MPF
Ministério Público Federal

ROTEIRO DE ATUAÇÃO

SISTEMA BRASILEIRO DE PROTEÇÃO E ACESSO A DADOS PESSOAIS:

ANÁLISE DE DISPOSITIVOS DA LEI DE ACESSO À INFORMAÇÃO, DA LEI DE IDENTIFICAÇÃO CIVIL, DA LEI DO MARCO CIVIL DA INTERNET E DA LEI NACIONAL DE PROTEÇÃO DE DADOS

3ª Câmara de Coordenação e Revisão

III

SISTEMA BRASILEIRO DE PROTEÇÃO E ACESSO A DADOS PESSOAIS:

ANÁLISE DE DISPOSITIVOS DA LEI DE ACESSO À INFORMAÇÃO, DA LEI DE IDENTIFICAÇÃO CIVIL, DA LEI DO MARCO CIVIL DA INTERNET E DA LEI NACIONAL DE PROTEÇÃO DE DADOS

MINISTÉRIO PÚBLICO FEDERAL

Procuradora-Geral da República
Raquel Elias Ferreira Dodge

Vice-Procurador-Geral da República
Luciano Mariz Maia

Vice-Procurador-Geral Eleitoral
Humberto Jacques de Medeiros

Ouvidor-Geral do Ministério Público Federal
Juliano Baiocchi Villa-Verde de Carvalho

Corregedor-Geral do Ministério Público Federal
Oswaldo José Barbosa Silva

Secretário-Geral
Alexandre Camanho de Assis

Secretária-Geral Adjunta
Eloá Todarelli Junqueira

MINISTÉRIO PÚBLICO FEDERAL
3ª CÂMARA DE COORDENAÇÃO E REVISÃO

ROTEIRO DE ATUAÇÃO

SISTEMA BRASILEIRO DE PROTEÇÃO E ACESSO A DADOS PESSOAIS:

ANÁLISE DE DISPOSITIVOS DA LEI DE ACESSO À INFORMAÇÃO, DA LEI DE IDENTIFICAÇÃO CIVIL, DA LEI DO MARCO CIVIL DA INTERNET E DA LEI NACIONAL DE PROTEÇÃO DE DADOS

Volume 3

Brasília – DF
MPF
2019

Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr3/publicacoes.

Dados Internacionais de Catalogação na Publicação (CIP)

B823s

Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 3.
Sistema brasileiro de proteção e acesso a dados pessoais : análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados – Brasília : MPF, 2019.
85 p. – (Roteiro de Atuação ; v. 3)

Disponível em: <www.mpf.mp.br>.

1. Proteção de dados pessoais - Brasil. 2. Direito à informação - Brasil. 3. Direito à privacidade - Brasil. 4. Ministério Público Federal – atuação. I. Título. II. Série.

CDDir 341.2732

Elaborado por Isabella de Oliveira e Nóbrega – CRB 1/3131

3ª CÂMARA DE COORDENAÇÃO E REVISÃO

Titulares:

Coordenador - Augusto Aras
Subprocurador-Geral da República

Alcides Martins
Subprocurador-Geral da República

Brasilino Pereira dos Santos
Subprocurador-Geral da República

Suplentes:

Maria Emília Moraes de Araújo
Procuradora Regional da República, PRR 3ª Região/São Paulo

Luiz Augusto Santos Lima
Procurador Regional da República, PRR 1ª Região/Brasília

Marcus Vinícius Aguiar Macedo
Procurador Regional da República, PRR 4ª Região/Porto Alegre

Autores e revisores:

Carlos Bruno Ferreira da Silva
Coordenador do GT
Procurador da República no Distrito Federal - PR-DF

Lúcio Mauro Carloni Fleury Curado
Procurador da República no Município de São Carlos/SP

Alexandre Assunção e Silva
Procurador da República no Piauí - PR-PI

Manoel Antônio Gonçalves da Silva
Procurador da República no Município de Arapiraca/AL

Planejamento visual e diagramação:
Héber Peixoto Sabino / Secretaria de Comunicação Social (Secom)

Revisão de texto:
Ana Paula Rodrigues de Azevedo / Secom
Fernanda Gomes Teixeira de Souza / Secom

Normalização Bibliográfica:
Coordenadoria de Biblioteca e Pesquisa (Cobip)

Procuradoria-Geral da República
SAF Sul, Quadra 4, Conjunto C
Fone (61) 3105-5100
70050-900 - Brasília - DF

www.mpf.mp.br

Sumário

APRESENTAÇÃO

Este projeto é fruto da intenção do Grupo de Trabalho de Tecnologias da Informação e Comunicação e da 3ª Câmara de Coordenação e Revisão do Ministério Público Federal de produzir doutrina e popularizar a temática de proteção de dados no nosso país.

