidade do usuário pode ser comprometida, em especial quando existe uma segmentação de publicidade comportamental, aprimorando a manipulação do consumidor.

Mesmo dados aparentemente irrelevantes podem prever informações pessoais confidenciais após o processamento. A análise contínua de dados atualiza constantemente os perfis digitais, arriscando discriminação no acesso aos serviços.

No presente artigo serão analisados dois casos em que o Ministério Público Federal atuou em face de duas das maiores empresas mundiais de tratamento de dados pessoais, o *Facebook* (atualmente Meta) e o *Google*.

2. O ACESSO À INTERNET COMO REFLEXO DO DIREITO FUNDAMENTAL À INFORMAÇÃO

Analisando dados coletados de 1998 a 2000, Manuel Castells demonstrou que 88% dos usuários da internet estavam nos países industrializados, apesar destes concentrarem apenas cerca de 15% da população mundial. Enquanto na Finlândia e nos Estados Unidos o percentual da população com acesso à internet era de 28% e 26,3%, respectivamente, apenas 2,4% da população mundial tinha esse acesso. Além disso, na América Latina a população com renda mais alta representava 90% dos usuários (Castells, 2019, p. 432).

Segundo o Comitê Gestor da Internet no Brasil, de 2008 para 2018, o Brasil apresentou um considerável aumento de 18% para 67% de domicílios com acesso à internet. Contudo, em 2018, enquanto apenas 40% dos domicílios das classes DE estavam conectados, entre as classes A, B e C o acesso à internet foi verificado em, respectivamente, 99%, 94% e 76% dos lares. A pesquisa apontou ainda que apenas 44% da população rural estava conectada (CGI, 2019, p. 104).

Em 2018, segundo o IBGE, 27,6% dos brasileiros possuíam restrição à educação e 20,1% à internet. Além disso, apenas 44,6% dos jovens residentes na área rural haviam completado o ensino médio, enquanto na área urbana esse percentual era de 69,8%. A pesquisa identificou ainda dentre os 20% da população com os menores rendimentos, o percentual de analfabetos era de 22,8%. (IBGE, 2019).

Segundo Pierre Lévy (2010), a pessoa desconectada da internet não poderia participar comunidades virtuais e, com isso, perderia a oportunidade não apenas de receber conhecimento, mas também para cria-lo, em um espectro de inteligência coletiva. Assim, o ciberespaço seria não apenas um meio de comunicação, mas também de vida social (Maciel, 2017). Para Ingo Wolfgang Sarlet e Carlos Alberto Molinaro (2016), o direito da informação não seria apenas uma garantia fundamental de alta relevância, mas também "uma técnica democrática de alta densidade na conformação das relações humanas numa determinada comunidade política e social".

Assim, a democratização do acesso à internet (inclusão digital) tem grande importância na difusão da cultura e do conhecimento, bem como ao exercício da cidadania. Durante a pandemia do novo coronavírus que o mundo enfrentou em 2020 isto ficou ainda mais perceptível. Em relação à cultura, os cidadãos em quarentena com acesso à internet puderam ver parte do acervo do Louvre, do *Metropolitan Museum of Art* (*Met*), do Museu do Vaticano, do Museu Nacional de Antropologia e do Museu da Arte Assis Chateaubriand (MASP), dentre outros, por meio de seus *websites*.[2] Além disso, o *Google* em parceria com mais de 4.500 museus no Brasil e no mundo disponibilizou na plataforma *Google Arts & Culture* um passeio virtual por seus corredores.[3]

Quanto ao conhecimento, o cidadão com acesso à *web* pode ler títulos clássicos que estão em domínio público, como a obra completa de Machado de Assis.[4] A internet possibilita ainda o fomento à pesquisa de artigos científicos por meio das plataformas como a do Portal de Periódicos da Capes, da *Scientific Electronic Library Online* (SciELO), do *Google* Acadêmico e do *Educational Resources Information Center* (ERIC).[5] A supracitada tecnologia possibilitou ainda localizar informações sobre o Covid-19 em fontes seguras, bem como que professores e alunos dessem continuidade a grupos de estudo por meio de plataformas de conferência remota.

Quanto ao exercício da cidadania, por meio da internet é possível consultar gastos públicos federais, estaduais e municipais por meio dos portais da transparência, bem como, caso se verifique irregularidades, encaminhar

2. Disponíveis respectivamente em <https://www.louvre.fr/en>, <https://www.metmuseum.org/> <http://www.museivaticani.va>, <https://www.mna.inah.gob.mx/> e <https://masp.org.br/>.

3. Estão disponíveis nesta plataforma o MASP, a Pinacoteca de São Paulo, o Museu Nacional das Belas Artes, o Museu Imperial, o Museu Afro Brasil, o Museu da Arte Moderna de São Paulo e do Rio de Janeiro, o Museu Oscar Niemeyer, o Museu Paulista, o Museu do Amanhã e o Instituto Vladimir Herzog, dentre outros do Brasil e do mundo. Disponível em <https://artsandculture.google.com/partner>.

4. Disponível em <http://machado.mec.gov.br/>.

5. Disponíveis respectivamente em <http://www.periodicos.capes.gov.br>, <https://scielo.org>, <https://scholar.google.com> e <https://eric.ed.gov>.

solicitação de apuração aos entes de fiscalização.[6] Além disso, o exercício da liberdade de expressão e intercâmbio de ideias por meio de redes digitais tem se demonstrado um instrumento de desenvolvimento social. Cabe ainda destacar que com a internet foi possível que durante a supracitada pandemia certas atividades do setor público e do setor privado continuassem a ser oferecidas em plataformas de teletrabalho (CGI, 2020, p. 6).

3. A ATUAÇÃO DO MINISTÉRIO PÚBLICO FEDERAL EM FACE DO *FACEBOOK*

Em abril de 2015, com a promessa de possibilitar o acesso à internet a brasileiros com menor poder aquisitivo, o *Facebook* firmou parceria com o executivo federal e anunciou a vinda do projeto *internet.org* para o Brasil.[7] Segundo a empresa, o objetivo da plataforma era levar o acesso à internet e seus benefícios para pessoas carentes, como, por exemplo, um agricultor que necessita de um boletim meteorológico preciso ou uma criança que não tem livros didáticos e necessita de uma enciclopédia.[8] Além disso, informou que de 85% da população do mundo vivia em áreas com cobertura de internet móvel, mas sem acesso em razão do custo da contratação do serviço. Neste sentido, a empresa faria parceria com operadoras de telefonia móvel e, por meio do serviço *Free Basics by Facebook*, iria disponibilizar gratuitamente acesso a informações de emprego, saúde, educação e informações locais.[9]

No mesmo ano, o Ministério Público Federal emitiu nota técnica[10] aduzindo que a supracitada plataforma não poderia ser considerada ".org" as sim comercial, pois o acesso supostamente gratuito seria apenas a *websites* pré-aprovados pelo *Facebook* e seus parceiros comerciais. Para realizar outros acessos, o usuário teria que pagar. Além disso, o *Facebook* iria aumentar sua receita com a venda de anúncios personalizados acessando dados pessoais de milhões de novos usuários em situação de vulnerabilidade informacional, sem o consentimento informado deles.

---

6. Os portais da transparência do governo federal e do Ministério Público Federal estão respectivamente disponíveis em <http://www.portaltransparencia.gov.br> e < https://www.transparencia.mpf.mp.br/>. A plataforma para o cidadão apresentar solicitação de investigações pela internet ao Ministério Público Federal (MPF) está disponível em <http://peticionamento.mpf.mp.br/>.

7. Informação disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2015-04/dilma-anuncia-parceria-com-o-facebook>.

8. Informação disponível em <https://info.internet.org/en/mission/>.

9. Informação disponível em <https://info.internet.org/en/story/free-basics-from-internet-org/>.

10 Nota técnica nº 02/2015: análise do projeto "internet.org" e o princípio da neutralidade da rede. Disponível em <http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/notas-tecnicas/nota-tecnica-no-2>.

Segundo a nota, os novos usuários poderiam não ter o conhecimento necessário para autorizar, conscientemente, a utilização de seus dados pelo *Facebook* e suas empresas parceiras, com destaque para o fato de que a rede social se monetiza com a venda de publicidade comportamental.

O *Facebook* monetiza o perfil comportamental dos usuários com a venda de anúncios com alto poder de direcionar suas escolhas, de modo que seu serviço gera um contrato oneroso, e não gratuito – com todos os efeitos jurídicos desta classificação decorrentes. (Furtado, Bezerra, 2020, p. 227).

Além disso, o projeto *internet.org* estaria violando o princípio da neutralidade instituído estabelecido no art. 9º, §3º do Marco Civil da Internet (Lei Federal nº 12.965/2014) que impõe aos provedores de acesso, onerosos ou gratuitos, a vedação de bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados.

Segundo Daniel César e Irineu Junior (2017), a neutralidade da rede está relacionada a "condutas aceitáveis e não aceitáveis por parte dos provedores de conexão, sendo esses proibidos de discriminar, priorizar e bloquear aplicativos, degradar o tráfego na rede", bem ausência de transparência com os usuários.

Assim, as limitações impostas pela plataforma poderiam gerar o oposto do que se espera da inclusão digital, pois seus usuários não teriam a liberdade de buscar diferentes fontes de conhecimento, cultura, bem como para exercer sua cidadania.

Percebe-se que ofertas de empresas privadas, como o *Facebook,* de conexão gratuita limitada condicionada à coleta e tratamento de dados dos usuários necessitam ser avaliadas com cautela, em especial quando a finalidade do tratamento é determinar com maior precisão o perfil comportamental dos indivíduos, "inundando esses consumidores como uma publicidade assertiva e quase irrecusável" (Almeida, 2016, p. 163).

O acesso à *web* é importante instrumento de inclusão social, mas iniciativas como a da *internet.org* podem trazer mais danos que benesses, violando direitos fundamentais do usuário, dentre eles, o da privacidade.

4. A ATUAÇÃO DO MINISTÉRIO PÚBLICO FEDERAL EM FACE DO GOOGLE

No caso analisado no item anterior, verificou-se que empresa privada estava oferecendo acesso supostamente gratuito à internet, todavia violando o princípio da neutralidade. Existem também situações em que mesmo o cidadão pagando pela conexão à internet, a utilização de serviços "gratuitos" pode colocar sua privacidade em risco. No Inquérito Civil Público nº 1.27.000.001406/2015-03 que deu origem a ação, verificou-se que, apesar do transcurso de mais dois anos da entrada em vigor do Marco Civil da Internet,

o *Google* estava realizando o tratamento de dados pessoais dos usuários do serviço *Gmail* sem previamente obter seu consentimento expresso e de forma destacada.

Em novembro de 2016 o Ministério Público Federal por meio da Procuradoria da República no Estado do Piauí (MPF/PRPI) propôs Ação Civil Pública contra o *Google* Brasil Internet Ltda, autuada na 2ª Vara Federal da Seção Judiciária do Estado do Piauí sob o nº 0025463-45.2016.4.01.4000 em decorrência do descumprimento da regra do disposto no artigo 7º, IX do Marco Civil da Internet acerca da exigência de destaque da cláusula de consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais.[11]

Na inicial, o Ministério Público Federal destacou que, no trâmite do Inquérito Civil Público, o próprio *Google* reconheceu que analisava do conteúdo dos *e-mails* de seus consumidores com a finalidade de "oferecer produtos e anúncios relevantes aos seus usuários".

Para a empresa, os usuários concordavam com esse tratamento de dados ao aceitarem os termos de serviço e política de privacidade do *Google* no momento da criação da conta. Contudo, restou comprovado que não havia destaque para a informação da atividade de tratamento, bem como que o internauta não tinha a escolha de utilizar o serviço sem consentir com a análise de suas mensagens.

Além de obter um consentimento genérico do consumidor, isto é, sem destaque para o tratamento de dados pessoais, o Ministério Público Federal ressaltou que o *Google* não informava com clareza uma das principais finalidades desta atividade, qual seja, a construção do perfil digital do usuário para venda de anúncios com alto poder de manipular do seu comportamento.

Neste ponto, destacou-se que, mesmo sem exigir a contrapartida em pecúnia pela utilização de seus serviços, os provedores de aplicações de internet que obtém vantagens econômicas através do oferecimento de serviço supostamente gratuitos estão sujeitos às normas consumeristas, conforme jurisprudência do Superior Tribunal de Justiça:

> DIREITO CIVIL E DO CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. [...] 1. A exploração comercial da internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo "mediante remuneração" contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor [...].[12]

11. Disponível em <http://www.mpf.mp.br/pi/sala-de-imprensa/noticias-pi/mpf-pi-ajuiza-acao-contra-google-por-descumprir-normas-de-protecao-de-dados>.

12. Brasil. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial nº 1.193.764/SP, Rel. Ministra Nancy Andrighi, julgado em 14/12/2010, DJe 08/08/2011.

> CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. [...] 2. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. 3. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo [...].[13]

Portanto, sendo os usuários do *Gmail* consumidores e o *Google* fornecedor do serviço, a cláusula do tratamento dos dados pessoais, por configurar uma limitação de seu direito à privacidade, deveria ser escrita com destaque nos termos de serviço, de modo a permitir a imediata e fácil compreensão, conforme o estabelecido no artigo 54, §4º do Código de Defesa do Consumidor.

Para adequação de tais termos, o Ministério Público Federal propôs ao *Google* a assinatura de Termo de Ajuste de Condutas (TAC), no qual a empresa firmaria compromisso de obedecer a exigência do artigo 7º, IX do Marco Civil da Internet. Contudo, a referida plataforma aduziu que não estaria descumprindo a lei, não assinou o TAC e permaneceu tratando os dados pessoais de seus consumidores sem obter destes o consentimento expresso e destacado.

Ocorre que ao realizar a análise automatizada de todas as interações de seus consumidores na plataforma *Gmail*, sem informá-los previamente dos riscos dessa atividade, o *Google* violou o direito à privacidade de seus usuários, à época do ajuizamento da ação garantido pelo artigo 5º, X da Constituição Federal de 1988, bem como pelo artigo 3º, II e III do Marco Civil da Internet. (SILVA, 2017, p. 27).

Segundo Michal Kosinski (2015) até mesmo fragmentos de informação supostamente irrelevantes podem, após a atividade de coleta e tratamento, predizer dados pessoais sensíveis da pessoa humana como raça, opção sexual, crença religiosa e ideologia política. Além disso, como a atividade de análise ocorre todas as vezes que o consumidor utiliza o *Gmail*, o perfil digital construído sem a consciência do indivíduo está em constante atualização, o que pode afetar não só a sua privacidade, mas também gerar discriminações no acesso a determinado bem ou serviço.

O Ministério Público Federal ressaltou que, apesar do *Google* não omitir a informação de que analisa as mensagens dos usuários do *Gmail* e vende anúncios relevantes, a empresa não informou acerca da prática da publicidade comportamental. Isto porque tendo acesso aos pontos da personalidade do consumidor, a plataforma é capaz predizer o seu comportamento e criar anúncios aptos a direcionar suas escolhas.

Portanto, para devidamente informar o consumidor acerca da prática da publicidade comportamental e resguardar a sua liberdade de escolha, seria necessário um consentimento prévio do usuário em toda e qualquer ocasião

13. Brasil. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial nº 1.444.008/RS, Rel. Ministra Nancy Andrighi, julgado em 25/10/2016, DJe 09/11/2016.

em que a plataforma enviasse tais anúncios. Dito de outra forma, antes do *Google* enviar uma publicidade comportamental ao consumidor, este deveria ser informado de quais dados pessoais a plataforma analisou para decidir acerca do envio.

Se por exemplo uma pessoa, endividada e tendo a compulsão para compra de itens supérfluos, recebesse a informação de que iria receber dezenas de novos anúncios de produtos em decorrência de seu perfil digital de pessoa consumista, isto poderia levá-la à decisão de não mais consentir com o tratamento de seus dados pessoais, deixar de usar o *Gmail* e, até mesmo, parar de usar o cartão de crédito até quitar suas dívidas.

Na Ação Civil Pública nº 0025463-45.2016.4.01.4000 destacou-se ainda o precedente da Autoridade de Proteção de Dados Pessoais da Itália (*Garante Per La Protezione Dei Dati Personali*) que rejeitou o argumento do *Google* de que a concordância com os termos de serviço seria suficiente para configurar a existência de um consentimento expresso e destacado ao tratamento de dados pessoais e determinou, em julho de 2014, que o consentimento prévio informado seria condição para o processamento automatizado de dados pessoais dos usuários da *Gmail* para fins de criação de perfil e consequente veiculação de anúncios comportamentais.[14]

Conforme notícia de julho de 2016, o *Google* cumpriu as determinações da Autoridade de Proteção de Dados Pessoais da Itália ao adotar um mecanismo de escolha destacada e expressa, pois, por meio da apresentação de um *banner*, a solicitação de consentimento passou a ser repetida por três vezes no decorrer de dois meses, levando até mesmo o bloqueio do acesso aos serviços caso a escolha não seja feita. Além disso, os usuários poderiam negar o consentimento ou liberar o consentimento parcial no que diz respeito aos diferentes fins para os quais os dados podem ser usados, tendo, inclusive, a possibilidade de desativar o recebimento de publicidade direcionada.[15]

Por fim, o Ministério Público Federal ressaltou que a reiterada prática do tratamento de dados pessoais dos usuários do *Gmail* para construção de perfis e envio de anúncios comportamentais sem o consentimento expresso e destacado dos consumidores, além de violar dispositivos do Marco Civil da Internet e do Código de Defesa do Consumidor, gerou dano moral a coletividade de consumidores do referido serviço que estavam tendo sua privacidade e o livre desenvolvimento de sua personalidade tolhidos pela atividade da empresa.

---

14. Italia. GPDP, Garante per la Protezione dei Dati Personali. Decision setting forth measures Google Inc. is required to take to bring the processing of personal data under Google's New Privacy Policy into line with the Italian Data Protection Code. Disponível em <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3295641>.

15. Italia. GPDP, Garante per la Protezione dei Dati Personali. Google adempie agli impegni presi con il Garante italiano e migliora le sue politiche di privacy. Disponível em <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5305211>.

Neste sentido, o MPF requereu em sede liminar a suspensão da análise do conteúdo dos *e-mails* dos usuários no território nacional do *Gmail* enquanto não fosse colhido o consentimento prévio, expresso e destacado do titular da conta de *e-mail*, inclusive para o envio de publicidade comportamental, sob pena de multa diária no valor de R$ 100.000,00 (cem mil reais), bem como, nos termos artigo 7°, IX do Marco Civil da Internet, a condenação do *Google* na obrigação de, em todo o território nacional, apenas analisar o conteúdo de *e-mails* dos usuários do *Gmail* mediante consentimento prévio, expresso e destacado, assegurando ainda que a qualquer momento o usuário poderia revogar a autorização. Por fim, o MPF requereu a condenação do *Google* por dano moral coletivo, em razão do período em que analisou os *e-mails* dos usuários do *Gmail* para envio de publicidade comportamental sem consentimento expresso e destacado, no valor de 1.000.000,00 (um milhão de reais).