A proposta é que essa seja a primeira edição de uma obra a ser atualizada e expandida, agregando novos temas e autores, de forma a servir como texto de consulta sempre útil aos procuradores da República com interesse no tema, bem como para a população em geral.

O objetivo é trazer ao leitor textos de caráter atual e instigantes, que permitam reflexionar e debater as possíveis regulações jurídicas sobre a informática no campo cível. Queremos trazer ao público geral as inquietações e conclusões que surgem dos debates diuturnos que os membros do GT travam no seu grupo de mensagens, muitas vezes em reflexo de notícias de periódicos, o que demonstra uma realidade que não nos permite mais fugir desse enfrentamento. Ao contrário, devemos explorar os potenciais das novas tecnologias de modo a trazer um cenário de concorrência, pujança econômica e respeito ao consumidor cada vez mais firme para nosso país.

1 INTRODUÇÃO

Carlos Bruno Ferreira da Silva

O avanço da circulação de informações no mundo atual evidencia que não é despropositada a alcunha de que vivemos hoje em uma "sociedade de informação". Quando nos referirmos aqui à "Sociedade de Informação" como caracterizador do momento atual da experiência humana, fazemo-lo admitindo que podemos caracterizar o modo de desenvolvimento atual como baseado na informação, assumindo-o como núcleo de importantes transformações na esfera econômica, de poder e cultural. Assim, enquanto a Revolução Industrial definiu bases econômicas que buscavam eminentemente o aumento da produção por meio de maquinário alimentado por novas fontes de geração e distribuição de energia, hoje, mesmo que esse ideal não tenha sido evidentemente abandonado, há uma centralidade na busca de procedimentos que permitam a evolução crescente das tecnologias de processamento, informação e comunicação, impulsionados pelo reconhecimento de que essas técnicas compõem hoje o eixo da riqueza e do poder mundiais[1].

Podemos dizer que a terminologia sociedade de informação "representa una forma de economía y un tipo de sociedad postindustrial en la que el protagonismo de la producción y de la distribución de bienes parece desplazarse hacia una sociedad de servicios en cuyo centro se sitúa la obtención, procesamiento y distribución de información"[2].

Isso não significa menosprezar a importância da informação em épocas passadas, nem o impacto de desenvolvimentos como a invenção do papel ou as melhorias nas técnicas de impressão e tipografia realizadas por Johannes Gutenberg, mas sim assumir que só agora há a proeminência dos meios para aproveitá-los integralmente, por meio da potencialidade incomparável de relacionar aquilo que era existente antes com o que a informática e o texto eletrônico forneceram para o armazenamento de dados e a consequente acumulação de conhecimento, ainda mais quando combinados com um estágio comunicacional que permite acesso instantâ-

1 CASTELLS, Manuel. **A Sociedade em Rede**. São Paulo: Paz e Terra, 2007, p. 61. (A Era da Informação: Economia, Sociedade e Cultura, v. 1).

2 BARNES VÁZQUEZ, Javier. Sobre el procedimiento administrativo: evolución y perspectivas. In: _____. (coord.). **Innovación y reforma en el derecho administrativo**. Sevilla: Derecho Global, 2006, p. 301.

neo a qualquer ponto do planeta, evidentemente modificando nossa relação com o espaço e o tempo. Há assim duas grandes modificações na sociedade e na economia que são dignas de destaque. Por um lado, houve uma valorização da quantidade e do alcance da produção eminentemente intelectual, veiculada por meio de mídia. Ademais, de uma forma mais geral, a interligação gerou um mercado de trabalho absolutamente ininterrupto e cuja cooperação pode ocorrer sem limitações de proximidade física e simultaneidade[3].

Do ponto de vista de amplitude e velocidade, podemos também traçar uma distinção significativa entre a Revolução Industrial e revolução causada pelas novas "tecnologias da informação". Enquanto aquela ocorreu de maneira gradual e seletiva, primeiro afetando a vida na Grã-Bretanha, e daí se espalhando para o mundo, em diferentes abrangências e épocas, se observamos a História do Estados Unidos, da Europa Ocidental, da América Latina, África e Ásia, pode-se comprovar que a mudança informacional atingiu fortemente todos os cantos do globo em apenas 40 anos[4].