Em sede de contestação o *Google* aduziu cumprir a legislação brasileira no que se refere à coleta de consentimento expresso, em documento separado, destacado em janela específica, dos usuários do *Gmail*, antes da leitura automatizada do conteúdo dos *e-mails*, podendo o usuário revogar o consentimento para coleta de dados e cancelar o recebimento de anúncios direcionados. Ponderou que não ocorria compartilhamento das informações colhidas com terceiros e que o caso ocorrido na Itália não seria semelhante ao brasileiro, pois teria ocorrido uma alteração na Política de Privacidade a nível global apta a beneficiar os usuários do *Gmail.* Argumentou que o Poder Judiciário não é foro adequado para discussão de políticas regulatórias complexas, que a Justiça Federal não teria competência para julgar a demanda e o que o Ministério Público Federal não teria atribuição ajuizar a ação. Aduziu ainda a ausência de interesse processual, pois o *Google* já teria cumprido o que havia sido pedido na ação, de modo que não teria ocorrido dano moral coletivo e não estariam presentes os requisitos para tutela de urgência ou evidência.[16]

Por sua vez, o Ministério Público Federal asseverou que a Secretaria Nacional de Defesa do Consumidor (SENACON) já havia instaurado procedimento de averiguação para apurar o desatendimento da regra do artigo 7°, IX do Marco Civil da Internet pelo *Gmail*, de modo que o interesse direto de órgão federal no objeto da lide tornava competente a Justiça Federal. Quanto a atribuição do Ministério Público Federal, destacou o disposto no artigo 51, §4° do Código de Defesa do Consumidor acerca de sua legitimidade para propor ação anulatória de cláusula contratual abusiva ou ilegal.

No mérito, ressaltou que o *Google* confessou que "nossos sistemas automatizados analisam o conteúdo do usuário (incluindo e-mails)" e,

16. O resumo da contestação do Google está no início da minuta de contrarrazões do Ministério Público Federal disponível em <https://www.dropbox.com/s/pwgsye5fq2wk4pu/R%C3%A9plica%20GOOGLE.pdf?dl=0>.

quanto à alegação de que "o consumidor, ao abrir uma conta *Google*, precisa concordar expressamente, em janela específica para tal, com o uso dos dados" aduziu a Secretaria de Apoio Pericial da Procuradoria Geral da República elaborou parecer técnico demonstrando que o texto dos termos de uso eram apresentados em bloco, sem destaque para a atividade da coleta de dados.

A informação sobre a análise de conteúdo dos *e-mails* encontrava-se no meio de um longo documento, de modo que poucos consumidores visualizariam tal cláusula. Portanto, nos termos do parecer técnico, o MPF reforçou que, no processo de criação de conta *Google*, o consentimento ao tratamento de dados pessoais ocorria de forma conjunta, isto é, sem ser expressa e destacada a cláusula que informava da leitura do conteúdo das mensagens enviadas e recebidas no *Gmail*, violando os deveres de informação dispostos no artigo 6º, III e 8º do Código de Defesa do Consumidor, bem como a exigência de destaque para cláusula limitadora de direitos estipulada no artigo 54, §4º do referido código.[17]

Em julho de 2017 a Justiça Federal no Estado do Piauí decidiu acerca do pedido liminar do Ministério Público Federal, indeferindo-o por considerar que inexistiria nos autos comprovação de violação da privacidade da coletividade de consumidores do *Gmail* com a leitura do conteúdo de seus *e-mails*. Ponderou que ao abrir uma conta *Google*, o usuário precisaria, em janela específica, concordar expressamente com a política de privacidade da empresa e que, em cognição sumária, a atuação do *Google* não deixaria o consumidor em posição de desvantagem. Por fim, considerou que não haveria risco de dano pois o consumidor poderia a qualquer tempo revogar o consentimento para a coleta de dados excluindo sua conta.[18] Contra esta decisão o Ministério Público Federal apresentou agravo de instrumento, autuado no Tribunal Regional Federal da 1ª Região sob o número 0037191-21.2017.4.01.0000, mas que foi julgado prejudicado após ter sido prolatada a sentença de mérito.

Quanto à sentença de mérito, proferida em janeiro de 2018, julgou-se improcedente o pedido ministerial com a fundamentação de que a matéria já teria sido enfrentada na decisão que indeferiu o pedido liminar. Remetendo-se apenas à referida decisão, o Juízo aduziu que não teria sido comprovada invasão de privacidade dos usuários do *Gmail* e que, ao abrir uma conta, os consumidores precisariam concordar expressamente com o uso de dados. Ponderou ainda que o *Google* teria informado que a versão corporativa do serviço *Gmail* não mais era usada para personalização de anúncios e os

17. A íntegra das contrarrazões do Ministério Público Federal disponível em <https://www.dropbox.com/s/pwgsye5fq2wk4pu/R%C3%A9plica%20GOOGLE.pdf?dl=0>.

18. A íntegra da decisão está disponível na aba inteiro teor da consulta do processo 0025463-45.2016.4.01.4000 em <https://processual.trf1.jus.br/consultaProcessual/numeroProcesso.php?secao=PI>

consumidores poderiam desativar tal função.[19] Cabe destacar que enquanto a inicial da Ação Civil Pública teve vinte e quatro laudas com fundamentação na Constituição Federal, Código de Defesa do Consumidor, Marco Civil da Internet e até mesmo em precedente da Autoridade de Proteção de Dados Pessoais da Itália, a referida sentença teve quatro laudas, sendo quase três delas utilizadas com cópia *ipsis litteris* da decisão liminar que, cabe ressaltar, aduziu apenas em cognição sumária que a atuação do *Google* não deixaria o consumidor em posição de desvantagem.

Contra esta decisão o Ministério Público Federal interpôs tempestivamente em fevereiro de 2018 recurso de apelação com pedido de tutela de urgência e evidência para que o *Google* informasse de forma expressa no momento da criação da conta do consumidor que: "Nós fazemos uma leitura automática de seus e-mails, por questões operacionais e de segurança. Essa inspeção não pode ser desativada pelo usuário".

Além disso, requereu o provimento do recurso para fosse reconhecida a nulidade da sentença de primeira instância por ausência de fundamentação, passando ao Tribunal a análise do mérito. Na fundamentação do recurso, destacou-se, nos termos do artigo 489, §1°, IV do Código de Processo Civil (Lei Federal n° 13.105/2015), que a sentença não teve fundamentação, pois não enfrentou os argumentos deduzidos no processo. Ao invés disso, simplesmente transcreveu a decisão que negou o pedido liminar que, por sua vez, não analisou a prova pericial de parecer técnico produzido Secretaria de Apoio Pericial da Procuradoria Geral da República. No mérito, asseverou que a empresa entrou em contradição ao aduzir não verificar nem ler as mensagens do *Gmail*, pois esta já havia explicitamente registrado nos autos a continuidade da análise de *e-mails* por motivos operacionais e de segurança. Destacou-se ainda que apesar do *Google* ter alegado que deixaria de ler *e-mails* para fins de envio de publicidade, não juntou prova, ao passo que o parecer técnico ministerial demonstrou a impossibilidade de desativar a referida análise automatizada.[20]

O Ministério Público Federal aduziu que o *Google* ilude e engana os consumidores do Gmail ao omitir informações sobre a atividade de monitoramento, de modo a violar o disposto no artigo 7°, VI do Marco Civil da Internet e artigo 6°, III do Código de Defesa do Consumidor. Ressaltou que a janela mencionada na decisão que negou o pedido liminar como específica para concordância com a atividade da leitura do conteúdo dos e-mails não passava de um dos tópicos da política de privada, inserido sem qualquer destaque.

19. A íntegra da sentença está disponível na aba inteiro teor da consulta do processo 0025463-45.2016.4.01.4000 em <https://processual.trf1.jus.br/consultaProcessual/numeroProcesso.php?secao=PI>

20. A íntegra da apelação está disponível em <https://www.dropbox.com/s/1g4dtl0nu0y5lpd/25463-45.2016%20apelacao%20google.pdf?dl=0>.

Por fim, ponderou-se que o dano à coletividade não estava adstrito à publicidade comportamental enviada pelo *Google*, mas pela leitura do conteúdo dos e-mails dos consumidores sem seu consentimento destacado e expresso, sendo papel do Ministério Público Federal defender o interesse da coletividade em especial que quando os prejudicados se encontram em situação de vulnerabilidade fática, técnico e informacional. A apelação atualmente encontra-se tramitando perante o Tribunal Regional Federal da 1ª Região, ainda sem decisão.

De todo modo, a entrada em vigor do artigo 9º, §3º da Lei Geral de Proteção de Dados Pessoais pacificou o direito do titular de dados pessoais ser informado com destaque, caso o atividade de tratamento destes seja condição para o fornecimento de serviço, sobre esse fato e sobre os meios para exercer seus direitos. Portanto, caso o *Google* continue com a atividade de análise de mensagens dos usuários serviço *Gmail* sem obter o consentimento expresso, destacado e devidamente informado de seus consumidores, o Juízo de segundo grau tende a deferir o pedido ministerial em prol da coletividade afetada.

5. CONCLUSÃO

O acesso à internet traz desafios que envolvem a privacidade dos titulares de dados pessoais e as responsabilidades das principais empresas de tecnologia. Muitos novos usuários podem não entender completamente como seus dados estão sendo utilizados por plataformas como *Facebook* e *Google*. Essa falta de conhecimento pode levar ao consentimento não totalmente informado para o uso de dados para publicidade direcionada, que é a principal fonte de receita para essas empresas.

A necessidade de inclusão digital não pode justificar o desrespeito a Lei Geral de Proteção de Dados Pessoais, bem como ao artigo 5º, LXXIX da Constituição Federal. É certo que a falta de conexão à internet pode dificultar o acesso a informações e recursos, consolidando ainda mais as desigualdades sociais. Todavia, isto não permite que empresas privadas forneçam um acesso suspostamente gratuito, como o *Facebook* buscou implementar com o *internet.org*, com potencial de agravar a situação de vulnerabilidade dos indivíduos.

Além disso, para os cidadãos brasileiros que tem acesso à internet por meio de assinaturas ou laboratórios de informática estatais, a suposta gratuidade de serviços como o de correio eletrônico também não permite que empresas atuem sem adequação à LGPD. Conforme demonstrado no presente artigo, o *Google*, em seu serviço *Gmail*, não informava adequadamente os usuários sobre as especificidades do processamento de dados, particularmente na criação de perfis digitais para fins publicitários.

O Ministério Público Federal teve papel fundamental nos dois casos analisados, demonstrando a necessidade do respeito à Lei para garantir

que as empresas obtenham o consentimento explícito e informado dos usuários antes de processar seus dados pessoais. Com o aumento da conscientização dos cidadãos brasileiros acerca dos riscos dos anúncios comportamentais enviados por plataformas "gratuitas", maior será o número de representações ao Ministério Público Federal em face de tais plataformas, criando um ciclo virtuoso de combate ao tratamento de dados pessoais inadequado.

6. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Almeida, Daniel Evangelista Vasconcelos; **De Almeida**, Juliana Evangelista. Uma análise crítica do internet.org como uma prática de difusão de acesso à rede mundial de computadores. *Revista de Direito, Governança e Novas Tecnologias*, v. 2, n. 1, p. 148-166, 2016.

Brasil. Instituto Brasileiro de Geografia e Estatística. *Síntese de indicadores sociais: uma análise das condições de vida da população brasileira: 2019* / IBGE, Coordenação de População e Indicadores Sociais. - Rio de Janeiro: IBGE, 2019.

Brasil. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial nº 1.193.764/SP, Rel. Ministra Nancy Andrighi, julgado em 14/12/2010, DJe 08/08/2011.

Brasil. Superior Tribunal de Justiça (Terceira Turma). Recurso Especial nº 1.444.008/RS, Rel. Ministra Nancy Andrighi, julgado em 25/10/2016, DJe 09/11/2016.

Castells, Manuel. *Sociedade em rede*. São Paulo, SP: Paz e Terra, 2019.

César, Daniel; **Junior**, Irineu Francisco Barreto. Marco Civil da Internet e Neutralidade da Rede: aspectos jurídicos e tecnológicos. *Revista Eletrônica do Curso de Direito da UFSM*, v. 12, n. 1, p. 65-88, 2017. p. 67.

Cgi, Comitê Gestor da Internet no Brasil. Painel TIC COVID-19: Pesquisa sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus - 3ª edição: *Ensino remoto e teletrabalho*. Novembro de 2020.

Cgi, Comitê Gestor da Internet no Brasil. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC domicílios 2018. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2019.

Furtado, Gabriel Rocha; **Bezerra**, Daniel Teixeira. Privacidade, consentimento informado e proteção de dados do consumidor na internet. In: *Revista de Direito do Consumidor*. vol. 128. ano 29. São Paulo: Ed. RT, mar./abr. 2020. p. 205-225.

ITALIA. GPDP, *Garante per la Protezione dei Dati Personali. Decision setting forth measures Google Inc. is required to take to bring the processing of personal data under Google's New Privacy Policy into line with the Italian Data Protection Code*. Disponível em <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3295641>.

ITALIA. GPDP, *Garante per la Protezione dei Dati Personali. Google adempie agli impegni presi con il Garante italiano e migliora le sue politiche di privacy*. Disponível em https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5305211.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 2010.

MACIEL, Ira Maria. Inclusão digital: experiências e desafios com tecnologias de informação e comunicação. *Revista Teias*, [S.l.], v. 2, n. 3, p. 13 pgs., ago. 2007. ISSN 1982-0305. Disponível em https://www.e-publicacoes.uerj.br/index.php/revistateias/article/view/23876/16849.

KOSINSKI, Michal *et. al*. *Computer-based personality judgments are more accurate than those made by humans. Proceedings Of The National Academy Of Sciences*, [S.L.], v. 112, n. 4, p. 1036-1040, 12 jan. 2015. Proceedings of the National Academy of Sciences.

SARLET, Ingo Wolfgang; **MOLINARO**, Carlos Alberto. O direito à informação na ordem constitucional brasileira: breves apontamentos. In: SARLET, Ingo W.; MARTOS, José A. M.; RUARO, Regina L. (coord.). *Acesso à informação como direito fundamental e dever estatal*. Porto Alegre: Livraria do Advogado Editora, 2016.

SILVA, Alexandre Assunção e. *Sigilo das comunicações na internet*. Curitiba: Juruá, 2017.

A ESPETACULARIZAÇÃO DAS GRAVAÇÕES AUDIOVISUAIS DE AUDIÊNCIAS (JUDICIAIS) REALIZADAS COM A PARTICIPAÇÃO DO MINISTÉRIO PÚBLICO

Ana Paula Machado Franklin[1]
Carlos Renato Silvy Teive[2]
Guilherme Magalhães Martins[3]

Resumo: Os avanços tecnológicos ocorridos, sobretudo a partir do final do século XX, implicaram aumentos exponenciais na capacidade de coleta, processamento e compartilhamento de dados. Neste contexto, verifica-se a necessidade, cada vez maior, de se protegerem os dados pessoais, em especial nas audiências judiciais. Nestes atos, som e imagem de pessoas naturais são frequentemente coletados, editados e publicados em redes sociais, em afronta ao direito fundamental em questão, espetacularizando o ato com nítido propósito de promoção pessoal e/ou comercial. Para coibir essa prática, mostra-se necessária uma regulamentação específica, por exemplo, como a já existente na Espanha.

---

1. Promotora de Justiça do Estado de Goiás e Encarregada pelo Tratamento de Dados Pessoais do Conselho Nacional do Ministério Público. Integrante da Unidade Especial de Proteção de Dados Pessoais do CNMP. Pós-graduada pela Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Especialista em Proteção de Dados Pessoais pela Universidade de Santiago de Compostela (USC).

2. Promotor de Justiça e Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado de Santa Catarina. Mestre em Direito pela Universidade Veiga de Almeida do Rio de Janeiro. Pós-graduado em Proteção de Dados: LGPD e GDPR pela Faculdade de Direito da Fundação Escola Superior do Ministério Público. Especialista em Proteção de Dados Pessoais pela Universidade de Santiago de Compostela (USC). Integrante da Unidade Especial de Proteção de Dados do CNMP.

3. Procurador de Justiça e Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado do Rio de Janeiro. Professor associado de Direito Civil da Faculdade Nacional de Direito – Universidade Federal do Rio de Janeiro. Professor permanente do Doutorado em Direitos, Instituições e Negócios da Universidade Federal Fluminense e do Mestrado em Direito da Universidade Candido Mendes-Centro. Pós-doutor em Direito Comercial pela Faculdade de Direito da USP. Doutor e Mestre em Direito Civil pela Faculdade de Direito da UERJ.

Palavras-chave: Avanços tecnológicos. Proteção dados pessoais. Audiências judiciais. Gravações. Espetacularização. Regulamentação.

Resumen: Los avances tecnológicos ocurridos, sobre todo a partir del final del siglo XX, implicaron aumentos exponenciales en la capacidad de recolección, procesamiento y compartición de datos. En este contexto, se verifica la necesidad, cada vez mayor, de proteger los datos personales, especialmente en las audiencias judiciales. En estos actos, el sonido y la imagen de personas naturales son frecuentemente recolectados, editados y publicados en redes sociales, en afrenta al derecho fundamental en cuestión, espectacularizando el acto con un claro propósito de promoción personal y/o comercial. Para frenar esta práctica, se muestra necesaria una regulación específica, por ejemplo, como la ya existente en España.

Palabras clave: Avances tecnológicos. Protección de datos personales. Audiencias judiciales. Grabaciones. Espetacularización. Regulación.

1. INTRODUÇÃO

É fato que os avanços tecnológicos, ocorridos sobretudo nos últimos anos, fizeram com que houvesse um avanço exponencial na capacidade de coleta, processamento e compartilhamento de dados[4]. Nesse contexto, cresce em todo mundo, e também no Brasil, a preocupação em se protegerem os dados pessoais – tais como voz e imagem – das pessoas naturais.

Os frutos da sociedade da informação são facilmente visíveis, com *smartphones* em cada bolso, computadores em cada mochila e grandes sistemas de tecnologia na retaguarda de toda e qualquer organização. Mas menos perceptível é a informação em si.

Meio século depois que os computadores ingressaram na sociedade convencional, os dados começaram a se acumular, de modo que algo novo e especial passa a tomar lugar. Não apenas o mundo é inundado com mais

4. A quantidade total de dados criados, capturados, copiados e consumidos globalmente está prevista para aumentar rapidamente, alcançando 149 zettabytes em 2024. Nos próximos cinco anos, até 2028, a criação global de dados deverá crescer para mais de 394 zettabytes. Em 2020, a quantidade de dados criados e replicados atingiu um novo recorde. O crescimento foi maior do que o esperado anteriormente, causado pelo aumento da demanda devido à pandemia de COVID-19, já que mais pessoas trabalharam e estudaram em casa e usaram opções de entretenimento doméstico com mais frequência. Disponível em: <https://www.statista.com/statistics/871513/worldwide-data-created/#statisticContainer>. Acesso em 02 fev. 2025.

informações do que em qualquer época anterior, mas essa informação se torna mais rápida e precisa. Determinadas ciências, como a Astronomia e o Genoma, que em primeiro lugar passaram por um salto qualitativo a partir de um salto quantitativo, primeiramente cunharam o termo "*Big Data*". Atualmente, o conceito migrou para todas as áreas do conhecimento humano (Mayer-Schönberger e Cukier, 2014, p. 6; Martins, 2022, p. 32).

O que caracteriza o "*Big Data"* é a quantidade de dados criados, o número de associações que permitem o seu rastreamento por *sites* e plataformas e crescentes mercados de dados e colaborações nas quais essa informação é compartilhada entre os envolvidos (Jones, 2016, p. 7).

Como reação a esse processamento massivo de dados pelas novas tecnologias e suas implicações no campo da privacidade, foi editada no Brasil a chamada Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709/18), inspirada no Regulamento Europeu de Proteção de Dados Pessoais (GDPR), que tem por escopo garantir a proteção dos dados pessoais dos indivíduos.

Pouco tempo após a entrada em vigor da referida norma, a proteção de dados pessoais foi alçada à categoria de direito fundamental expresso, por meio da EC n. 115/2022, aprovada por unanimidade em ambas as Casas do Congresso Nacional, como uma resposta à necessidade de regulação, pelo Direito, dos fatos emergentes do uso de novas tecnologias e das novas condutas sociais, reforçando a ideia de contemporaneidade fático-jurídica de Habermas (1997, p. 17-48) que definia "Direito como categoria de mediação social entre facticidade e validade".

Além da sensibilidade do Poder Legislativo ao tema, outro marco digno de destaque na evolução jurisprudencial do tema no Brasil, foi o julgamento da ADI n. 6387 em 2020 em que o STF, antes mesmo da aprovação da referida emenda constitucional, já reconhecia o caráter de direito fundamental à proteção de dados pessoais[5] e sua natureza mutável com a evolução tecnológica e social[6].

---

5. "2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados". (STF, ADI 6387, Rel.Min.Rosa Weber, j. 07/05/2020).

6. [...] No clássico artigo *The Right to Privacy*, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, originalmente publicado no volume 193 da *Harvard Law Review* (1890), considerado pioneiro ao estabelecer um marco na doutrina do direito à privacidade, além de ser de certa forma profético ao antecipar a importância que a matéria viria a assumir com o desenvolvimento das tecnologias da informação que então já começavam a se fazer sentir. Disponível em: <www.louisville.edu/library/law/brandeis/privacy.html>. Acesso em: 17 maio 2006. Ali se

No campo da normatização pode-se destacar, ainda, a aprovação pelo Conselho Nacional do Ministério Público (CNMP), da Resolução nº 281/2023 que instituiu a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público brasileiro, como instrumento normativo basilar de regulação da contemporânea realidade social informacional.

Ocorre que a despeito dessa rápida evolução legislativa, jurisprudencial e regulamentar no campo da proteção de dados pessoais, persistem desafios significativos relacionados à sua efetiva implementação, e a espetacularização das audiências judiciais com divulgação de registros audiovisuais em redes sociais representa um sintoma crítico dessa problemática, em que prevalece o sensacionalismo sobre a técnica jurídica, e a exposição inadequada de dados pessoais sobre a finalidade processual.

O presente artigo busca demonstrar – notadamente a partir das normas vigentes, da Orientação n. 001/2024/UEPDAP do CNMP e da legislação estrangeira, em especial espanhola – que a gravação por dispositivos particulares sem o consentimento dos titulares dos dados pessoais envolvidos (e, muitas vezes, sem sequer ciência destes), e a posterior divulgação desse conteúdo audiovisual em redes sociais em completo desvirtuamento da finalidade do registro, é uma prática que afronta o direito fundamental à proteção de dados pessoais, além de colocar em xeque o princípio da verdade real.

2. DA PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS

Embora não seja o propósito deste artigo fazer uma abordagem ampla acerca da evolução histórica do tema, desde o seu surgimento até os dias atuais, tem-se que para melhor compreendê-lo, inclusive quanto à sua crescente importância, seja oportuno destacar alguns marcos sobre privacidade e proteção de dados pessoais e relacioná-los com a evolução tecnológica vivenciada no mundo, desde o final do século XIX.

Nessa esteira, a evolução do conceito jurídico de privacidade representa uma trajetória complexa de releitura dos direitos individuais, transitando de uma concepção inicial restritamente física para uma dimensão informacional contemporânea.

---

reconhecia que as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo. Independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Em seus dizeres, *ä invasão injustificada da privacidade individual deve ser repreendida e, tanto quanto possível, prevenida".* (STF, ADI 6387, j. 07/05/2020).

Inicialmente compreendida como "o direito de ser deixado só"[7] (*the right to be let alone*), ao longo do tempo a privacidade progressivamente ganhou contornos de um direito fundamental à autodeterminação informativa, especialmente no contexto digital, em que os dados pessoais adquirem valor econômico e estratégico.

A tensão histórica entre privacidade e publicidade constitui um dilema jurídico fundamental, caracterizado pela dialética permanente entre o direito individual à intimidade e o princípio constitucional da transparência. Essa dinâmica complexa manifesta-se especialmente nos espaços institucionais, onde a publicidade – elemento essencial ao regime democrático e ao controle social – frequentemente colide com a necessidade de preservação da intimidade e da vida privada dos sujeitos, exigindo permanente equacionamento hermenêutico dos operadores do direito para estabelecer limites e ponderações que garantam simultaneamente a publicidade dos atos e o respeito às garantias individuais.

Esse processo evolutivo decorre de uma construção jurídica dinâmica que busca equilibrar liberdades individuais, avanços tecnológicos e garantias fundamentais em um cenário de crescente complexidade informacional.

Como consequência dessa constante e inafastável tensão, a privacidade conta com um problema reputacional: costuma ser associada ao atraso e à aversão ao progresso, à segurança nacional e à eficiência (Martins e Ramos, 2022, p. 124-125; Cohen, 2013, p. 1905). Esta má fama é tributária de uma inversão conceitual relacionada à cunhagem do propósito da privacidade, cara à afirmação do direito de o indivíduo ser deixado só[8]. Não por acaso,

---

7. Este conceito foi formalmente articulado pela primeira vez no famoso artigo "The Right to Privacy" de Samuel Warren e Louis Brandeis, publicado em 1890.

8. A expressão foi utilizada pelo Justice Louis D. Brandeis, em seu célebre voto no julgamento do caso *Olmstead v. United States*, pela Suprema Corte estadunidense. Disse ele, *in verbis*: "Os elaboradores de nossa Constituição se esforçaram para garantir condições favoráveis à busca da felicidade. Eles reconheceram a significância da natureza espiritual do homem, de seus sentimentos e de seu intelecto. Eles sabiam que somente uma parte das dores, prazeres e satisfações da vida podem ser encontradas nos bens materiais. Eles procuraram proteger os americanos em suas crenças, pensamentos, emoções e sensações. Eles conferiram, contra o Governo, o direito a ser deixado só – o mais abrangente dos direitos e o direito mais valorado pelo homem civilizado. Para proteger tal direito, toda intrusão injustificável do Governo na privacidade do indivíduo, qualquer que seja o meio empregado, deve ser considerado uma violação à Quarta Emenda. E o uso, como prova, no processo penal, de fatos apurados por tal intrusão devem ser considerados violadores da Quinta Emenda" (Dissenting opinion of Justice Louis D. Brandeis in Olmstead v. United States. In: Hamm, R. F. *Olmstead v. United States*: the Constitutional Challenges of Prohibition Enforcement. Washington DC: Federal Justice Center, 2010, p. 64). Tradução livre. No original: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government,

Rodotà (2008, p. 13) aponta que "exigências de segurança interna e internacional, interesses de mercado e a reorganização da administração pública estão levando à diminuição de salvaguardas importantes, ou ao desaparecimento de garantias essenciais". Esta perda de tônus culmina com as recorrentes afirmações de que *a privacidade está morta*.

Dissociada desse vetusto suporte, a privacidade se revela, ao contrário, como um motor do desenvolvimento e como instrumento de proteção de um *self* construído socialmente. E assim é porque, segundo Cohen (2013, p. 1905), ela "resguarda subjetividades dinâmicas e emergentes contra os esforços de atores governamentais para tornar indivíduos e comunidades fixos, transparentes e previsíveis"[9]. Nessa ordem de ideias, a privacidade é curial ao enfrentamento dos problemas do presente, já que, conforme Rodotà (2008, p. 15), "indivíduos estão cada vez mais transparentes e [...] órgãos públicos estão mais e mais fora de qualquer controle".

A renovação das preocupações concernentes ao sentido de privacidade para o Direito e aos instrumentos que este oferece a sua proteção e promoção se justifica diante do crescimento do acesso à (e da dependência da) tecnologia. Isso porque ela tem uma espécie de rosto de Jânus: ao tempo em que contribui para a moldagem de uma esfera privada mais rica, importa sua crescente fragilização e exposição a ameaças. Aí está, portanto, nas palavras de Rodotà (2008, p. 95) "a necessidade do fortalecimento contínuo de sua proteção jurídica, da ampliação das fronteiras do direito à privacidade".

Como ressaltou Rodotà (2012, p. 26), o corpo não se limita ao "perímetro delineado pela pele", devendo ser considerado para a formação da identidade a reunião de dados pessoais que fluem no ciberespaço sobre um determinado sujeito, constituindo seu "*corpo elettronico*".

Dados pessoais que servirão de *input* para algoritmos voltados à tomada de decisões automatizadas e perfilamento de indivíduos, em situações que podem afetar substancialmente os interesses das pessoas, como acesso ao mercado de trabalho, contratação de empréstimo e seguros de saúde, entre outros, demonstram a importância de compreender os novos veios da tutela da privacidade, na medida em que esta já não se volta somente à reserva e ao isolamento, mas à construção de uma esfera pessoal na qual seja possível a liberdade de escolha, e, consequentemente, o desenvolvimento da personalidade.

---

the right to be l*et a*lone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth".

9. Tradução livre. No original: "*Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent and predictable*".

A proteção de dados tem um enfoque puramente objetivo, não envolvendo os aspectos subjetivos como se opera na privacidade (Colombo, *in* Martins e Faleiros Júnior, 2024, p. 7). Finocchiaro (2012, p. 1-3), por sua vez, leciona que o direito à proteção de dados pessoais se refere ao direito do sujeito exercitar um controle ativo sobre seus próprios dados, envolvendo o direito ao acesso e à sua retificação, enquanto o direito à "riservatezza" se volta à vida privada, familiar, ao domicílio e às comunicações (Rodottà, 2012, p. 26).

Com efeito, a partir desta correlação – tecnologia e privacidade/proteção de dados pessoais – pode-se melhor visualizar que a evolução tecnológica está diretamente relacionada com o surgimento e desenvolvimento deste direito, bem como com a necessidade de, cada vez mais, tutelá-lo.

Nessa senda, um dos seus primeiros marcos foi a publicação, em 15 de dezembro de 1890, na *Harvard Law Review*, do artigo intitulado *The Right to Privacy*, de autoria de Samuel Warren e Louis Brandeis. Nele, os autores já destacavam que mudanças sociais, políticas e econômicas, bem como o surgimento de novos inventos, (fotografia instantânea), demandam o reconhecimento de novos direitos[10].

Ocorre que à época, o direito à privacidade entendido como um direito individualista, estático, patrimonialista e de não intervenção era suficiente para garantir ao indivíduo sua liberdade contra intromissões indesejadas.

Entretanto, o contínuo avanço tecnológico vivenciado no mundo, em que a capacidade de coleta, processamento e armazenamento de dados vêm crescendo de forma exponencial, notadamente nas últimas décadas, implica alterações fáticas substanciais de forma a ser insuficiente a tutela da privacidade, apenas nos moldes cunhados no final do século XIX.

Assim, a partir do momento em que se inicia um maior desenvolvimento da tecnologia da informação, permitindo uma maior capacidade de processamento de dados, com potencial de transformar dados brutos em informações valiosas, a partir do uso de computadores mais eficientes,

10. "Zanon (2013, p. 40) ressalta que foi Thomas McIntyre Cooley (1824-1898), jurista norte-americano e Presidente da Suprema Corte de Michigan, quem cunhou, em 1888, a expressão *o direito de estar só* (*the right to bel et alone*). No entanto, por mais que a noção de privacidade não seja de todo recente, fato é que o impulso dado ao tema por Warren e Brandeis serviu para valorizar e chamar a atenção para esse direito em gestação, de forma autônoma e protagonista. Motivado pela divulgação não autorizada, nos jormais da época, de determinados fatos íntimos acerca do casamento de sua filha, Samuel Warren (que veio a se tornar juiz da Suprema Corte dos EUA), juntamente com Louis Brandeis deu vazão à construção da doutrina do *right to privacy*, em moldes adequados às necessidades da sociedade burguesa norte-americana do final do século XIX (Doneda, 2000, p. 2)" (Vieira de Lorenzi Cancelier, Mikhail. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. Seqüência Estudos Jurídicos e Políticos, Florianópolis, v. 38, n. 76, p. 5, 2017. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213>. Acesso em: 7 fev. 2025.

surge, especialmente na Europa, a percepção quanto à necessidade de se tutelarem os dados pessoais dos indivíduos, sendo digno de registro o primeiro compromisso internacional juridicamente vinculante sobre proteção de dados pessoais: a Convenção nº 108 do Conselho da Europa, em 28 de janeiro de 1981.

Nessa linha evolutiva tecnológica vivenciada desde o final do século XX – de computadores com capacidade de processamento de dados cada vez maior; em que a internet viabiliza a disseminação de conteúdo de forma instantânea para bilhões de pessoas; em que as redes sociais revolucionam a comunicação e a interação social; em que os smartphones, além de possuírem grande capacidade de processamento de dados, são capazes de coletar som e imagem em excelente qualidade, transformando qualquer pessoa em potencial produtor de conteúdo; em que câmeras afixadas em locais públicos são capazes de capturar e processar expressões faciais para fins comerciais e publicitários; em que lidamos com o uso crescente da inteligência artificial – as normativas para tutelar a proteção de dados pessoais também precisaram avançar, assim como precisa evoluir a interpretação a ser dada às normas aplicáveis.

Quanto às normas, sem propósito exauriente, no âmbito europeu, pode-se destacar a Diretiva nº 95/46 (1995); a Carta de Direitos Fundamentais da União Europeia (2000), que já previa expressamente a proteção de dados pessoais como um direito fundamental em seu art. 8º; o Regulamento Geral sobre Proteção de Dados nº 2016/679 e, especificamente no tocante à proteção de dados pessoais nas gravações audiovisuais em processos judiciais na Espanha, o Decreto-Lei nº 6/2023.

No Brasil, conforme já mencionado, temos como principais marcos normativos a LGPD (Lei nº 13.709/18) e a EC nº 115/2022, além de outras normas específicas, como a Resolução do Conselho Nacional do Ministério Público n. 281/2023.

Enfim, antes de se analisar propriamente as normas aplicáveis ao tratamento de dados pessoais consistente nas gravações audiovisuais de audiências judiciais, bem como a Orientação nº 01/2024/UEPDAP do CNMP e a normativa espanhola que disciplina de forma específica a questão, entende-se importante fazer essa contextualização, encerrando-a, mais uma vez, com um trecho do voto da Ministra Rosa Weber, proferido em 07/05/2020, no julgamento da ADI nº 6387, que corrobora o exposto:

> [...] Certamente há quem ainda se lembre de que há poucas décadas, antes da ubiquidade da telefonia móvel, era comum a edição de listas telefônicas impressas contendo nomes, telefones e endereços dos assinantes residenciais e comerciais dos serviços de telefonia em uma dada localidade. Além de ser facultado aos usuários dos serviços de telefonia em uma dada localidade. Além de ser facultado aos usuários dos serviços de telefonia optarem pela exclusão dos próprios dados dessas listas, é crucial ter presente que o que podia ser feito a

> partir da publicização de tais dados pessoais não se compara ao que pode ser feito no patamar tecnológico atual, em que poderosas tecnologias de processamento, cruzamento e filtragem de dados permitem a formação de perfis individuais extremamente detalhados (Grifou-se).

3. A SOCIEDADE DO ESPETÁCULO: DAS GRAVAÇÕES AUDIOVISUAIS DE AUDIÊNCIAS JUDICIAIS E A PROTEÇÃO DE DADOS PESSOAIS

O compromisso com a ética e veracidade pelos meios de comunicação ocorre no contexto que Llosa (2013, p. 277) denomina civilização do espetáculo, ou seja, "a civilização de um mundo onde o primeiro lugar na tabela de valores vigente é ocupado pelo entretenimento, onde divertir-se, escapar do tédio, é a paixão universal. Esse ideal de vida é perfeitamente legítimo, sem dúvida. Só um puritano fanático poderia reprovar os membros de uma sociedade que quisessem dar descontração, relaxamento, humor e diversão a vidas geralmente enquadradas em rotinas deprimentes e às vezes imbecilizantes. Mas transformar em valor supremo essa propensão natural a divertir-se tem consequências inesperadas: banalização da cultura, generalização da frivolidade e, no campo da informação, a proliferação do jornalismo irresponsável da bisbilhotice e do escândalo" (Martins, 2022, p. 66).

Anteriormente, nos anos 1960, Debord (1997, p. 13) previu a sociedade do espetáculo, de modo que "as imagens que se destacaram de cada aspecto da vida fundem-se num fluxo comum, no qual a unidade dessa mesma vida já não pode ser restabelecida. A realidade considerada parcialmente apresenta-se em sua própria unidade geral como um pseudomundo à parte, objeto de mera contemplação".[11]

Na obra "A Sociedade do Espetáculo", o autor apresenta uma análise crítica da sociedade contemporânea, caracterizando-a como dominada pela lógica do espetáculo, onde as relações sociais são mediadas por imagens e representações. Esta sociedade, segundo Debord, caracteriza-se pela transformação da vida social em mercadoria, num contexto em que a aparência se sobrepõe à essência, e a representação substitui a experiência direta (Debord, 1997, p. 13).

Esse fenômeno de mercantilização da vida social se intensifica na era digital contemporânea, em que a espetacularização das relações sociais encontra

11. E prossegue o grande sociólogo francês: "A especialização das imagens do mundo se realiza no mundo da imagem autonomizada, no qual o mentiroso mentiu para si mesmo. O espetáculo em geral, como inversão concreta da vida, é o movimento autônomo do não-vivo".

nas redes sociais e mídias digitais seu ápice de manifestação e monetização. Não por acaso observa-se um crescente número de publicações de trechos de audiências judiciais em redes sociais, com o propósito de autopromoção ou depreciação de atores processuais, finalidades diversas daquelas que autorizaram a gravação do ato.

Posta assim a questão, é possível afirmar que a disseminação de gravações de audiências judiciais em redes sociais exemplifica de modo paradigmático a teoria de Debord sobre a sociedade do espetáculo, evidenciando a transformação do processo judicial em objeto de entretenimento midiático e de promoção pessoal.

De fato, a exposição seletiva de momentos processuais nas mídias digitais, frequentemente descontextualizados e editados para aumentar o engajamento, representa a materialização da lógica espetacular no âmbito jurídico, onde a busca por visibilidade e repercussão social sobrepõe-se aos princípios do devido processo legal e da proteção de dados pessoais dos sujeitos processuais, promovendo a mercantilização do cenário judicial na sociedade contemporânea.

Sem dúvida a gravação audiovisual das audiências judiciais representa um avanço à tutela jurisdicional, pois permite a realização do ato de forma mais célere e um registro mais fidedigno do conteúdo dos depoimentos das testemunhas em juízo, por exemplo, quando comparados à redução a termo dos depoimentos colhidos.

Isso porque aquele registro, além de permitir aos Promotores de Justiça, Magistrados e Advogados, que não participaram diretamente da colheita da prova, aferirem pela imagem e pelo áudio das testemunhas suas reações espontâneas e expressões, que muitas vezes não poderiam ser retratadas com a fria transcrição do conteúdo, evita registros equivocados das manifestações, e isso de forma mais rápida e eficiente.

Aliás, não por outra razão, tanto o Conselho Nacional de Justiça quanto o Conselho Nacional do Ministério Público expediram, respectivamente, a Recomendação nº 94/2021 e a Recomendação nº 92/2022 para recomendarem aos Tribunais brasileiros e aos ramos e unidades do Ministério Público brasileiro a adoção de medidas incentivadoras da prática da gravação dos atos processuais e dos atos instrutórios nos procedimentos administrativos em curso no Ministério Público.

Dessa forma, convém ressaltar não se está aqui a defender um retrocesso, ou seja, de que doravante não se realizem mais essas gravações de atos processuais em nome da proteção de dados pessoais.