A disseminação rápida da informação dependeu do desenvolvimento acelerado da "informática", entendida como ciência do tratamento automático da informação[5]. As máquinas iniciais, de custo alto e dimensões equivalentes a verdadeiras moradias, foram gradualmente evoluindo para equipamentos que realizam milhões de vezes mais rapidamente as mesmas operações em pequenos circuitos eletrônicos com preço acessíveis a boa parte do indivíduos. É possível mesmo dizer que estamos testemunhando uma 2ª revolução industrial, tendo em vista que o avanço científico nesse campo permitiu transformações econômicas, culturais, sociais e políticas de magnitude semelhante às que sucederam quando a força animal foi substituída pela máquina a vapor[6]. Isso se soma ao igualmente espetacu-

3 TINNEFELD, Marie-Theres; EHMANN, Eugen; GERLING, Rainer W. **Einführung in das Datenschutzrecht**: Datenschutz und Informationsfreiheit in europäischer Sicht. München; Wien: Oldenbourg, 2005, p. 8.

4 Muito embora, evidentemente, possa-se falar em diferentes situações de abertura e estágio tecnológicos, o fato é que esse tipo de tecnologia se tornou de fácil acesso a cada indivíduo, que mesmo a opressão estatal ou pobreza de um país não lhes permitem o isolamento a essa "comunidade de informação global", como demonstra o fluxo constante de dados que podemos receber de países tão distintos como Irã, China, Sudão, Brunei, Honduras ou Albânia. No mesmo sentido, CASTELLS, Manuel. **El Poder de la Identidad**. Barcelona: Alianza Editorial, 1997, p. 286. (La era de la información: economía, sociedad y cultura, v. II).

5 CONDE ORTIZ, Concepción. **La protección de datos personales**: un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid: Dykinson, 2005, p. 13.

6 TÉLLEZ AGUILERA, Abel. **Nuevas tecnologías, intimidad y protección de datos**: con estudio sistemático de la Ley Orgánica 15-1999. Madrid: Edisofer, 2001, p. 22. Sintetiza Bobbio a distância histórica: "Hoje é impossível comparar o conhecimento que um monarca absoluto como Luiz XIII ou Luiz XIV tinha dos próprios súditos com o conhecimento que o governo de um Estado bem organizado pode ter dos próprios cidadãos. Quando lemos as histórias dos jacqueries, reparamos quão pouco conseguia 'ver' o monarca com o seu aparato de funcionários, e como as revoltas estouravam sem que o poder, apesar de absoluto, estivesse em condições de preveni-las, embora não fosse sutil ao reprimi-las" (BOBBIO, Norberto. **O futuro da democracia**. São Paulo: Paz e Terra, 2004, p. 120).

lar desenvolvimento das telecomunicações que permitem praticamente que haja transmissão de dados em tempo real e em qualquer lugar do mundo[7].

É fácil constatar que na economia atual a informação se tornou a matéria-prima de valor mais elevado e o consumidor/eleitor, elemento central do patrimônio das empresas/governos. Com a internet, o marketing de massas pode ser substituído pela propaganda individualizada, o que permite àquele que pretende conquistar oferecer a promessa de dar exatamente o que aquele indivíduo quer ouvir. A vantagem na competição, pela facilidade de acesso a várias ofertas, que a navegação pelos grande sites de busca confere é neutralizada quando o fornecedor recolhe tantos dados sobre as características, hábitos e preferências dos cidadãos particulares do seu público-alvo que conhece suas tendências até melhor do que ele próprio. E se os grandes processadores resolvem o problema do processamento desse total de informações, o recolhimento destas é objeto de estratégias mais sutis.

Há na internet um foco privilegiado para essa coleta involuntária. Na internet, quando estamos identificados (seja por meio de um login ou de um IP já conhecido) durante o acesso a um site e possível à empresa ver, por meio da troca de páginas ou mesmo do deslizar do cursor, todos aqueles elementos que atraem o nosso interesse. Consequentemente, podem-se estabelecer projetos de atendimento personalizado em nossa próxima visita e estimular vontades que talvez fossem inconscientes para nós mesmos. Em âmbito coletivo, uma empresa, por exemplo, pode traçar perfis de usuários com os mesmos perfis socioeconômicos e, assim, estabelecer melhor seus focos de atuação. A primeira e mais comum é a falsa gratuidade de algumas ofertas. Esta não deve ser confundida com as possibilidades de cooperação de trabalho entre profissionais sem direto interesse econômico, com se vê na feitura de softwares de código livre como o Linux e o Open Office. Abordam-se aqui as propostas encontradas com fartura na Grande Rede de certos benefícios ao internauta que dispensam qualquer contraprestação, especialmente a pecuniária, salvo o preenchimento de um "simples" formulário.