Entretanto, é indubitável que as gravações audiovisuais desses atos, em que são coletados som e imagem de Promotores de Justiça, Magistrados, Advogados, Defensores Públicos, servidores, testemunhas, vítimas, réus, enfim, de todos que se encontram presentes no ato, caracterizam uma forma

de tratamento de dados pessoais, nos termos do art. 5º, X, da LGPD[12], e, como tal, devem observar o direito fundamental à proteção de dados pessoais (art. 5º, LXXIX, da CF) e as disposições previstas na LGPD.

Em razão do fenômeno crescente de exposição indevida de registros audiovisuais de atos processuais em redes sociais e aplicativos de mensagens, a Unidade Especial de Proteção de Dados Pessoais (UEPDAP), criada pela Resolução nº 281/2023 do CNMP, expediu a Orientação nº 001/2024/UEPDAP, com o objetivo de estabelecer parâmetros de atuação ministerial na tutela do direito à proteção de dados pessoais no contexto das gravações realizadas em audiências judiciais e procedimentos extrajudiciais.

Neste ponto, cumpre destacar que, não obstante a LGPD, em seu art. 4º, III, "d"[13], afaste de sua incidência o tratamento de dados pessoais realizado para fins exclusivos de "atividades de investigação e repressão de infrações penais", a própria norma ressalva, em seu art. 4º, § 1º, que "O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei".

Assim, não há dúvidas de que, tanto em razão da previsão como direito fundamental expresso no art. 5º, LXXIX da CF, quanto por disposição da própria lei ordinária, as gravações audiovisuais, sejam de processos cíveis, sejam de processos criminais, deverão observar os princípios gerais de proteção elencados no art. 6º da LGPD[14].

---

12. Art. 5º Para fins desta Lei, considera-se: [...]
X- tratamento: toda operação realizada com dados pessoais, como as 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;

13. Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...]
III- realizado para fins exclusivos de: [...]
d) atividades de investigação e repressão de infrações penais; ou

14. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Isso porque, para um tratamento de dados pessoais ser considerado regular não basta apenas existir hipótese legal que legitime o tratamento – no caso aquela prevista no art. 7º, VI e 11, II, "d", ambos da LGPD – mas também se faz necessário o respeito aos princípios gerais de proteção elencados no art. 6º da LGPD.

Nesse norte, colhe-se da Orientação nº 001/2024/UEPDAP do CNMP:

> CONSIDERANDO que o art. 367, do CPC, ao estabelecer a possibilidade de gravação de audiências cíveis diretamente pelas partes, não pode ser interpretado de maneira dissociada da nova ordem constitucional, por outras palavras, alheio à posterior e expressa previsão do art. 5º, LXXIX, da Constituição (inserido pela Emenda Constitucional 115/2022) relativa ao direito fundamental à proteção de dados pessoais, deve-se considerar a incidência de toda a carga principiológica do sistema brasileiro protetivo dos dados pessoais no tocante ao tratamento dos dados pessoais nos procedimentos investigatórios e nos processos judiciais, ou seja, as gravações somente devem ser possibilitadas com a finalidade específica de registro dos atos procedimentais e processuais ocorridos em audiências e para utilizações exclusivamente para as finalidades inerentes à atuação dos atores do sistema de Justiça;

A propósito, disciplinando de forma específica a Proteção de dados coletados em suporte audiovisual em processos judiciais, tem-se o artigo 67 do Decreto-Lei nº 6/2023 da Espanha, o qual prevê, em sua alínea "1", que, nos processos judiciais que se realizam de forma telemática, deverá ser respeitada a normativa vigente em matéria de proteção de dados.[15]

Dessa forma, restando esta premissa clara, incumbe analisar primeiro qual a finalidade das gravações audiovisuais realizadas nas audiências judiciais para, na sequência, abordar sua prática frente aos mencionados princípios.

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

15. Artículo 67. Control sobre la difusión de actuaciones telemáticas.
1. Las actuaciones judiciales que se realicen de forma telemática deberán respetar la normativa vigente em matéria de protección de datos.

Ora, é evidente que a finalidade desse tratamento de dados pessoais é registrar os atos processuais relevantes ao processo, em substituição à lavratura de termo do resumo da audiência.

Com efeito, a única norma processual brasileira que prevê expressamente essa gravação, inclusive diretamente pelas partes, é a contida no art. 367 do CPC, ou seja, inserida no Capítulo XI do Código de Processo Civil, que trata "Da audiência de Instrução e Julgamento".

Além disso, o *caput* do mencionado artigo 367 deixa muito claro que o dispositivo está regulando o registro dos atos relevantes da audiência, tanto que prevê que "O servidor lavrará, sob ditado do juiz, termo que conterá, em resumo, o ocorrido na audiência", possibilitando, contudo, em seu §§ 5º e 6º a gravação integral em imagem e áudio pelo juízo e diretamente pelas partes.

Assim, restando clara a finalidade da gravação audiovisual em questão, cabe, então, verificar em quais hipóteses esse tratamento de dados pessoais mostra-se consentâneo com os princípios gerais de proteção, notadamente com os da finalidade, adequação, necessidade, transparência, segurança e prevenção, além da boa-fé.

Sobre os princípios da finalidade, adequação e necessidade, têm-se os ensinamentos de Basan (2022, p. 62):

> Em resumo, o que a LGPD determina é que o uso de dados pessoais deve se restringir às informações adequadas para a finalidade almejada, promovendo o tratamento do mínimo de dados necessários para o alcance do objetivo pretendido. Esse raciocínio também encontra amparo no GDPR, que prevê a minimização dos dados e a limitação da conservação, restringindo o tratamento somente dos dados pertinentes e efetivamente necessários para os propósitos definidos [...].

Extrai-se, a partir desses princípios, que a gravação audiovisual das audiências judiciais estará em consonância com esses princípios quando, por exemplo, embora contenha registro integral do ato, a gravação se restrinja ao mínimo necessário a esse registro e não importa em replicação desnecessária de repositório de informações, nem é utilizada para finalidade diversa da documentação do ato processual, especialmente para publicação em redes sociais.

É importante destacar que o mínimo necessário ao registro do ato deve ser entendido não como um registro parcial, mas sim aquele registro que busca restringir a captura de som e de imagem àquilo que seja efetivamente relevante à instrução do processo e, portanto, sem tratar dados pessoais desnecessários à instrução processual, como, por exemplo: filmar terceiros alheios ao feito que estejam presentes na audiência, efetuar a captura do registro audiovisual por meio de vários aparelhos, ou, ainda, providenciar a gravação mediante a montagem de um verdadeiro estúdio de filmagem para produção de filme profissional, o que, por si só, já denota finalidade diversa do mero registro processual.

Além disso, é prescindível maiores digressões a respeito para demonstrar que a gravação, levada a efeito por dispositivos particulares, quando já realizada uma gravação pelo próprio Poder Judiciário ou pelo Ministério Público, além de representar uma replicação desnecessária de base de dados (violação ao princípio da necessidade), gera um grande risco aos titulares dos dados pessoais envolvidos, pois esses aparelhos poderão ser extraviados ou violados com mais facilidade, incrementando o risco de violação ao direito fundamental.

Por seu turno, o princípio da finalidade, elemento estruturante do sistema de proteção de dados pessoais, veda expressamente o tratamento posterior de dados pessoais de forma incompatível com sua destinação originária, qual seja, o registro de atos processuais juridicamente relevantes, configurando-se como irregular qualquer desvio desta finalidade precípua.

Assim, considerando que não há dúvidas de que a finalidade da gravação audiovisual em audiências judiciais é apenas o registro dos atos processuais relevantes ao processo, é indubitável que a posterior divulgação dessas filmagens em redes sociais afigura-se incompatível com essa finalidade e configura um tratamento irregular de dados pessoais.

Ora, não se pode anuir com a espetacularização dos atos processuais, transformando Promotores de Justiça, Magistrados, Advogados, testemunhas, jurados, vítimas, réus, requeridos e requeridas em protagonistas e/ou coadjuvantes de uma trama, a bel-prazer do editor, em que o menos importante seja o registro processual e o mais relevante seja a promoção pessoal e/ou profissional.

É bem verdade que, nos termos do art. 20 do Código Civil Brasileiro, a eventual utilização indevida da imagem de uma pessoa poderá ser objeto de posterior responsabilização civil. Entretanto, no estágio tecnológico atual, em que gravações podem ser facilmente editadas e imediatamente compartilhadas com milhões de pessoas ou que – a partir do uso de inteligência artificial e do uso de som e imagem reais de uma pessoa – é possível a criação dos chamados "*deepfakes*", uma vez ocorrido o tratamento indevido dos dados pessoais, o dano é irreparável e o risco é permanente aos titulares.

Neste cenário, merecem especial atenção os princípios da segurança e da prevenção, os quais preconizam justamente a adoção de medidas técnicas e administrativas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Dito isso, não se mostra consentâneo com a tutela do direito fundamental à proteção de dados pessoais relegar a adoção de medidas prévias efetivas a evitarem a ocorrência da violação, deixando essa discussão para eventual análise posterior em responsabilização civil, pois o dano, como mencionado, caso ocorrido, não poderá ser devidamente reparado após a disseminação indevida do registro audiovisual em redes sociais que contam com compartilhamento em larga escala.

Nessa linha, traz-se à colação, mais uma vez, a Orientação n. 001/2024/UEPDAP do CNMP:

> 2.1- Caso o Poder Judiciário disponha de meios próprios para registro audiovisual, orienta-se:
>
> A) ao membro do Ministério Público que [...] a qualquer momento processual, mas, preferencialmente, desde o seu início, requeira ao Magistrado, de forma fundamentada (modelo do anexo III), que este expressamente determine a proibição de gravação audiovisual pelos demais presentes nas audiências judiciais, por meio de dispositivos particulares, bem como consigne a vedação da utilização da gravação realizada pelo Poder Judiciário para finalidades diversas da atuação [...].

No mesmo sentido da orientação acima, o já mencionado artigo 67 do Decreto-Lei nº 6/2023 da Espanha prevê, em sua alínea "2", que, nos processos judiciais telemáticos e nos serviços não presenciais, as partes, intervenientes ou qualquer pessoa que tenha acesso ao processo não poderá gravar, coletar imagem ou utilizar qualquer meio que permita uma posterior reprodução do som e/ou da imagem do ocorrido. E mais, referida normativa dispõe, em suas alíneas "3" e "4", que as gravações a que qualquer pessoa tenha tido acesso em razão de um procedimento judicial não poderá ser utilizada, sem autorização judicial, para fins diversos dos jurisdicionais, sob pena de multa de 180 a 60.000 euros, sem prejuízo da responsabilização administrativa, civil ou penal cabíveis[16].

No tocante aos princípios da transparência e da boa-fé, cabe ressaltar que o titular dos dados pessoais a serem tratados deve ter ciência prévia acerca dessa gravação, não se mostrando regular a gravação clandestina realizada por uma das partes ou por quem quer que esteja presente no ato.

16. Artículo 67. Control sobre la difusión de actuaciones telemáticas.
[...]
2. Em las actuaciones judiciales telemáticas y em los servicios no presenciales descritos em el presente título, las partes, intervenientes o cualesqueira personas que tengan acceso a dicha actuación, no podrán grabar, tomar imágenes o utilizar cualesquiera médios que permitan uma posteior reproducción del sonido y o de la imagen de lo acontecido.
3. Las grabaciones a las que cualquier persona haya tenido acceso com motivo de um procedimento judicial no podrán ser utilizadas, sin autorización judicial, para fines distintos de los jurisdiccionales.
4. Em caso de incumplimiento de las obligaciones estabelecidas em el presente artículo, el juez o tribunal podrá imponer motivadamente uma multa de 180 a 60.000 euros, que estará sujeta al régimen de recursos previsto em el título V del libro VII de la Ley Orgánica 6/1985, de 1 de julio, sin perjuicio de las sanciones que correspondan si la actuación constituyera uma infracción a la normativa sobre protección de datos de carácter personal, y de las responsabilidades administrativas, civiles o penales a que haya lugar. Para la imposición de las sanciones se tendrá em cuenta la intencionalidade, el perjuicio real causado a la Administración o a los ciudadanos y la reiteración o reincidência de la conducta.

Um exemplo paradigmático e amplamente noticiado dessa espetacularização das audiências judiciais ocorreu durante uma instrução processual no fórum de Jacarepaguá, em março de 2024, quando o juiz, provocado pela representante do Ministério Público, determinou a apreensão de uma gravação velada realizada pelo advogado, sem qualquer aviso prévio às partes envolvidas no ato, o que terminou por ocasionar embates que geraram entraves ao correto desempenho da atividade jurisdicional.[17]

Apesar da insurgência da representante ministerial quanto ao registro audiovisual velado feito pelo advogado, da fundamentação de violação à Lei Geral de Proteção de Dados Pessoais, e da determinação judicial de apreensão do vídeo, o advogado deixou de cumprir a determinação judicial e divulgou o registro feito em audiência em seus perfis nas redes sociais Instagram, X e Tik Tok.

O vídeo fora publicado com edições de som, legendas e cortes descontextualizados, e divulgado nas diversas redes sociais com conteúdo desvirtuado, acompanhado de legendas que imputavam adjetivos ultrajantes e depreciativos à representante ministerial e alteravam a realidade dos fatos, com claro objetivo de promoção pessoal do advogado.

Não é difícil imaginar o alcance que tais vídeos, impulsionados pelos algoritmos das referidas redes sociais, atingiram. Iniciou-se, após a divulgação indevida das imagens, um verdadeiro processo de linchamento virtual da representante ministerial, com comentários e compartilhamentos injuriosos formulados por um grande número de usuários.

O linchamento virtual, ou *"online shaming"* é um fenômeno contemporâneo caracterizado pela exposição massiva e depreciativa de indivíduos em ambientes digitais, e representa uma grave violação aos direitos fundamentais propiciada pelo uso indevido de dados pessoais em ambientes digitais. Esse mecanismo de justiçamento informal é potencializado pelas redes sociais, cujo ambiente possibilita a propagação viral desses conteúdos lesivos, cujos danos comprometem a integridade psicossocial dos indivíduos e evidenciam a premente necessidade de estabelecimento de marcos regulatórios capazes de mitigar práticas de exposição vexatória em ambientes informacionais de larga escala.

Convém destacar que esse cenário de espetáculo e exacerbação midiática gerados no caso ora analisado derivou de mera divergência hermenêutica e de sustentação jurídica formulada pela representante ministerial no exercício de suas funções, sem qualquer violação a dever funcional, e com acolhimento do pleito pelo Juiz de Direito que conduzia o ato jurisdicional.

Os danos ocasionados pela divulgação indevida de dados pessoais colhidos em audiência judicial, potencializados pelo impulsionamento dos

17. Disponível em <https://www.migalhas.com.br/quentes/404164/lgpd-pode-ser-invocada-para-proibir-a-gravacao-de-audiencia>. Acesso em: 04 fev. 2025.

algoritmos das redes sociais, dificilmente será reparado. Da mesma forma, os registros audiovisuais divulgados indevidamente na internet em clara violação à LGPD jamais serão apagados por completo, o que reforça a necessidade de uma atuação preventiva em casos semelhantes.

4. CONCLUSÃO

Diante da análise realizada, conclui-se que o compartilhamento indiscriminado de registros audiovisuais de audiências judiciais em redes sociais representa uma grave violação ao direito fundamental à proteção de dados pessoais. Isso porque a finalidade original da coleta desses registros - a instrução processual - é desvirtuada quando tais conteúdos são disseminados em plataformas digitais, expondo indevidamente dados pessoais dos participantes do ato judicial em busca de engajamento. Esta prática não apenas transgride os princípios basilares da Lei Geral de Proteção de Dados, como também compromete a própria prestação jurisdicional.

De fato, a espetacularização das audiências judiciais representa flagrante violação aos princípios constitucionais da dignidade da justiça, verdade real e devido processo legal, na medida em que transforma o ato processual em produto midiático, subordinando a relevância jurídica à lógica do entretenimento.

Esse fenômeno compromete a seriedade institucional do Poder Judiciário, desvirtuando a função jurisdicional para uma performance sensacionalista, onde a busca pela visibilidade e engajamento supera o compromisso com a verdade processual, a imparcialidade e o respeito aos direitos fundamentais dos sujeitos processuais. Essa dinâmica espetacular não apenas banaliza o processo judicial, mas potencialmente contamina a formação da convicção jurisdicional, a busca pela verdade real e se afasta dos princípios constitucionais da razoabilidade e da tutela jurisdicional efetiva.

Em virtude dessas considerações, é possível afirmar que uma regulamentação clara sobre o uso de gravações em audiências jurisdicionais e em atos extrajudiciais emerge como imperativo para salvaguardar a dignidade dos atores processuais, exigindo marco normativo que discipline o registro, armazenamento e tratamento dos registros audiovisuais.

Impõe-se a construção de mecanismos jurídicos capazes de equilibrar o princípio da publicidade processual com a proteção integral dos direitos fundamentais à privacidade, imagem e proteção de dados pessoais, mediante o estabelecimento de protocolos rigorosos que inviabilizem a exposição vexatória e o uso espetacularizado de dados pessoais, de forma a resguardar a essência do processo judicial, impedindo a transformação de atos processuais em verdadeiros instrumentos de violação da dignidade da pessoa humana.

5. REFERÊNCIAS BIBLIOGRÁFICAS E DOCUMENTAÇÃO

Basan, A.P. Art. 6°. In: Martins, G.M., Faleiros Júnior, J.L. de M., Longhi, J.V.R. (2024). *Comentários à Lei Geral de Proteção de Dados Pessoais*. 2. Indaiatuba: Foco.

Brasil. Conselho Nacional de Justiça. (2021). *Recomendação n. 94, de 9 de abril de 2021*. Disponível em https://atos.cnj.jus.br/files/original143058202104146076fca2b64c9.pdf

Brasil. Conselho Nacional do Ministério Público. (2022). *Recomendação n. 92, de 9 de Agosto de 2022.* Disponível em: https://www.cnmp.mp.br/portal/images/Recomendacoes/Recomendao-n-92.2022.pdf

Brasil. Conselho Nacional do Ministério Público. (2023). *Resolução n. 281, de 12 de dezembro de 2023.* Disponível em: https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-n-281-de-2023-com-anexo.pdf

Brasil. Conselho Nacional do Ministério Público. Unidade Especial de Proteção de Dados Pessoais. (2024). *Orientação n. 001/UEPDAP/CNMP, de 22 de maio de 2024*. Disponível em: https://www.cnmp.mp.br/portal/images/Comissoes/CPAMP/uepdap/ORIENTACAO_UEPDAP_N%C2%BA_01__DE_22_DE_MAIO_DE_2024_Assinada.pdf

Brasil. (1988). *Constituição da República Federativa do Brasil*. Brasília. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Brasil. (2022). *Emenda Constitucional n. 115*, de 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais

Brasil. (2002). *Lei n. 10.406, de 10 de janeiro de 2002*. Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

Brasil. (2015). *Lei n. 13.105, de 16 de março de 2015*. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm

Brasil. (2018) *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brasil. (2020). Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6.387 – Distrito Federal. Relatora Ministra Rosa Weber. j. 07 maio 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629

Cancelier, M.V. de L. (2017). O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. *Sequência Estudos Jurídicos e Políticos*, 38 (76), 213–240. DOI: 10.5007/2177-7055.2017v38n76p213. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2017v38n76p213

Cohen, J. E. (2013). What Privacy is for. *Harvard Law Review*, 126, 1904-1933. Disponível em https://scholarship.law.georgetown.edu/facpub/2526

Colombo, C. Art. 1°. In: Martins, G.M., Faleiros Júnior, J.L. de M., Longhi, J.V.R. (2024). *Comentários à Lei Geral de Proteção de Dados Pessoais*. 2. Indaiatuba: Foco.