Tanto nesses casos quanto em operações de comércio eletrônico ou em qualquer atendimento não presencial (pelo telefone, por exemplo) há frequentemente uma desavisada passagem de dados privados pelo usuário para uma pessoa jurídica[8], que, na ausência de limites legais, poderá utilizá-los ou vendê-los para outra empresa que deseja conhecê-los profundamente. Além dos campos a serem preenchi-

7 LUCAS MURILLO DE LA CUEVA, Pablo. **El derecho a la autodeterminación informativa**: la protección de los datos personales frente al uso de la informática. Madrid: Tecnos, 1990, p. 106.

8 TINNEFELD, Marie-Theres; EHMANN, Eugen; GERLING, Rainer W. **Einführung in das Datenschutzrecht**: Datenschutz und Informationsfreiheit in europäischer Sicht. München; Wien: Oldenbourg, 2005, p. 51.

dos, os quais os analistas preveem que se tornarão passo a passo mais inquisitoriais, adentrando profundamente a intimidade do internauta[9]. Negocia-se também tudo o que pode ser observado a distância pelo dono do site, como a origem do seu IP e os banners que lhe provocaram mais interesse.

Nas redes sociais (como Facebook, Orkut etc.), a retirada de informação necessita de pesquisa[10] de quem quer formar o banco de dados (em regra não é o usuário que vai a ele), mas envolve categorias mais privadas, porque o indivíduo elenca características e opiniões cujo conhecimento o usuário reservaria a amigos e familiares. Pior é quando há técnicas maliciosas de invasão dos computadores pessoais para retirada de informações que não desejamos revelar[11].

Mesmo com o simples uso de computadores e internet, desassociado das situações acima, já se permitem registros. As companhias telefônicas mantêm controle constante de quem utiliza determinado IP naquela hora, e o simples deletar de um arquivo no disco rígido não impede que um perito veja aquele registro posteriormente.

Não só por meio da internet e da telefonia o recolhimento de dados faz parte de nossas vidas. Nas ruas, é trivial sermos fotografados sem percebermos ou câmeras de vigilância gravarem nossas atitudes, e as técnicas de identificação facial automática se veem em franca expansão. O mesmo ocorre no ambiente de trabalho. GPS e veículos mais avançados emitem nossa latitude e longitude atual, frequentemente por nossa vontade para proteção e auxílio no trânsito.

Por fim, o barateamento do uso da identificação pelo DNA na biométrica nos garante com praticamente absoluta certeza asseverar fatos passados com determinados indivíduos e já se falam em cadastros nacionais de dados genéticos dos cidadãos[12]. Além disso, as organizações de medicina utilizam crescentemente técnicas de telemetria, recolhida a distância, de dados sobre pacientes[13], como forma de centralizar (e baratear) os custos de diagnósticos.

---

9 BELLEIL, Arnaud. **@-privacidade**. O mercado de dados pessoais: protecção da vida privada na idade da internet. Lisboa: Instituto Piaget, 2001, p. 21.

10 Isso, claro, quando não é o próprio criador da rede sociais que pretende armazenar e vender as informações escritas sem perguntar ao usuário. Para uma contextualização dessa prática na regulação dos dados pessoais, veja **Grimmelmann**, James. **Saving Facebook**. Iowa: Iowa Law Review, 2009, p. 1195 *et seq*.

11 E, como defesa, surgem os softwares de *firewall* , para controlar o fluxo de dados entre nossos computadores e a rede de computadores, assim como de detecção de vírus (TINNEFELD, Marie-Theres; EHMANN, Eugen; GERLING, Rainer W. **Einführung in das Datenschutzrecht**: Datenschutz und Informationsfreiheit in europäischer Sicht. München; Wien: Oldenbourg, 2005, p. 33).

12 FROOMKIN, A. Michael. The Death of Privacy?. **Stan. L. Rev**., v. 52, p. 1495, 1999.

13 GARCÍA-BERRIO HERNÁNDEZ, Teresa. **Informática y libertades**: la protección de datos personales y su regulación en Francia y España. Murcia: Servicio de Publicaciones de la Universidad de Murcia, 2003, p. 78.