Conselho da Europa. (1981). *Convenção n. 108, de 28 de Janeiro de 1981.* Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2

Debord, G. (1997). *A sociedade do espetáculo*. Tradução de Estela dos Santos Abreu. Rio de Janeiro: Contraponto.

Espanha. (2023). Real Decreto-Lei n. 6, de 19 de dezembro de 2023. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2023-25758

Finocchiaro, G. (2012). *Privacy e protezione del dati personali: disciplina e strumenti operativi*. Turim: Zanichelli.

Habermas, J. (1997). Direito e Democracia. Rio de Janeiro: Tempo Brasileiro.

Hamm, R.F. (2010). *Olmstead v. United States: the Constitutional Challenges of Prohibition Enforcement*. Washington DC: Federal Justice Center.

Jones, M.L. (2016). *The right to be forgotten*. New York: New York University Press.

Llosa, M.V. (2013). *A civilização do espetáculo: Uma radiografia do nosso tempo e da nossa cultura*. Tradução de Ivone Benedetti. Rio de Janeiro: Objetiva.

Martins, G.M. (2022). O direito ao esquecimento na sociedade da informação. São Paulo: Revista dos Tribunais.

Martins, G.M., **Ramos**, A.A. (2022). Da privacidade à proteção de dados pessoais: o julgamento histórico do STF e a MP 954/2020. *Revista dos Tribunais*, 1036, 124-125.

Mayer-Schönberger, V., **Cukier**, K. (2014). Big Data. Nova Iorque: Mariner Books.

Migalhas. (2024). *LGPD pode ser invocada para proibir a gravação de audiências?* Disponível em: https://www.migalhas.com.br/quentes/404164/lgpd-pode-ser-invocada-para-proibir-a-gravacao-de-audiencias

Rodotà, S. (2008). *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar.

Rodotà, S. (2012). *Il diritto di avere diritti*. Roma/Bari: Laterza.

Statista. (2024). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028*. Disponível em: https://www.statista.com/statistics/871513/worldwide-data-created/#statisticContainer

Uniao Europeia. (1995). *Diretiva n. 95/46/CE, de 24 de outubro de 1995.* Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046

Uniao Europeia. (2000). *Carta dos Direitos Fundamentais da União Europeia*. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf

Uniao Europeia. (2016). *Regulamento (UE) 2016/679, de 27 de abril de 2016*. Regulamento Geral de Proteção de Dados (GDPR). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Warren, S.D., **Brandeis**, L.D. (1890). *The Right to Privacy*. Cambridge: Quid Pro, LLC.

PLANEJAMENTO ESTRATÉGICO NACIONAL: A PROTEÇÃO DE DADOS PESSOAIS COMO DIRETRIZ DE ATUAÇÃO DO MINISTÉRIO PÚBLICO

Paulo Roberto Gonçalves Ishikawa[1]

Resumo: Este documento aborda o Plano Estratégico Nacional do Ministério Público e sua revisão ocorrida no ano de 2023, que na oportunidade incluiu um Programa e uma Ação Estratégica voltada à atuação na tutela coletiva do direito fundamental à proteção de dados pessoais do cidadão, mediante a inciativa do Colégio de Encarregado pela Proteção de Dados Pessoais do Ministério Público.

Palavras-chave: Ministério Público. Plano Estratégico Nacional. Proteção de Dados Pessoais.

Resumen: Este documento aborda el Plan Estratégico Nacional del Ministerio Público y su revisión realizada en el año 2023, la cual incluyó un Programa y una Acción Estratégica orientados a la actuación en la tutela colectiva del derecho fundamental a la protección de los datos personales del ciudadano, mediante la iniciativa del Colegio de Encargados de Protección de Datos Personales del Ministerio Público.

Palabras clave: Ministerio Público. Plan Estratégico Nacional. Protección de Datos Personales.

---

1. Promotor de Justiça e Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado de Mato Grosso do Sul.

1. INTRODUÇÃO

O presente texto tem por objetivo abordar e registrar um importante momento do Planejamento Estratégico do Ministério Público brasileiro. Momento em que foram incluídos, pela primeira vez, um Programa e uma Ação Estratégica voltados à proteção de dados pessoais, destacando a importância desse novo direito fundamental do cidadão, bem como direcionando as Unidades do Ministério Público a definirem os órgãos de execução responsáveis pela defesa do direito à proteção de dados pessoais no âmbito coletivo.

Tais providências repercutirão em âmbito nacional, considerando o caráter direcionador do Plano Estratégico Nacional e seu monitoramento pelo Conselho Nacional do Ministério Público.

Tal inclusão só ocorreu em razão a iniciativa do Colégio de Encarregados pelo Tratamento de Dados Pessoais do Ministério Público, que, no momento oportuno, viabilizou a inclusão desse tema tão relevante no Plano Estratégico, que impulsiona e incentiva a atuação dos órgãos de execução do Ministério Público brasileiro.

2. PLANO ESTRATÉGICO NACIONAL DO MINISTÉRIO PÚBLICO BRASILEIRO

Tratar do assunto planejamento estratégico para um profissional da área jurídica é um desafio. Desafio maior é discorrer sobre esse tema tendo como público-alvo os Membros do Ministério Público, considerando a formação jurídica e a ausência deste conteúdo nos cursos de graduação de Direito. Isso porque a formação jurídica foca na interpretação das normas jurídicas, ficando de lado toda a teoria que diz respeito à organização administrativa e funcional das organizações privadas e entes públicos relacionados ao sistema de justiça.

No entanto, no ano de 2010, o Conselho Nacional do Ministério Público (CNMP) deu início a uma nova concepção na atuação do Ministério Público brasileiro, com a formulação do primeiro plano estratégico de âmbito nacional, orientando e envolvendo todas as Unidades e Ramos do Ministério Público nos programas e ações estratégicas decorrentes do trabalho coletivo de Promotores e Procuradores de todo o Brasil.

Assim, o primeiro plano estratégico teve como período de vigência o período de 2010 a 2015, renovado para 2017 (21ª Sessão Ordinária do CNMP de 2014) e também para o ano 2019. Já no ano de 2018 iniciaram-se os trabalhos para elaboração do Planejamento Estratégico Nacional do Ministério Público Brasileiro para o período 2020-2029 (PEN-MP). Após sua entrada em vigência, conforme já previsto em sua metodologia, no ano de

2023 se deu a primeira revisão desse plano estratégico, justamente quando foram incluídos o programa e a ação estratégica que tratou da proteção de dados pessoais como direcionadores dos trabalhos do ministério público, algo inédito sem nenhuma previsão anteriormente definida nesse sentido.

Essa é uma breve introdução para ressaltar a importância do Conselho Nacional do Ministério na definição da estratégia nacional do Ministério Público, e como isso repercute nas demais Unidades e Ramos.

2.1. CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

Para melhor compreensão do que será abordado na sequência, importante tecer algumas considerações sobre o Conselho Nacional do Ministério Público e como sua atuação pode influenciar e impactar nos trabalhos dos Membros do Ministério Público brasileiro.

Foi com a publicação da Emenda Constitucional n. 45/2004, conhecida como Reforma do Judiciário, que o CNMP passou a existir no ordenamento jurídico. Assim, foi introduzido na Constituição Federal o artigo 130-A, que definiu os parâmetros de constituição e funcionamento do órgão, estabelecendo, em seu §2º, o seguinte:

> Compete ao Conselho Nacional do Ministério Público o controle da atuação administrativa e financeira do Ministério Público e do cumprimento dos deveres funcionais de seus membros, cabendo-lhe:
>
> I - zelar pela autonomia funcional e administrativa do Ministério Público, podendo expedir atos regulamentares, no âmbito de sua competência, ou recomendar providências" (negritamos).

No âmbito do CNMP, foi criada a Comissão de Planejamento Estratégico, prevista no artigo 31, inciso V, de seu Regimento Interno,[2] que também disciplina, a partir de seu artigo 157, disposições específicas sobre o planejamento estratégico nacional do Ministério Público:

> Art. 157 O Plenário promoverá permanentemente o planejamento estratégico do Ministério Público nacional, que consistirá em:
>
> I – definir e fixar, com a participação dos órgãos do Ministério Público, os planos de metas e os programas de avaliação institucional do Ministério Público, visando ao aumento da eficiência, à racionalização e à produtividade, podendo ser ouvidas as associações nacionais de classe (...)

E para disciplinar as diretrizes do planejamento e gestão estratégica do Ministério Público brasileiro, foi então editada a Resolução 147 do Conselho

2. Disponível em https://www.cnmp.mp.br/intranet/images/2020/TV/Regimento_Interno_do_CNMP_2020_agosto.pdf. Acesso em 02 de fevereiro de 2025.

Nacional do Ministério Público,[3] que trouxe as definições, dispositivos sobre governança, processo de elaboração, revisão e monitoramento do plano estratégico nacional.

Importante destacar que o artigo 8ª da Resolução 147 estabelece que o PEN-MP tem "caráter direcionador para todas as unidades e ramos do Ministério Público e para seus membros e servidores". Com isso, todos os objetivos, programas e ações estratégicas previstas no PEN-MP devem ser considerados na atuação dos membros do Ministério Público de todo o país.

Além disso, a referida resolução também define, no seu §3º do artigo 8º, que "anualmente, a CPE providenciará a publicação de ranking das unidades e ramos do Ministério Público quanto à implementação e ao cumprimento do PEN-MP". Isso porque compete à CPE "monitorar o PEN-MP e adotar as providências necessárias à sua implementação e cumprimento", conforme previsto no art. 4º, §1º, III da Resolução n. 147 do CNMP. Para tanto, poderá a CPE, "a qualquer tempo, solicitar das unidades e ramos do Ministério Público informações sobre a implementação e o cumprimento do PEN-MP em âmbito local, notadamente no que tange a seus indicadores, metas, projetos, processos, ações e iniciativas nacionais" (art. 4º, §5º, da Resolução 147).

Com essas informações, torna-se possível o monitoramento nacional do Plano Estratégico Nacional do Ministério Público, que ocorre por meio do denominado "Radar Estratégico"[4], que consiste na consolidação das informações fornecidas pelas unidades e ramos do Ministério Público brasileiro, instrumentalizado por um painel de BI – *Business Intelligence*.

2.2. REVISÃO DO PLANO ESTRATÉGICO NACIONAL

Passar por essa rápida abordagem acerca do Planejamento Estratégico Nacional é fundamental para compreendermos as consequências e os benefícios advindos da previsão de temas relevantes para a sociedade, pelo "caráter direcionador" que possui em razão da expressa previsão normativa, conforme acima apontado.

Seguindo esse raciocínio, importante destacar o processo de revisão novo Plano Estratégico Nacional, pois foi justamente nesse procedimento é que foram incluídos um programa e uma ação estratégica relacionados à proteção de dados pessoais pelo Ministério Público.

3. Disponível em https://www.cnmp.mp.br/portal/images/Normas/Resolucoes/Resolucao_147.pdf. Acesso em 02 de fevereiro de 2025.

4. Pode ser acesso no seguinte link: https://public.tableau.com/app/profile/cnmp/viz/RadarEstratgico/RadarEstratgico

Conforme previsão regimental, compete à Comissão de Planejamento Estratégico do Conselho Nacional do Ministério Público não só a elaboração, mas também a revisão do PEN-MP, nos termos do artigo 5º, IV da Resolução 147 do CNMP.

Assim, no ano de 2023 a Comissão de Planejamento Estratégico do CNMP promoveu reuniões com representantes de todas as Unidades e Ramos do Ministério Público para definição de novos Programas e Ações Estratégicas, mantendo-se os demais elementos do Mapa Estratégico. Essa revisão abrangeu não só as matérias relacionadas às atividades finalísticas do Ministério Público, mas também temas estruturantes (área-meio), com a participação de técnicos das áreas de Administração, Gestão Estratégica, Gestão Orçamentária, Gestão de Pessoas, Comunicação, Gestão de Pessoas e Tecnologia da Informação.[5]

Em relação à atuação finalística do Ministério Público, especificamente em relação aos Programas, foram convidadas todas as demais Comissões do CNMP para sugestões de temas: Corregedoria Nacional do Ministério Público; Ouvidoria Nacional do Ministério Público; Comissão da Infância, Juventude e Educação – CIJE; Comissão da Saúde – CS; Comissão de Acompanhamento Legislativo e Jurisprudência – CALJ; Comissão de Controle Administrativo e Financeiro – CCAF; Comissão de Defesa da Probidade Administrativa – CDPA; Comissão de Defesa dos Direitos Fundamentais – CDDF; Comissão de Meio Ambiente – CMA; Comissão de Preservação da Autonomia do Ministério Público – CPAMP; Comissão do Sistema Prisional, Controle Externo da Atividade Policial e Segurança Pública – CSP; Comitê Gestor do Plano Nacional de Gestão de Documentos e Memória do Ministério Público – COPLANAME; Comitê Nacional do Ministério Público de Combate ao Trabalho em Condição Análoga à de Escravo e ao Tráfico de Pessoas – CONATETRAP; Comitê Permanente Nacional de Fomento à Atuação Resolutiva – CONAFAR; Estratégia Nacional de Justiça e Segurança Pública – ENASP; e Unidade Nacional de Capacitação do Ministério Público – UNCMP.

A intenção de elencar no parágrafo anterior todas as comissões que participaram do processo de revisão foi justamente para demonstrar que, até então, não havia nenhuma representação do CNMP que tratasse da temática "Proteção de Dados Pessoais".

Por outro lado, os Membros do Ministério Público especializados nas matérias Probidade Administrativa, Educação, Saúde, Infância e Juventude, Criminal, Execução Penal e Segurança Pública, Direitos Humanos, Meio Ambiente e Consumidor, representando suas unidades e ramos, também não sugeriram nenhum programa relacionado à Proteção de Dados Pessoais.

5. Relatório da Revisão do PEN disponível em: https://www.cnmp.mp.br/portal/images/Comissoes/CPE/pen/Revis%C3%A3o/Relat%C3%B3rio/20240227_2%C2%BA_Ciclo_do_PEN-MP_2020-2029-Relatorio_da_Revis%C3%A3o_V.4.1.pdf Acesso em 02/02/2025.

Esse é um dado que merece reflexão, pois num processo de revisão planejamento estratégico de abrangência nacional do Ministério Público nada foi mencionado acerca da proteção de dados pessoais, apesar da vigência da Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados[6]. Nem mesmo o advento da Emenda Constitucional n. 115, de 10 de fevereiro de 2022, que incluiu o inciso LXXIX no artigo 5º da Constituição Federal, foi suficiente para motivar a inclusão de um programa tratando da matéria no PEN -MP.

Diz o artigo 5º, LXXIX da Constituição Federal:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Nota-se, pela redação acima, que o direito à proteção dos dados pessoais passou a constituir um Direito Fundamental da pessoa, um direito autônomo como a privacidade, liberdade e inviolabilidade da intimidade. Com isso, o cidadão passa a estar protegido de qualquer norma infraconstitucional que venha a confrontar-se, sendo, portanto, impossibilitada qualquer tentativa de se restringir ou mesmo revogar esse direito.

Também tem efeitos relevantes em relação ao próprio Poder Público, que deverá também resguardar esse direito quando estiver tratando dados pessoais dos cidadãos em seus processos internos. Embora seja o consentimento dispensado, nos termos do artigo 7º e 23 da Lei Geral de Proteção de Dados, tem o poder público a obrigação de observar o §2º do artigo 23, que impõe o dever de informar claramente a base legal e finalidade do tratamento de dados pelo Poder Público ao cidadão.

Exatamente nesse ponto que emerge a importância do Encarregado pelo Tratamento de Dados Pessoais do Ministério Público. É de sua responsabilidade o esforço para que o órgão mantenha, conserve e proteja os dados pessoais dos cidadãos, interferindo e sugerindo mudanças administrativas nos processos internos para que esse ativo seja resguardado. Serve ele como interlocutor entre a sociedade e a própria Instituição, cabendo a ele providências inclusive junto à autoridade nacional caso haja violação a esse direito.

---

6. Art. 65. Esta Lei entra em vigor: I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

3. O COLÉGIO DOS ENCARREGADOS PELO TRATAMENTO DE DADOS PESSOAIS DO MINISTÉRIO PÚBLICO

Com a publicação da Lei Geral de Proteção de Dados – LGPD, as Unidades e Ramos do Ministério Público iniciaram as primeiras providências no tocante à proteção de dados pessoais no âmbito interno. Com isso, os dados pessoais tratados pelo Ministério Público passaram a receber a proteção legal prevista na referida lei, gerando alterações na gestão e administração em geral, principalmente nos processos em que tais dados estão no formato digital.

No cenário externo, com a publicação da Lei 13.853, de 8 de Julho de 2019, que alterou a LGPD, foi instituída a Autoridade Nacional de Proteção de Dados – ANPD, mas sem previsões ou intervenções no tocante à atuação do Ministério Público. No Conselho Nacional do Ministério Público havia tramitação de uma proposta de regulamentação da LGPD, mas foi somente aprovada em dezembro de 2024.

Não obstante, as Unidades e Ramos do Ministério Público começaram a nomear seus Encarregados pelo Tratamento de Dados Pessoais, cuja articulação resultou na criação do CEDAMP.

3.1. DOS ENCARREGADOS PELO TRATAMENTO DE DADOS PESSOAIS DO MINISTÉRIO PÚBLICO

A Lei Geral de Proteção de Dados prevê a figura do Encarregado pelo Tratamento de Dados Pessoais em seu artigo 41, descrevendo algumas atividades a serem por ele exercidas.

No início, no âmbito do Ministério Público, muitas dúvidas surgiram quanto à pessoa que exerceria essa nobre e desafiadora função. Com o tempo, firmou-se o entendimento de que tal cargo deveria ser ocupado por um Membro da carreira, ou seja, um Promotor ou Procurador.

Tal escolha se mostrou acertada, pois o Encarregado pelo Tratamento de Dados Pessoais necessita de certa autonomia e independência para o pleno exercício de sua função[7]. Além disso, precisa de trânsito junto à Administração Superior para que possa ter interlocução direta com todas as secretarias e setores que integram a administração. Não obstante, a formação jurídica dos Membros, no mais das vezes, não é suficiente para compreender o alcance

7. "§ 3º Ao encarregado deverão ser asseguradas a independência e a autonomia necessárias ao bom desempenho de suas funções, devendo o respectivo ramo ou unidade do Ministério Público ao qual ele se vincula garantir, para tanto, a estrutura mínima de apoio técnico, jurídico e administrativo, com estrutura de apoio à governança e gestão, inclusive" (Resolução 281 do Conselho Nacional do Ministério Público" (negritamos).

e a importância da proteção dos dados pessoais, razão pela qual deve obter conhecimentos técnicos suficientes para enfrentar as dificuldades que surgem no decorrer do tratamento dos dados pessoais.

Além disso, grande parte dos dados pessoais encontram-se em arquivos digitais, servidores, serviços de nuvem, o que exige conhecimentos mínimos na área de Tecnologia da Informação, até mesmo para dialogar com os técnicos que trabalham nessa área.

Outra dificuldade é que os Membros designados para exercer a função de Encarregado não o fazem de forma exclusiva. Pelo contrário, salvo raríssimas exceções, sempre cumulando outras atribuições no órgão, nas mais diversas áreas de atuação. Ressalta-se que, nesse ponto, a Resolução 281 do Conselho Nacional do Ministério Público[8], que institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público, orienta que "*o exercício das funções de encarregado deve ocorrer, preferencialmente, sem o acúmulo com outras funções*".

Neste cenário, uma rede de comunicação se estabeleceu entre os Encarregados pelo Tratamento de Dados Pessoais do Ministério Público, resultando em reuniões técnicas onde foram compartilhadas dúvidas e soluções para os casos que surgiram ao longo do tempo.

3.2. DO SURGIMENTO DO CEDAMP

O contato entre os Encarregados pelo Tratamento de Dados Pessoais do Ministério Público gerou alinhamento e sentimento de pertencimento. De forma orgânica, sem qualquer imposição normativa, os laços foram se estreitando, resultando na criação de uma associação de natureza civil que se denominou "Colégio dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público", composto por todos os que exercem tal função no âmbito do Ministério Público.

Desde sua criação, além do trato de assuntos diários, foram realizados trabalhos de pesquisa, gerando pareceres e estudos que foram acolhidos e seguidos pelas Administrações Superiores dos MPs. Parecerias acadêmicas e encontros nacionais passaram a ocorrer com frequência, resultando no amadurecimento institucional tão necessário para o desempenho da função. Neste ponto, destaca-se a "Formação de Alto Nível em Proteção de Dados decorrente de convênio com a Universidade de Santiago de Compostela", em abril de 2024.

O Estatuto do CEDAMP foi registrado em cartório no dia 18 de Julho de 2023 e traz, em seu artigo 1°, o seguinte:

8. Disponível em https://www.cnmp.mp.br/portal/images/CALJ/resolucoes/Resoluo-n-281-de-2023-com-anexo.pdf . Acesso em 03 de fevereiro de 2025.

> O Colégio dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público – CEDAMP – é uma associação, de âmbito nacional e sem fins lucrativos, integrada por membros do Ministério Público investidos na função de Encarregado pelo Tratamento de Dados Pessoais do Ministério Público dos Estados, da União e do Conselho Nacional do Ministério Público.

Dentre seus fins, destaca-se:

> Propor ao Conselho Nacional do Ministério Público (CNMP) e/ou à Autoridade Nacional de Proteção de Dados (ANPD) sugestões para a adequação e/ou elaboração de atos normativos na área de proteção de dados pessoais, considerando a natureza e as peculiaridades do Ministério Público (art. 2º, VII do Estatuto do CEDAMP).

Portanto, com sua existência jurídica, o CEDAMP passa a ter um papel fundamental na proteção de dados pessoais no Brasil, pois agrega todos os Encarregados pela Proteção de Dados Pessoais dos Ministérios Públicos. Com isso, torna-se possível uma atuação planejada e estruturada na defesa desses direitos no âmbito interno de cada Unidade, sem violar sua autonomia administrativa e orçamentária que cada Ministério Público possui para garantir suas atribuições constitucionais.

4. A DEFESA COLETIVA DOS DADOS PESSOAIS PELO MINISTÉRIO PÚBLICO BRASILEIRO

Conforme abordado nos capítulos anteriores, o Encarregado pelo Tratamento de Dados Pessoais do Ministério Público exerce papel de grande relevância em cada Unidade do Ministério Público.

Conforme previsto expressamente na Lei Geral de Proteção de Dados, por definição, o Encarregado é "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados" (art. 5º, VIII da LGPD).[9]

Além disso, a LGPD estabelece, em seu artigo 23, que:

> O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir atribuições legais do serviço, desde que:

9. O artigo 4º, XXI da Resolução 281 do Conselho Nacional do Ministério Público estabelece o encarregado como sendo a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade de Proteção de Dados Pessoais no Ministério Público (APDP/MP)", no caso o próprio CNMP (artigo 4º, V, da Resolução n. 281 do CNMP).

> I – (...)
>
> II – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 destas lei" (negritamos).
>
> Outro ponto a ser destacado são as atividades a serem exercidas pelo Encarregado, descritas no art. 41, §2º, nos seguintes termos:
>
> III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
>
> IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (negritamos).

Em complementação, o artigo 46, da Resolução 281, do Conselho Nacional do Ministério Público determina que são atribuições do encarregado: "I - implementar, capacitar, conscientizar, estabelecer responsabilidades e monitorar a conformidade da atuação da Instituição com a Política Nacional de Proteção de Dados Pessoais no Ministério Público e a LGPD".

Fica evidente, nos dispositivos acima mencionados, a função do Encarregado na implementação da LGPD e da Política Nacional de Proteção de Dados Pessoais do Ministério Público, instituída pela Resolução 281 do CNMP, como catalizador e impulsionador das medidas necessárias para fomentar e aperfeiçoar o tratamento dos dados pessoais na Instituição.

No entanto, o Ministério Público, por meio da atuação do seu Encarregado, não é responsável apenas por tratar dos dados pessoais que estão sob a usa guarda. Por constituir um Direito Fundamental, compete ao Ministério Público também atuar na defesa coletiva dos dados pessoais contra lesões de terceiros.

A Seção III do Capítulo III (Do Sistema Nacional de Proteção de Dados Pessoais (SINPRODAP/MP), estabelece as diretrizes da atuação do Ministério Público no âmbito coletivo, consistente:

> na defesa da ordem jurídica e da dimensão coletiva do direito à proteção aos dados pessoais, diante de violações à legislação por pessoas físicas ou jurídicas, de direito público e privada" (art. 56 da Resolução 281 do CNMP).

De forma exemplificativa, estabelece o artigo 57 da Resolução 281 do CNMP:

> Incumbe ao Ministério Público a proteção de dados pessoais no âmbito das relações de consumo, das relações de trabalho, nos serviços públicos e de relevância pública ou em relações jurídicas de outra natureza, quando se revelar afetação à coletividade.

Mas para que tal atribuição se concretize, é necessário que haja órgãos de execução com atribuições legais para atuar nessa seara, devendo inclusive constar expressamente nas suas respectivas normas internas.

Desta forma, diante da premente necessidade de se designar nas Unidades do Ministério Público os Promotores e Procuradores responsáveis

pela proteção dos dados pessoais no âmbito coletivo, a Resolução 281 do Conselho Nacional do Ministério Público estabeleceu prazo para que tais providências fossem tomadas, nos seguintes termos:

> Art. 159. A tutela coletiva do direito fundamental à proteção de dados pessoais, pelos órgãos de execução do Ministério Público, deverá ser implementada imediatamente.
>
> Parágrafo único. No prazo de 90 (noventa) dias a partir da entrada em vigor da presente Resolução, os ramos e as unidades do Ministério Público deverão informar à UEPDAP quais os órgãos de execução que possuem atribuição para a tutela coletiva do direito fundamental à proteção de dados pessoais (negritamos).

Da leitura do dispositivo acima, é possível constatar o senso de urgência do Conselho Nacional do Ministério Público na designação de órgãos de execução para a tutela coletiva da proteção de dados pessoais, considerando previsão expressa de que tal providência "deverá ser implementada imediatamente", com a obrigação comunicar ao órgão de controle interno no prazo de 90 dias.

Assim sendo, a novel resolução deixa clara a missão que o Ministério Público tem a exercer perante a sociedade. Em que pese a clareza a força normativa do texto, visto que originada do órgão de controle externo do Ministério Público, de natureza cogente, existe um longo caminho a percorrer para que atuação na proteção dos dados pessoais seja massiva, não só pelo ingresso recente de tais disposições no ordenamento jurídico, mas também pela percepção da sociedade da importância desse direito.

Nesta senda, qualquer fator que venha despertar e acelerar esse processo é muito bem-vindo. Chegamos então ao ponto fulcral da presente exposição, conforme se verá no próximo capítulo.

5. A PROTEÇÃO DE DADOS PESSOAIS NO PLANO ESTRATÉGICO NACIONAL DO MINISTÉRIO PÚBLICO BRASILEIRO

Conforme mencionado nos capítulos anteriores, por meio da Comissão de Planejamento Estratégico do Ministério Público, foram realizados esforços para que representantes do *parquet* pudessem reavaliar e rever os Programas e Ações Estratégicas do PEN-MP.

Em que pese toda a importância do tema, a princípio, os dados pessoais não foram contemplados dentre as novas diretrizes. Como já discorrido acima, alguns fatores levaram a esse resultado, de sorte que a conjugação deles impossibilitaram que estivessem inseridos dentre os direitos fundamentais elencados como prioritários na atuação do Ministério Público.

Como justificativa, em que pese a participação de todas as comissões temáticas do Conselho Nacional do Ministério Público com sugestões de Programas para a revisão do PEN-MP, na época ainda não havia sido instituída a Unidade Especial de Proteção de Dados Pessoais (UEPDAP), o que só ocorreu quando da publicação da Resolução 281 do Conselho Nacional do Ministério Público[10]. Assim, não foram previstos programas visando a proteção de dados pessoais nessa fase do procedimento de revisão, nem mesmo nas etapas posteriores, com participação dos representantes de diversas Unidades e Ramos do Ministério Público, de várias áreas de atuação, conforme já mencionado.

Foi então que o Colégio de Encarregados pela Proteção de Dados Pessoais do Ministério Público - CEDAMP deliberou, em reunião ordinária e decisão unânime ocorrida no dia 5 de setembro de 2023, a sugestão de um Programa, e respectiva Ação Estratégica, para encaminhamento ao Conselho Nacional do Ministério Público:

> Objetivo Estratégico do PEN-MP:
> Programa: Defesa do dado pessoal como direito fundamental do cidadão.
> Ação Estratégica: Fomentar a proteção dos dados pessoais na atividade finalística do Ministério Público.

Após análise, a Comissão de Planejamento Estratégico do Conselho Nacional do Ministério Público deferiu a solicitação e incluiu o Programa e Ação Estratégica sugerida pelo CEDAMP no Plano Estratégico Nacional do Ministério Público, agregando ao Objetivo Estratégico: "Garantir a transversalidade dos direitos fundamentais em toda a atividade ministerial".

O PEN-MP tem o prazo de vigência de três anos, vale dizer, do ano de 2024 a 2026. Isso significa que todas as Unidades e Ramos do Ministério Público brasileiro, neste triênio, deverão desenvolver projetos que tenham por escopo a proteção de dados pessoais na atividade finalística do Ministério Público. Isso deverá ser demonstrado anualmente, atendendo ao monitoramento da execução do plano pelo CNMP.

Ficou evidente que a inciativa do Colégio de Encarregado pelo Tratamento de Dados Pessoais do Ministério Público - CEDAMP, de forma acertada e proativa, cumpriu seu papel estatutário, ao contribuir para a disseminação da proteção dos dados pessoais pelo país.

Destaca-se, por fim, que o CEDAMP é integrado pelos Encarregados pelo Tratamento de Dados Pessoais de todas as unidades do Ministério Público. Dessa forma cada um, em sua unidade ministerial, com seu conhecimento

10. "Art. 25. Fica instituída a Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público (CPAMP), que exercerá a função de Autoridade de Proteção de Dados Pessoais do Ministério Público (APDP/MP)..."

técnico e apoio irrestrito, poderá ser fator decisivo na implementação do Programa e Ação Estratégica, auxiliando tanto interna quanto externamente.

6. CONCLUSÃO

Após essas breves considerações, ficou evidenciado que o Conselho Nacional do Ministério Público – CNMP - tem papel fundamental na definição dos rumos do Ministério Público brasileiro.

Com fundamento constitucional, o órgão de controle externo tem atribuição, não só regulamentar questões relevantes para atuação do Ministério Público, mas também de atuar diretamente por meio de suas Comissões.

No presente texto, ficou evidente o papel da Comissão de Planejamento Estratégico na coordenação dos trabalhos de elaboração, revisão e monitoramento do Plano Estratégico Nacional PEN-MP, cujo papel direcionador orienta a atuação de todos os Promotores de Justiça e Procuradores do Ministério Público brasileiro. Também ficou evidente os trabalhos desenvolvidos pela Unidade Especial de Proteção de Dados Pessoais, vinculada à Comissão de Preservação da Autonomia do Ministério Público, que vem acompanhando a implantação da Lei Geral de Proteção de Dados nas Unidades do Ministério Público.

Ainda, não houvesse o interesse e o comprometimento dos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público, o direito fundamental à proteção de dados pessoais estaria relegado à norma fria de leis e outros atos normativos, sem qualquer impacto na vida dos cidadãos, impossibilitados de exercer um direito que mal tem conhecimento. Por essa razão é que foi instituído o Colégio de Encarregados pelo Tratamento de Dados Pessoais do Ministério Público, que desde sua criação vem participando ativamente das conquistas e dos desafios enfrentados neste início de implantação da LGPD no Ministério Público brasileiro.

Assim, fica evidente que a conjugação desses esforços poderá promover mudanças significativas, que aos poucos começarão a ser percebidas pela população. Trata-se de uma mudança de cultura que precisa ser implementada, para que o cidadão possa perceber a importância de seus dados pessoais e lutar protegê-los, com os instrumentos normativos disponíveis no ordenamento jurídico.

Por fim, não se teve a pretensão neste presente texto de se aprofundar nos conceitos, objetivos e diretrizes que disciplinam a proteção de dados pessoais, mas apenas registrar um momento institucional importante para o Ministério Público brasileiro. São os primeiros passos que poderão fazer a diferença num futuro distante, e somente nessa ocasião é que poderemos aquilatar, com clareza, o resultado de todo o trabalho desenvolvido nessa quadra da história.

7. DOCUMENTAÇÃO

Brasil. Conselho Nacional do Ministério Público (CNMP). *Manual de Planejamento Estratégico para o Ministério Público.* Brasília, DF: CNMP, 2023. Disponível em: https://www.cnmp.mp.br/portal/images/stories/planejamento_estrategico/PGR_Cartilaha_CNMP_Miolo.pdf.

Brasil. Conselho Nacional do Ministério Público (CNMP). *Planejamento Estratégico Nacional – PEN-MP*. Brasília, DF: CNMP, 2018. Disponível em: https://www.cnmp.mp.br/portal/institucional/comissoes/comissao-de-planejamento-estrategico/planejamento-estrategico-nacional/pen-2020-2029.

Brasil. Conselho Nacional do Ministério Público (CNMP). *1ª Revisão PEN 2020-2029*. Brasília, DF: CNMP, 2023. Disponível em: https://www.cnmp.mp.br/portal/institucional/comissoes/comissao-de-planejamento-estrategico/planejamento-estrategico-nacional/1-revisao-pen-2020-2029.

Brasil. Conselho Nacional do Ministério Público (CNMP). *Regimento Interno do Conselho Nacional do Ministério Público*. Brasília, DF: CNMP, 2023. Disponível em: https://www.cnmp.mp.br/intranet/images/2020/TV/Regimento_Interno_do_CNMP_2020_agosto.pdf.

SEGREDO DO NEGÓCIO FRENTE A TRANSPARÊNCIA ALGORÍTMA: O INQUÉRITO CIVIL COMO FERRAMENTA DE BUSCA DA EXPLICABILIDADE

José Fernando Ruiz Maturana[1]

Resumo: As legislações nacionais costumam proteger a propriedade industrial e os segredos de negócio, apontados como essenciais para estimular a competitividade e a inovação. Por outro lado, a transparência no tratamento de dados pessoais e a explicabilidade das decisões automatizadas são fundamentais para proteger os direitos dos indivíduos, conforme regulamentações como o GDPR e a LGPD. O presente artigo procura abordar os conceitos de "segredo de negócio" e a "transparência no tratamento de dados pessoais", mas destacando o papel do Ministério Público e inserindo o inquérito civil como ferramenta constitucional e útil para se conferir maior efetividade ao princípio da transparência, à explicabilidade algorítma, à correção de viéses e consequente promoção da tutela da proteção de dados pessoais em seu aspecto coletivo.

Palavras-chave: Segredo do Negócio. Transparência e Explicabilidade. Dados Pessoais. Ministério Público. Inquérito Civil.

Resumen: Las legislaciones nacionales suelen proteger la propiedad industrial y los secretos comerciales, señalados como esenciales para estimular la competitividad y la innovación. Por otro lado, la transparencia en el tratamiento de datos personales y la explicabilidad de las decisiones automatizadas son fundamentales para proteger los derechos de los individuos, conforme a regulaciones como el GDPR y la LGPD. El presente artículo busca abordar los conceptos de "secreto comercial" y la "transparencia en el tratamiento de datos personales", destacando el papel del Ministerio Público e insertando la investigación civil como herramienta constitucional y útil para conferir mayor efectividad al principio de transparencia, a la explicabilidad

1. Procurador do Trabalho. Pós-Graduado em Direito do Trabalho pela Universidade Federal do Amazonas. Pós-Graduado em Governança e Gestão da Tecnologia da Informação pela Escola Superior do Ministério Público da União – ESMPU.

algorítmica, a la corrección de sesgos y a la consecuente promoción de la tutela de la protección de datos personales en su aspecto colectivo.

Palabras clave: Secreto Comercial. Transparencia y Explicabilidad. Datos Personales. Ministerio Público. Investigación Civil.

Sumário: 1. Introdução. 2. Segredo do Negócio. 3. Princípio da Transparência. 4. Explicabilidade. 5. Inquérito Civil. 6. Conclusão. 7. Referências bibliográficas.

1. INTRODUÇÃO

Desde a Convenção de Paris de 1883[2], que teve o Brasil como um de seus signatários originais, a propriedade industrial está harmonicamente protegida no mundo ocidental, de maneira a assegurar exclusividade exploratória e econômica para os proprietários das patentes, marcas, processos e outros conteúdos intelectuais intangíveis. Geralmente durante certo, mas longo, período de tempo fixado em legislação positivada.

E com a natural evolução da sociedade econômica e dos modelos de comércio e negócio também foi se cunhando o conceito de "segredo de negócio", de viés mais fluído e não legislativamente definido no Brasil, mas que sói compreender todo um conjunto de elementos, como informações estratégicas, listas de clientes, métodos de predição e tudo o mais que possa conferir vantagem competitiva e econômica a determinado agente e que segundo a doutrina especializada e a jurisprudência dominante também merece proteção jurídica.

Dado o caráter nitidamente empresarial desses conceitos, as principais demandas jurídicas e judiciais em torno do tema sempre gravitaram no campo do direito concorrencial, colocando, de um lado, o detentor do segredo do negócio, e de outro, os seus supostos violadores, em litígios versando sobre a concorrência desleal, espionagem, quebra de contratos de confidencialidade, responsabilidade civil, etc.

Por outro prisma, o substancial e acelerado desenvolvimento tecnológico experimentado ao longo das últimas décadas, especialmente materializado em potentes algoritmos e sistemas de inteligência artificial generativa, com capacidade para analisar e perfilar gigantescos volumes de dados e "aprender" e tomar decisões de forma automatizada, nas mais distintas áreas da vida humana, também fez surgir justas e relevantes preocupações com o excessivo tratamento de dados de pessoais naturais e a possível violação de garantias individuais.

2. Brasil. *Decreto n.º 9233, de 28 de julho de 1884*. Promulga a convenção assinada em Paris a 20 de março de 1883, pelo qual o Brasil e outros estados se constituem em união para a proteção da propriedade industrial. Disponível em https://www.gov.br/inpi/pt-br/servicos/marcas/arquivos/legislacao/CUP.pdf. Acesso em 24 jul. 2024

Essa perspectiva culminou com a aprovação de normas voltadas à proteção dos dados pessoais e à transparência algorítma, com especial destaque para o Regramento Geral de Proteção de Dados da União Europeia (RGPD) pelo seu caráter inspirador e para a Lei n.º 13.709/2018 (LGPD), que conferiu aos titulares o direito de conhecer sobre o tratamento automatizado de seus dados pessoais.

Acontece que esse cenário fez igualmente surgir um novo ponto de tensão a ser dirimido pelo direito: a necessidade de equilibrar o "segredo do negócio" e a "transparência no tratamento de dados pessoais", com a agravante de que a complexidade de alguns sistemas de IA pode fazer com que o mero reconhecimento do "direito à transparência" não produza o efeito informativo normativamente almejado.

E uma vez que essa dificuldade em conhecer e explicar pode se constituir em relevante óbice à materialização de direitos fundamentais, apresenta-se o inquérito civil como ferramenta constitucional e útil para se conferir maior efetividade ao princípio da transparência, à explicabilidade algorítma, à correção de viéses e consequente promoção da tutela da proteção de dados pessoais em seu aspecto coletivo.