Chegamos à realidade atual, em que há uma série de atividades rotineiras, públicas e privadas, em que o indivíduo se vê, muitas vezes até sub-repticiamente, monitorado e catalogado por outrem. O Governo impõe a todo tempo o preenchimento de formulários para qualquer autorização que concede. Também movimentações bancárias e utilizações de cartão de crédito são constantemente monitoradas, a começar para evitar a lavagem de dinheiro, da criminalidade e do terrorismo. Todos esses cadastros se tornam passíveis de amplos rastreamentos computadorizados[14].

Esse avanço da denominada "telemática", incrementada exponencialmente pela consolidação da internet, torna ainda mais premente a nossa análise sobre o tema do ponto de vista do Direito, tal como técnica do exercício do poder que é, no Estado Moderno[15], pois a transformação da tecnologia garante a existência também de um "Poder Informacional"[16].

Podemos dizer que o setor jurídico tem interesse interno e externo sobre esse novo método de investigação e documentação. Internamente as novas tecnologias permitem arquivar e catalogar a enorme gama de informações ligadas à ciência jurídica, e o acesso a fontes legislativas, jurisprudenciais e doutrinárias que a tecnologia permite aos pesquisadores e operadores do Direito é de uma vastidão que, ao mesmo tempo, aumenta a interligação, facilita as análises e as torna mais completas. O interesse externo, porém, está ligado às soluções e aos problemas jurídicos para a sociedade e os cidadãos advindos da difusão de sistemas de tratamento eletrônico.

O manejo agregado de múltiplos dados individuais, a princípio insignificantes, permite facilmente a análise completa da sua personalidade, tornando-o "transparente" a quem gerencia o arquivo das informações. A mutação das nossas "sociedades de massa" em "sociedades de informação", ao contrário de facilitar a fuga humana da padronização dentro do coletivo, conduziria à hiperclassificação, que atrofia a liberdade pelo excesso de controle[17]. A tecnologia hoje existente torna possível o ideal panóptico, de conseguir a obediência ininterrupta por meio da indicação aos vigiados de que são vistos mesmo quando não são visíveis seus observadores[18].

14 TINNEFELD, Marie-Theres; EHMANN, Eugen; GERLING, Rainer W. **Einführung in das Datenschutzrecht**: Datenschutz und Informationsfreiheit in europäischer Sicht. München; Wien: Oldenbourg, 2005, p. 60.

15 TROPER, Michel. **A filosofia do direito**. São Paulo: Martins Editora, 2008, p. 70.

16 TINNEFELD, Marie-Theres; EHMANN, Eugen; GERLING, Rainer W. **Einführung in das Datenschutzrecht**: Datenschutz und Informationsfreiheit in europäischer Sicht. München; Wien: Oldenbourg, 2005, p. 1.

17 RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**. Rio de Janeiro: Editora Renovar, 2008, p. 157.

18 FOUCAULT, Michel. **Vigiar E Punir**: Historia da Violência nas Prisões. Petrópolis: Vozes, 2004, p. 165.

A proteção dos dados pessoais explicita que aquele cuja informação consta em um banco de dados não é um mero fornecedor de informação, mas um ser humano cujo dado registrado participa e influencia a sua experiência como ser humano. Ao garantir ao indivíduo direitos sobre a circulação e o uso dos seus dados, esse direito fundamental sublinha a importância de não se considerar o homem como meio ou objeto de determinadas estratégias ou políticas, mas sempre como elemento primordial de valorização pela ação estatal[19].

Porém a progressiva aceitação da inevitabilidade e continuidade do avanço da técnica mudou essa perspectiva. Não há como negar a importância de algum conhecimento pelo Estado de nossos dados pessoais. É indispensável o recolhimento de dados da sua população para a reorganização e melhora da Administração Pública, em franca crise financeira e tendo que escolher agora os beneficiários da benesses do Estado Social[20], pelas demandas gerais de atuação protetiva, como na segurança pública ou na vigilância sanitária, bem como para exercer de forma adequada a sua política fiscal, estabelecendo eficazmente sua previsão de receitas. A necessidade da realização dessa programação dos entes públicos como meio de redução de injustiças e desigualdades explica a impossibilidade de se negar a existência também de um interesse público na intervenção estatal[21].

Para a Administração Pública, a posse de informações sobre os seus administrados lhe dá a condição de fazer suas funções de modo mais bem-sucedido, tomando as melhores[22] decisões sobre as situações que lhe são apresentadas. Sobre esse aspecto, podemos dizer que a exigência de fornecimento de informações funciona como mais um tributo público[23].