2. SEGREDO DO NEGÓCIO

A legislação brasileira atual reconhece e protege com especificidade a propriedade industrial (Lei n.º 9.279/96[3]), a de softwares computacionais (lei n.º 9.609/98[4]) e a intelectual (Lei n.º 9.610/98[5]). Respeitadas as particularidades naturais de cada tipo de criação e preenchidos os requisitos, de forma geral, essas leis asseguram ao seu titular a fruição de um conjunto de direitos, como o uso exclusivo, licenciamento e venda, bem como a correspondente proteção contra a sua violação.

O cerne desse conjunto de normas está em evitar práticas industriais e comerciais desleais e incentivar a inovação, na medida em que garantindo a percepção exclusiva do benefício econômico da criação se agrega valor ao investimento criativo e se estimula a competitividade e o desenvolvimento

3. Brasil. *Lei n.º 9279, de 14 de maio de 1996*. Regula Direitos e obrigações relativos à propriedade industrial. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9279.htm. Acesso em 24 jul. 2024

4. Brasil. *Lei n.º 9609, de 19 de fevereiro de 1998*. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em:. https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em 24 jul. 2024

5. Brasil. *Lei n.º 9610, de 19 de fevereiro de 1998*. Altera, atualiza e consolida a legislação sobre direitos autorias e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em 24 jul. 2024

econômico. Acrescente-se que, na geopolítica internacional, a proteção do segredo industrial e da inovação estratégica sempre se constituiu em fator de riqueza e poderio influenciador de um país no plano regional e global.

E a esse arcabouço foi se construindo e somando o chamado "segredo do negócio", que segundo a doutrina possui conceito mais amplo e indefinido, abrangendo as informações confidenciais técnicas, comerciais, administrativas, contábeis, financeiras; enfim, todos os "dados que possam interessar e revelar um conteúdo econômico a uma determinada empresa ou atividade".[6]

Sobre a sua envergadura e proteção, tem-se que o Brasil, através do Decreto n.º 1.355/94[7], aprovou e incorporou os Resultados da Rodada Uruguai de Negociações Comerciais Multilaterais do GATT, que em sua Seção 07, artigo 39, versa sobre a proteção de informação confidencial, comprometendo-se que:

> 2. Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu consentimento, de maneira contrária a práticas comerciais honestas10, desde que tal informação:
>
> (a) seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes;
>
> (b) tenha valor comercial por ser secreta; e
>
> (c) tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta.

Na mesma linha, embora em contexto mais estrito - a penalização penal da concorrência desleal e tendo como destinatários participantes de relação contratual ou empregatícia ou que agiram "mediante fraude" -, prevê o artigo 195, da citada Lei n. º 9.279/96, que incide em crime quem "divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços" (incisos XI e XII).

Percebe-se, pois, que o conceito de informação, qualificada ou distinguida apenas pelo seu caráter de confidencialidade e imputação de valor econômico, possui tipologia bastante ampla e pode abarcar incontáveis aspectos de

---

6. Labrunie, J. *A proteção ao segredo do negócio*, *in* Adalberto Simão Filho e Newton De Lucca (coord.), Direito empresarial contemporâneo, 2.ª ed., São Paulo: Juarez de Oliveira, [2004], p. 98

7. Brasil. *Decreto nº 1355, de 30 de dezembro de 1994*. Promulga a Ata Final que Incorpora os Resultados da Rodada Uruguai de Negociações Comerciais do GATT. Disponível em: https://www.gov.br/inpi/pt-br/backup/legislacao-1/27-trips-portugues1.pdf. Acesso em 25 jul. 2024

determinada atividade econômica como ativo intelectual protegível, com a manifesta vantagem de que sua arguição como segredo e consequente defesa não carecem de prévio registro ou de qualquer outro procedimento legal anterior.

Amparada em boa doutrina, sintetiza Kilmar[8]:

> No regime de segredo do negócio como essencialmente delineado no artigo 39(2) do TRIPS, toda essa formalidade, os custos, o tempo e o trabalho atinentes á formalização e deferimento do registro, inexistem. Basta que o ativo intelectual em questão atenda aos já citados requisitos de ser informação sigilosa, cujo valor econômico para o titular derive de seu caráter confidencial e que, por isso mesmo, este faça esforços razoáveis para manter em segredo; e então referido ativo poderá ser resguardado enquanto segredo de negócio.
>
> Ademais, nos termos em que essencialmente delineado no artigo 39(2) do TRIPS o regime de segredos negociais tem potencial de incidência sobre ativos intelectuais diversos. Isso porque, justamente, basta que o ativo em questão atenda aos três requisitos referidos no parágrafo precedente para que possa ser objeto de proteção enquanto segredo negocial. Não se exige, nem mesmo, que referido ativo intelectual esteja sendo efetivamente explorado pelo titular em sua atividade.

Seja pela definição aberta e facilidade de proteção, seja pelo dinamismo inerente ao desenvolvimento e uso das novas tecnologias, seja pelo perfeito e natural enquadramento fático-jurídico, tem-se que o segredo de negócio tem se tornado escudo e base de resguardo dos modelos algoritmos, aprendizagem de máquinas, IA generativa, perfilamento e arranjos de tratamento de bases de dados, etc.

E não se pode negar que o uso de tecnologias de ponta a partir do tratamento de massas de dados implica vantagem competitiva que agrega valor ao negócio ou mesmo constitui a sua própria razão de existir, portanto, merecedora da devida proteção, mormente no campo comercial e concorrencial.

Como observa Costa[9] ao falar da "era da big data":

> A capacidade que os sistemas computacionais hoje possuem ao nível do armazenamento e processamento de informação a alta velocidade permite extrair dos dados um valor económico e social inestimável. Mais do que um mero objeto comercializado, os dados são hoje os responsáveis por alimentar o ecossistema digital.

8. Kilmar, S. G. *O segredo de negócio como direito de propriedade industrial em sentido estrito*. 2023. 59 p. PhD Thesis. Universidade de São Paulo, 2023.

9. Costa, I. S. *A proteção da pessoa na era dos big data*: a opacidade do algoritmo e as decisões automatizadas.2021. 6 p. Revista Electrónica de Direito. RED, 2021.

> O conceito de big data é polissémico: por um lado, refere-se genericamente a conjuntos de dados numa escala massiva, de múltiplas fontes e em distintos suportes; por outro, compreende as tecnologias e processos envolvidos numa "técnica de conversão de fluxos de dados num conhecimento altamente específico"9, nomeadamente, a recolha, o armazenamento e a análise dos dados. Os dados em bruto (raw data), sob a forma de imagens, vídeos, textos ou sons, não possuem per se qualquer valor. O processo de lapidação é levado a cabo por algoritmos, que os analisam e interpretam. É sobretudo através da descoberta de padrões e correlações entre bases de dados extensas (data mining)10 que estes algoritmos convertem os dados em informação, rectius, numa nova forma de conhecimento potencialmente lucrativa, e permitem a transformação de informações aparentemente irrelevantes em ativos valiosos11.

Tanto que mesmo as leis brasileiras vocacionadas à regulamentação e proteção do direito das pessoas na era digital, como a que estabeleceu o marco civil da internet (Lei n. 12.965/2014[10]) e a LGPD (Lei n.º 13.709/2018[11]), contam com disposições que fazem expressa menção à necessidade de respeito e observância dos segredos empresariais e industriais, restando estabelecer qual a verdadeira altura desse muro em relação aos direitos individuais e coletivos relacionados à transparência no tratamento dos dados pessoais.

3. PRINCÍPIO DA TRANSPARÊNCIA

Se a tecnologia, notadamente os diversos modelos de IA, de um lado, trouxe relevantes avanços e benefícios para a sociedade, como os diagnósticos médicos avançados, os usos agrícolas para o incremento da produção de alimentos, a automação de processos industriais com ganhos de produtividade, a otimização de sistemas de negócios com relevantes ganhos de eficiência e assertividade – todos dignos de proteção sob a batuta do segredo do negócio -, de outro, tem capacidade para produzir resultados reprováveis e atentatórios de importantes garantias, como a quebra do direito à privacidade, a violação de direitos do consumidor, a discriminação, o racismo, etc.

Os algoritmos são fórmulas ou modelos matemáticos precisos pensados para resolver problemas específicos. O correto atingimento de sua finalidade depende de sua correta parametrização e de grandes amostras de dados, em

10. Brasil. *Lei n.º 12965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 26 jul 2024.

11. Brasil. *Lei n.º 13709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 26 jul 2024.

especial dados das pessoas, para encontrar os padrões de probabilidade e agrupamento.

São, portanto, fruto da criação e das escolhas humanas, e que também podem refletir a desigualdade, o preconceito e os erros de percepção e análise presentes em uma determinada sociedade, silenciosamente registrados sob a forma de incontável volume de dados (maus dados, maus resultados).

Apresentou-se, pois, um relevante dilema ético a exigir resposta jurídica aos desafios da tecnologia, à essa possibilidade de ser agressiva à vida das pessoas, de perfilar até mesmo a personalidade e manipular as emoções e escolhas e de tirar do ser humano o controle de seus próprios dados pessoais.

Nessa quadra, uma das principais e mais articulada providência foi a aprovação do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR[12]), "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", com a indisfarçável finalidade de conferir à pessoa natural maior controle e conhecimento sobre a coleta e uso dos dados e informações pessoais em um contexto sócio-econômico marcado pela utilização massificada de dados pessoais.

E ainda que não seja escopo deste trabalho, vale acrescentar que a União Europeia já deu um passo à mais na discussão dos efeitos da IA sobre a vida das pessoas e no seu necessário domínio, também aprovando o Regulamento Europeu sobre Inteligência Artificial (AI Act[13]), que dentre seus importantes considerando, destaca que:

> (28) Além das suas inúmeras utilizações benéficas, a IA, pode também ser utilizada indevidamente e conceder instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e abusivas e deverão ser proibidas por desrespeitarem valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como os direitos fundamentais consagrados na Carta, nomeadamente o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças.

De toda sorte, inspirada na normativa europeia de proteção de dados, foi sancionada a Lei n.º 13.709/2018 (LGPD), focada na "proteção dos direitos

12. União Europeia. (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados*). Jornal Oficial da União Europeia

13. União Europeia. (2024). *Regulamento (EU) 2024/0138 do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da união (COM/2021/206 final*). EUR-Lex

fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, apontando como um de seus fundamentos a "autodeterminação informativa" (art. 2º, inciso II) e como um dos seus princípios a "transparência" (art. 6º, inciso VI).

A autodeterminação informativa constitui uma das bases em que se alicerça o sistema de proteção da pessoa natural no que tange à proteção de dados pessoais, porque empodera o cidadão sobre o seu uso. A estruturação jurídica dos direitos do titular está permeada pela necessidade de lhe ser fundamentalmente assegurada a autoderminação, o que naturalmente exige ter claro e suficiente conhecimento sobre todos os tipos de tratamento de seus dados pessoais.

É com isso em mira que a norma assenta como princípio a transparência, ou seja, a necessidade de externar para os titulares em geral "informações claras, precisas e ostensivas" sobre o tratamento de dados pessoais que se empreende, e que para o titular em particular se amplia para abranger o dever de fornecer informações claras e adequadas "a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada" que lhe atinge, conforme expressamente dispõem os artigos 9º e 20, § 1º, ambos da LGPD.

O princípio da transparência em cenários em que existe o emprego de sistemas de inteligência artificial e a presença de dados pessoais, portanto, como pontua Santana[14], denota:

> duas posturas complementares por parte dos agentes de tratamento: uma postura ativa e outra reativa. Ativamente o agente de tratamento deve fornecer ostensivamente uma série de informações, dentre as quais o fato de o titular encontrar- -se sujeito a uma I.A. e uma explicação a respeito do significado desta informação. Por sua vez, passivamente, isto é, mediante requisição do titular, a organização deve fornecer informações suficientes sobre um determinado resultado do sistema, que permita, ao titular, uma compreensão razoável de seu significado e como ele foi alcançado, de modo, inclusive, a ser apto a questioná-lo, se assim entender adequado.

Sucede que, nas mesmas passagens em que estabelece o direito à transparência sobre o tratamento dos dados pessoais, a LGPD igualmente prevê, como aparente limitador, a necessidade de observância "dos segredos comercial e industrial". Aliás, são várias as situações em que a Lei menciona o segredo comercial e industrial, havendo inclusive quem as veja como uma "hipótese de exceção de incidência de normas fundamentais que visam a proteger dados pessoais de indivíduos"[15].

14. Santana, J. M. D. *Inteligência artificial no contexto da proteção de dados*: garantindo-se a transparência com o titular. 2023. 16 p. 1º Prêmio Danilo Doneda de Monografias: ANPD Autoridade Nacional de Proteção de Dados, Brasília-DF, 2023.

15. Ibid. nota 7. 51 p.

Todavia, cabe ponderar desde logo que a proteção dos dados pessoais da pessoa natural se insere nos chamados direitos da personalidade, ou seja, tutelam a própria integridade do ser humano. Assim, mesmo antes da Promulgação da Emenda Constitucional n.º 115/2022[16], que elevou a proteção dos dados pessoais à condição de direito fundamental, no aspecto axiológico do direito, tem-se que sempre ocupou patamar normativo destacado e digno de compatível envergadura protetiva, uma vez que a dignidade da pessoa humana constitui um dos fundamentos da República Federativa do Brasil. Não se deve, pois, sobrevalorizar juridicamente um interesse econômico – o segredo comercial e industrial -, em detrimento da dignidade da pessoa humana.

Muito embora o direito fundamental à proteção de dados pessoais não se cuide de direito absoluto, incumbe ao Estado proporcionalmente garantir a integridade de seu núcleo essencial, mesmo que isso implique restrição da liberdade individual de guardar segredo, mormente em um contexto em que o detentor do segredo se vale e se apropria dos dados pessoais do titular para obter proveito.

Extrai-se de Sarlet[17] que:

> Assim, se é correto – como leciona Dieter Grimm – que os deveres de proteção, por exigirem intervenções por parte dos órgãos estatais – resultam em restrições de direitos, acarretando, nesta perspectiva, uma redução do âmbito de liberdade individual, tais restrições, vinculadas precisamente à necessidade de proteção de bens fundamentais (além de sujeitas, convém acrescentar, ao regime dos limites dos direitos fundamentais, nomeadamente, o respeito às exigências da proporcionalidade e da garantia do núcleo essencial), têm sempre por escopo a maximização dos direitos fundamentais, visto que as restrições objetivam, no plano geral, mais proteção da liberdade e dos direitos fundamentais das pessoas no âmbito da comunidade estatal.

E a esse propósito, também cabe relembrar que a própria Lei n.º 9.279/96, (i) ao mesmo tempo em que resguardou o segredo industrial e dos negócios, assinalou o seu caráter não absoluto, prevendo no artigo 206 a possibilidade de sua revelação em juízo, "para a defesa dos interesses de qualquer das partes"; (ii) o segredo do negócio está topograficamente situado no capítulo destinado à prevenção da concorrência desleal pelo seu uso e entre atores econômicos, devendo ter seu campo de incidência bastante restringido e

16. Brasil. [Constituição (1988)]. *Emenda Constitucional n.º 115, de 10 de fevereiro de 2022*. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 26 jul 2024.

17. Salet, I. W. *Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988*. Direitos Fundamentais & Justiça, 2020, p. 200-201

ponderado quando em confronto com questões relacionadas à defesa dos direitos da personalidade.

Vale aqui a observação de Frazão[18], no sentido de que "há boas razões para não considerar o segredo de empresa como algo absolutamente intocável ou sacrossanto, de forma a se exigir que, em algumas situações, ele seja sopesado diante de relevantes interesses sociais que possam ser prejudicados em virtude do segredo".

A melhor interpretação, consequentemente, é aquela que reconhece como inafastável em todos os cenários jurídicos a dignidade da pessoa humana, a sua autodeterminação informativa e o direito de conhecer quais e como os seus dados pessoais são tratados, até mesmo por sistemas automatizados, mas que à luz do caso concreto os concilia com a necessidade de assegurar o "desenvolvimento econômico e tecnológico e a inovação" (também integrantes do rol de fundamentos da LGPD), que para as empresas de tecnologia deve se refletir no respeito ao segredo do negócio até o máximo patamar possível, inclusive porque na maior parte das situações importa mesmo ao titular que haja a combinação da lisura e qualidade no tratamento dos dados e clareza e explicabilidade da decisão.

4. EXPLICABILIDADE

Afora a questão econômica do segredo do negócio, em nada serviria ao titular ter o seu direito à transparência observado sob a forma de abertura de códigos-fonte e conhecimento das fórmulas matemáticas que codificam instruções computacionais e orientam o funcionamento do sistema ou mediante informações técnicas compartimentadas, porque a sua complexidade técnica e a sua descontextualização de uso não produziria qualquer efeito produtivo, daí o direito à explicabilidade, como corolário do princípio de transparência.

O direito conferido à pessoa natural de obter "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento" (art. 20, da LGPD), somente se materializa se convertido em explicabilidade sobre todo o processo de tratamento de seus dados pessoais e dos resultados dele advindos, a fim de que possa exercer a sua autodeterminação informativa e igualmente se insurgir contra a eventual violação de seus direitos.

18. Frazão, A. *Transparência de algoritmos x segredo de empresa*. As controvérsias a respeito das decisões judiciais trabalhistas que determinam a realização de perícia no algoritmo da Uber. 2021. 4 p. Disponível em http://www.professoraanafrazao.com.br/files/publicacoes/2021-06-09-Transparencia_de_algoritmos_x_segredo_de_empresa_As_controversias_a_respeito_das_decisoes_judiciais_trabalhistas_que_determinam_a_realizacao_de_pericia_no_algoritmo_da_Uber.pdf. Acesso em 26 jul 2024.

E como os processos envolvendo as IAs e as decisões automatizadas são sempre muito complexos a busca desse desiderato não é simples, descortinando-se à frente todo um espaço que deve ser adequadamente preenchido pelos controladores dos dados e desenvolvedores das tecnologias.

Ressalta Paulo[19], apropriadamente, que a transparência e a explicabilidade:

> tem o condão de destronar a opacidade enquanto a principal característica quando se pensa em sindicabilidade dos algoritmos. Será a partir do antídoto da transparência que a própria defesa do cidadão, a partir do Poder Judiciário ou mesmo de outras instâncias fiscalizatórias ou reguladoras poderão controlar e melhor readequar os mecanismos e as aplicações que tomam decisões de forma autônoma.

Em síntese, o conjunto transparência e explicabilidade, portanto, deve seguir o nível e estar rigorosamente alinhado ao tipo de tratamento e ao uso feito dos dados pessoais, partindo das informações básicas, como a identidade do responsável pelo tratamento, rol de dados pessoais coletados, sua finalidade, base jurídica, compartilhamento, tempo de tratamento, natural e necessariamente evoluindo para lealmente informar o eventual uso de dados pessoais não obtidos diretamente do titular e sua procedência, a tomada de decisões através de ferramenta automatizada, a categorização e a formação de perfis e a lógica aplicada.

A finalidade é fornecer ao ser humano comum conhecimento para que, a seu exclusivo juízo, sem muito desforço ou embaraço, seja capaz de compreender o uso de seus dados pessoais, ter dúvidas sobre seu uso e obtenção e refletir sobre questões corriqueiras de sua vida, tais como: Eu preciso informar todos esses dados pessoais para comprar um remédio em uma farmácia ou para disputar uma vaga de emprego? E como serão guardados e utilizados esses dados? Será que servirão para formar o meu perfil de consumo? Houve uso de IA no meu processo de seleção para emprego? Posso ter sido discriminada por ser mulher, negro ou residir em determinado CEP? Será que meu empréstimo foi negado por que meu "score" de crédito é baixo? Mas quais dados foram utilizados para a sua formação? Será que estão corretos? Meus dados são decorrentes de coleta em fontes públicas, mais quais? Será que os dados utilizados pela IA não são produto de crime, como os obtidos através do acesso indevido a base do INSS ou outro órgão governamental? E os aplicativos de redes sociais, quais dados pessoais realmente coletam e para quais finalidades? Como posso me opor ao tratamento ou pedir a eliminação dos dados?

19. Paulo. L. M. *Opacidade dos Algoritmos e a Necessidade de Transparência*: Garantindo Explicabilidade. 2023. 18 p. Anais do Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea. Mostra Internacional de Trabalhos Científicos. 2023

As indagações podem ser quase incontáveis e sempre que o ser humano entender que o tratamento foi "irregular" e lhe causou danos, em seu benefício, a legislação lhe assegura que, no processo civil, o juiz poderá "inverter o ônus da prova em seu favor", mormente quando reconhecida a sua "hipossuficiência para fins de produção de provas ou quando a produção da prova pelo titular resultar-lhe excessivamente onerosa", nos termos do artigo 42, § 2º, da LGPD.

No entanto, embora não pareça exagerado afirmar que na era da *big data* o uso de sistemas automatizados e diversificados tipos de IA embasados no massivo tratamento de dados pessoais está disseminado em todos os setores da sociedade, e por maior que seja o debate público sobre o tema, na seara jurisdicional, ainda não se observa substancial volume de demandas relacionadas ao tratamento de dados pessoais, talvez porque: (i) em razão de sua natureza abstrata e imaterial não são facilmente percebidos como passíveis de proteção e reparação pelo cidadão comum; (ii) justamente em razão do uso massificado de dados pessoais nem sempre é perceptível para o titular o tratamento irregular e a violação de seu direito no plano individual. E é nesse contexto que se faz mais necessário considerar a proteção dos direitos em sua dimensão coletiva.

5. INQUÉRITO CIVIL

A LPGD faz importantes referências aos aspectos coletivos da tutela do direito. Assim, ao cuidar dos direitos e interesses do titular, dispõe que a sua defesa poderá ser feita individual ou coletivamente e que podem ser utilizados os instrumentos de tutela coletiva (art. 22), bem como que a responsabilização e o ressarcimento pelos danos causados se estende aos de natureza coletiva e podem ser judicialmente buscados através das ações coletivas (art. 42, *caput* e § 3º).

Inequívoco, portanto, que a nova lei foi concebida para dialogar e integrar o microssistema técnico e processual de defesa dos interesses difusos e coletivos, composto pelas Leis n. 7.347/85[20] (LACP) e 8.078/90[21] (CDC). Arcabouço jurídico finalizado com a promulgação da Emenda Constitucional n.º 115/2022, que inseriu a proteção de dados pessoais no rol de direitos e garantias fundamentais.

---

20. Brasil. *Lei n.º 7347, de 24 de julho de 1985*. Disciplina a ação civil pública de responsabilidade por danos causados ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico e dá outras providências. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm. Acesso em 29 jul 2024.

21. Brasil. *Lei n.º 8078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 29 jul 2024.

No ponto, observam Zanatta e Souza[22] que:

> Em síntese, a partir da leitura conjunta do art. 22 com o art. 42 da LGPD, bem como os dispositivos da Lei da Ação Civil Pública e do Código de Defesa do Consumidor, pode-se afirmar com segurança que a legislação brasileira (i) permitirá uma atuação repressiva, em nível administrativo, para a tutela da proteção de dados pessoais, valendo-se do microssistema de proteção dos direitos difusos, (ii) fomentará a atuação de entidades civis especializadas e do Ministério Público na tutela dos direitos difusos de proteção de dados pessoais, por meio do poder judiciário, e (iii) possibilitará o uso de um ferramental do processo civil brasileiro para interrupção de violações de direitos assegurados na LGPD, tornando a dinâmica regulatória mais complexa.

E quando se fala da defesa de direitos fundamentais em sua expressão coletiva, cumpre colocar em relevo o papel do Ministério Público brasileiro, por seus diversos ramos, *ex vi* do disposto no artigo 127, *caput*, da Constituição da República[23], que incumbe-lhe promover a defesa dos "interesses sociais e individuais homogêneos" e sua legitimidade para a promoção do "inquérito civil e a ação civil pública", nos termos do artigo 129, inciso III, da CF.

Contudo, diferentemente do que acontece com a ação civil pública, em que a legislação confere legitimação a outros atores jurídicos, o inquérito civil constitui ferramenta de manejo exclusivo do Ministério Público para a defesa de interesses difusos e coletivos. Como explica Mazzilli[24], cuida-se de procedimento administrativo destinado a "colher elementos de convicção para que, à sua vista, o Ministério Público possa identificar ou não a hipótese em que a lei exige sua iniciativa na propositura de alguma ação civil pública".

Concebido pela Lei n.º 7.347/85 (LACP) e elevado ao nível constitucional para dar sustentação procedimental ao também constitucional poder requisitório do Ministério Público (art. 129, inciso VI, da CF), em sua vertente original, apresenta-se como um valioso, idôneo e estratégico instrumento para a coleta de informações, aquisição de conhecimento sobre os fatos e consequente adensamento do conjunto probatório com foco na tutela do direito pela via jurisdicional.

Mas vai além disso.

Igualmente pautado nos princípios democráticos e igualitários e na relevante missão do Ministério Público de ser o guardião ativo dos valores

---

22. Zanatta, R. A. F.; Souza, M. A tutela coletiva na proteção de dados pessoais: tendências e desafios. De Lucca*, N.;* Rosa*, C.. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin*, 2019

23. Brasil. [Constituição (1988)]. *Constituição da República Federativa do Brasil. Brasília-DF*. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 29 jul 2024.

24. Mazzilli, H. N. *Pontos controvertidos sobre o inquérito civil*. Ação Civil Pública–Lei. 2000. 4 p.2000.

constitucionais, converte-se em campo apropriado para o diálogo humano e a construção participativa de soluções. Como pontua Cavaco[25], "o subjacente pluralismo ínsito às contendas coletivas impõe uma maior amplitude dialética à procedimentalização do inquérito civil, premissa básica a possibilitar a construção do consenso desjudicializado".

No bojo do inquérito civil ambas as vertentes se entrecruzam, permitindo lançar luz sobre os diversos fatores de opacidade das novas tecnologias através do exercício do poder requisitório e instrutório e, ao mesmo tempo, com a devida temperança, buscar a construção das alternativas à necessária maior transparência e assertividade no tratamento dos dados dos titulares.

A partir da situação concreta e da sua particular complexidade, abre-se um leque de possibilidades, podendo-se ilustrativamente citar:

a) Perquirir se o controlador informa os titulares, em linguagem adequada, no tempo oportuno e com a visibilidade necessária quais exatamente os dados coletados, o embasamento e todos os seus usos, a lógica do tratamento automatizado, seu tempo de guarda e forma de eliminação, as medidas de privacidade e segurança que adota, etc;

b) Aferir se o titular tem facilitado o acesso aos seus dados e ao Encarregado de Dados do controlador, a proceder às correções necessárias, a exercer a portabilidade e os direitos inerentes ao consentimento;

c) Obter conhecimento sobre a origem e os tipos de dados pessoais utilizados em tratamentos automatizados para chegar a determinado resultado, aferir a sua relevância contextual e se apresenta a explicabilidade necessária, em especial quando se vislumbrar a possibilidade de discriminação algorítma, violação à privacidade ou de outro direito fundamental;

Durante a sua tramitação, por um lado, faz-se possível colher informações e documentos, ouvir especialistas, realizar exames e perícias e requisitar serviços específicos inclusive de ordem técnica à administração pública (art. 8º, § 1° da LACP), - medidas que podem ser relevantes em se cuidando de transparência algorítma e suas consequências e que podem de alguma maneira reduzir o desequilíbrio técnico em relação ao detentor dos dados e da tecnologia -, e de outro, estabelecer imediato contato com o agente de tratamento para compreender sua perspectiva, conhecer as práticas e informações que considera integrar o "segredo do negócio" e ponderar sobre a sua juridicidade, etc.

25. Cavaco, B. de S. B. O Inquérito Civil como Instrumento Efetivo e Resolutivo na Tutela dos Interesses Transindividuais–Desjudicialização, Contraditório e Participação. *Revista do Ministério Público do Rio de Janeiro*, Rio de Janeiro, v. 59, 95 p, 2016.

Ao final, caso os elementos coligidos apontem para a violação de direitos e necessidade de aprimoramento do modelo de tratamento, a solução poderá se dar pela via consensual, normalmente mediante a assinatura de Termo de Ajustamento de Conduta, ou pelo manejo da Ação Civil Pública ou Ação Civil Coletiva.

E é preciso deixar claro que o Ministério Público tem operado nessa linha, porém, de maneira pontual, notadamente em relação à grandes agentes e envolvendo fatos de notória repercussão, mas na atual quadra do desenvolvimento tecnológico e informacional, em que as ferramentas automatizadas e o tratamento massivo de dados está disseminado na sociedade, afigura-se imperioso conferir escalabilidade à atuação do Ministério Público brasileiro a partir de sua vantajosa ramificação institucional (MPT, MPF, MPE, MPDFT, MPM) e de sua capilaridade nacional, a fim de dar concretude às garantias constitucionais da privacidade, não discriminação e proteção de dados pessoais e transmitir segurança à sociedade quanto ao seu uso e mitigação de riscos no mundo da *big data*.

Com esse intuito, vale destacar que o Conselho Nacional do Ministério Público (CNMP) aprovou a Resolução n.º 281, de 12 de dezembro de 2023, instituindo a "Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público"[26], e determinando em seu artigo 56 que "os ramos e as unidades do Ministério Público deverão promover a estruturação de suas promotorias e procuradorias para atuação na defesa da ordem jurídica e da dimensão coletiva do direito à proteção aos dados pessoais, diante de violações à legislação por pessoas físicas ou jurídicas, de direito público ou privado".

Cuida-se de dispositivo de evidente vanguarda que deve estimular a cultura da proteção de dados pessoais como prática social a ser perseguida e respeitada, operando positivamente para aproximar e envolver a sociedade civil na saudável discussão de tão importante assunto. E a atuação finalística do Ministério Público costuma se iniciar pelo inquérito civil. Que seu resultado seja alvissareiro.

6. CONCLUSÃO

Pelo presente artigo procurou-se fazer compreender que o segredo do negócio sempre teve seu embasamento jurídico na seara empresarial e concorrencial, buscando evitar práticas copiosas desleais e preservar os benefícios econômicos dos responsáveis pela inovação. Entretanto, com

26. CNMP – Conselho Nacional do Ministério Público. Resolução n.º 281, de 12 de dezembro de 2023. Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público e dá outras providências. Disponível em https://www.cnmp.mp.br/portal/atos-e-normas/norma/10515/. Acesso em 27 jul 2024

o notável desenvolvimento tecnológico experimentado pela sociedade contemporânea, destacadamente a partir da capacidade de reunir e analisar grandes volumes de informação, adveio a preocupação e a necessidade de se conferir transparência e explicabilidade ao tratamento aplicado aos dados pessoais.

O melhor caminho será sempre tentar conciliar o segredo do negócio e a transparência do tratamento, uma vez que ambos possuem sua sustentação jurídica, mas a alegação de segredo não pode se sobrepor ao direito humano de claramente conhecer os tratamentos feitos com seus dados pessoais e a lógica de decisões automatizadas. E também não pode encobrir resultados atentatórios a direitos fundamentais gerados a partir de bases de dados não confiáveis, aplicadas fora de contexto ou proveniente de erro de programação.

O assunto costuma se mostrar complexo do ponto de vista técnico e em regra alcança direitos difusos e coletivos, daí a importância da participação ativa do Ministério Público em seu enfrentamento e no desenvolvimento da cultura da proteção de dados pessoais, propondo-se que essa atuação se incremente a partir do inquérito civil, instrumento com embasamento constitucional, dotado da instrumentalidade e da dinâmica necessária para a devida compreensão e comprovação de vícios no tratamento de dados pessoais e consequente encaminhamento da proposta de solução, através de Termo de Ajustamento de Conduta consensualmente firmado ou mediante o manejo da Ação Civil Pública.

7. REFERÊNCIAS BIBLIOGRÁFICAS

Cavaco, B. de S. B. O Inquérito Civil como Instrumento Efetivo e Resolutivo na Tutela dos Interesses Transindividuais–Desjudicialização, Contraditório e Participação. *Revista do Ministério Público do Rio de Janeiro*, Rio de Janeiro, v. 59, 95 p, 2016.

Costa, I. S. *A proteção da pessoa na era dos big data*: a opacidade do algoritmo e as decisões automatizadas.2021. 6 p. Revista Electrónica de Direito. RED, 2021.

Da Silveira, S. A.; **Da Silva**, T. R. Controvérsias sobre danos algorítmicos: Discursos corporativos sobre discriminação codificada. *Revista Observatório*, 2020, 6.4: a1pt-a1pt

Frazão, A. *Transparência de algoritmos x segredo de empresa*. As controvérsias a respeito das decisões judiciais trabalhistas que determinam a realização de perícia no algoritmo da Uber. 2021. 4 p.

Fujimoto, M. Y.. *Segredo de negócios, proteção de dados pessoais e inteligência artificial* - os desafios do diálogo. 2023. PhD Thesis. Universidade de São Paulo. 2023.

Hoffmann-Riem, W.. *Proteção de dados e inteligência artificial*: perspectivas éticas e regulatórias. *Revista Direito Público, Porto Alegre*, 2019.

Kilmar, S. G. *O segredo de negócio como direito de propriedade industrial em sentido estrito*. 2023. 59 p. PhD Thesis. Universidade de São Paulo, 2023.

Labrunie, J. *A proteção ao segredo do negócio*, *in* Adalberto Simão Filho e Newton De Lucca (coord.), Direito empresarial contemporâneo, 2.ª ed., São Paulo: Juarez de Oliveira, [2004], p. 98.

Mazzilli, H. N. *Pontos controvertidos sobre o inquérito civil*. Ação Civil Pública–Lei. 2000. 4 p.2000.

Paulo. L. M. *Opacidade dos Algoritmos e a Necessidade de Transparência*: Garantindo Explicabilidade. 2023. 18 p. Anais do Seminário Internacional de Demandas Sociais e Políticas Públicas na Sociedade Contemporânea. Mostra Internacional de Trabalhos Científicos. 2023.

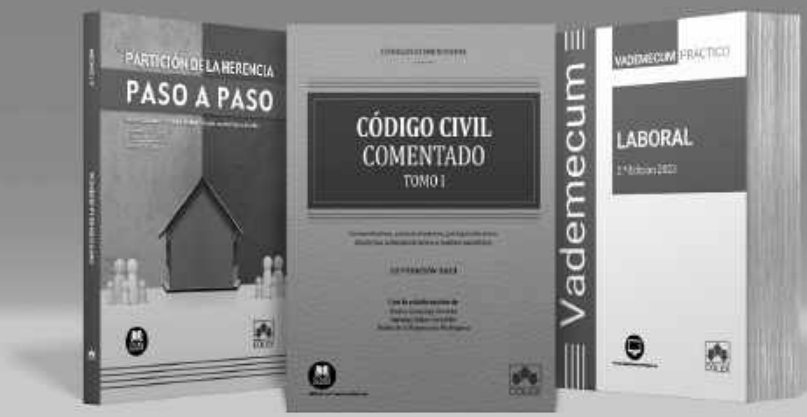
Salet, I. W. *Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988*. Direitos Fundamentais & Justiça, 2020, p. 200-201.

Santana, J. M. D. *Inteligência artificial no contexto da proteção de dados*: garantindo-se a transparência com o titular. 2023. 16 p. 1º Prêmio Danilo Doneda de Mografias*:* ANPD Autoridade Nacional de Proteção de Dados, Brasília-DF, 2023.

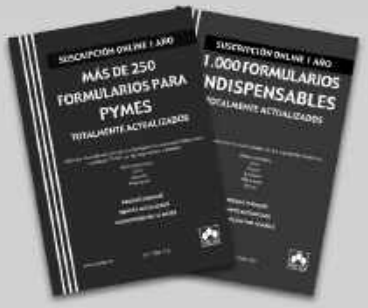
Zanatta, R. A. F.; **Souza**, M. A tutela coletiva na proteção de dados pessoais: tendências e desafios. De Lucca*, N.;* Rosa*, C.. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin*, 2019.

COLEX

LA EDITORIAL JURÍDICA DE REFERENCIA PARA LOS PROFESIONALES DEL DERECHO **DESDE 1981**

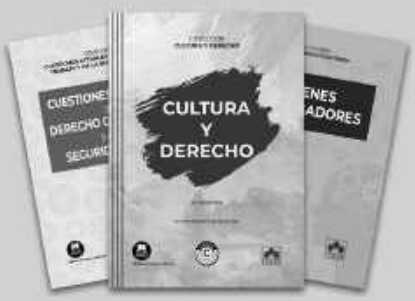


Paso a paso | Códigos comentados | Vademecum



Formularios

Flashes formativos



Colecciones científicas

DESCUBRA NUESTRAS OBRAS EN:

www.colex.es

Editorial Colex SL Tel.: 910 600 164 info@colex.es

A PROTEÇÃO DE DADOS PESSOAIS SOB A ÓTICA DO MINISTÉRIO PÚBLICO BRASILEIRO

Atualmente, a proteção de dados pessoais consolidou-se no Brasil como um verdadeiro direito fundamental, seguindo os passos da Espanha e de outros países da União Europeia. Isso é fruto de uma longa trajetória que se iniciou com os primeiros debates sobre privacidade por volta de 1990 e culminou com a promulgação da Emenda Constitucional 115, que lhe conferiu o status jurídico máximo no ordenamento jurídico brasileiro, classificando a proteção de dados como um dos Direitos Fundamentais previstos em sua Constituição Federal.

Nesse contexto, diferente de muitos outros países, o Ministério Público brasileiro assume papel central e distinto em sua defesa, possuindo amplas e diversas competências constitucionais para proteger os direitos dos cidadãos na esfera digital, que vão desde a fiscalização do cumprimento normativo por entes públicos e privados até a promoção de ações civis públicas e a defesa coletiva dos titulares de dados pessoais.

Assim, este é um livro essencial para a compreensão das dimensões da proteção de dados pessoais no Brasil sob a ótica de uma das mais importantes Instituições estatais, pois, esta obra dá voz aos Encarregados pelo Tratamento de Dados Pessoais do Ministério Público brasileiro, figura-chave prevista na Resolução 281/2023, do Conselho Nacional do Ministério Público (CNMP), com responsabilidades específicas relacionadas à governança e ao monitoramento do cumprimento da proteção de dados pessoais.

DIRETORES

João Santa Terra Júnior, Anxo Varela Hernández, Andrea Willemin.

AUTORIA

Maria Fernanda Tonini Blazius de Oliveira, Rui Carlos Kolb Schiefler, Jorge Augusto Caetano de Farias, Cláudia Pessoa Marques da Rocha Seabra, Andrea Cristina de Sousa Fialho, Francisco de Carvalho Neto, Lauro Francisco da Silva Freitas Júnior, Leonardo Andrade Macedo, Daniel Teixeira Bezerra, Ana Paula Machado Franklin, Carlos Renato Silvy Teive, Guilherme Magalhães Martins, Paulo Roberto Gonçalves Ishikawa, José Fernando Ruiz Maturana.

ISBN: 979-13-7011-277-6

9 791370 112776

O.A.