Em verdade, a combinação do estágio atual das tecnologias de armazenamento de informação e comunicação aumentou de forma mais acentuada o poder de controle descentralizado de cidadãos sobre outros do que incrementou as capacidades da vigilância vertical da burocracia. Ou seja, o Estado sozinho pode controlar melhor seus cidadãos com as novas tecnologias, mas aqueles também podem com es-

19 PÉREZ LUÑO, Antonio E. Informática y libertad. Comentario al artículo 18.4 de la Constitución. **Revista de Estudios Políticos**, n. 24, p. 38, nov. 1981.

20 RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**. Rio de Janeiro: Editora Renovar, 2008, p. 57.

21 BENDA, Ernst. Dignidad Humana y Derechos de la Personalidad. *In*: BENDA, E. **Manual de derecho constitucional**. Madrid: Marcial Pons, 2001, p. 131.

22 O que não equivale a aceitar o mito da perfectibilidade das decisões computadorizadas, que assim não seriam sujeitas à discussão ou resistência (BENDA, Ernst. Dignidad Humana y Derechos de la Personalidad. *In*: BENDA, E. **Manual de derecho constitucional**. Madrid : Marcial Pons, 2001, p. 141).

23 HOFFMANN-RIEM, Wolfgang (Hrsg.). **Verwaltungsrecht in der Informationsgesellschaft**. Baden-Baden: Nomos--Verl.-Ges., 2000, p. 13.

tas produzir mais danos à onipotência do aparato de vigilância. O direito à proteção de dados é, assim, um condicionamento do direito de informação do cidadão, mas também este complementa aquele. Há um evidente peso em sociedades democráticas em que a decisão popular tenha o maior número de subsídios fáticos possíveis e que se disponha de uma Administração Pública com transparência e, por consequência, mais próxima da população[24].

A existência de uma regulação que organiza o funcionamento de bancos de dados pessoais se conduz, portanto, num caminho de aceitação sem o endeusamento de seus potenciais nem o menosprezo da sua afetação à dignidade humana. Como garantir a segurança social sem perder de vista como a falta de controle de dados pessoais afeta a comunicação e participação humanas. Esse é o entorno de opções que permeará as soluções legislativas tratadas nos capítulos que se seguem, por meio de artigos escritos por procuradores da República integrantes do GTTIC da 3a CCR, que têm por foco a atuação do membro do Ministério Público Federal. Assim, a análise será realizada, em ordem cronológica, a partir de quatro das principais leis que compõem o subsistema de proteção de dados brasileiro, quais sejam: a Lei nº 12.527/2011 (Lei de Acesso à Informação), a Lei nº 13.444/2017 (Lei de Identificação Civil) e as Leis nº 12.965/2014 (Marco Civil da Internet) e nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

24 15. PETERSEN, Stefanie. **Grenzen des Verrechtlichungsgebotes im Datenschutz**. Münster; Hamburg: Lit, 2000, p. 194-195 e PÉREZ LUÑO, Antonio Enrique. **Derechos humanos, estado de derecho y constitución**. Madrid: Tecnos, 2005, p. 347.

2 DADOS ABERTOS GOVERNAMENTAIS E A PROTEÇÃO DE DADOS PESSOAIS

Lúcio Mauro Carloni Fleury Curado

2.1 A política de dados abertos governamentais

A chamada política de dados abertos governamentais (*"open data"*) é um movimento de abrangência mundial que preconiza, sobretudo em matéria governamental, a abertura na maior medida possível dos dados que interessam à sociedade, de maneira apta a viabilizar sua adequada análise por quaisquer interessados.

Consta do sítio eletrônico http://dados.gov.br/pagina/dados-abertos referência a três "leis" e oito princípios regentes dos dados abertos, segundo a formulação de um dos estudiosos do tema, David Eaves.[25]

As "leis" em questão são as seguintes:

1. Se o dado não pode ser encontrado e indexado na Web, ele não existe;
2. Se não estiver aberto e disponível em formato compreensível por máquina, ele não pode ser reaproveitado; e
3. Se algum dispositivo legal não permitir sua replicação, ele não é útil.

Por sua vez, os princípios que estabelecem a conformação ideal dos dados a serem disponibilizados são os que seguem:

I) completos: todos os dados públicos são disponibilizados. Dados são informações eletronicamente gravadas, incluindo, mas não se limitando a, documentos, bancos de dados, transcrições e gravações audiovisuais. Dados públicos são dados que não estão sujeitos a limitações válidas de privacidade, segurança ou controle de acesso, reguladas por estatutos;

II) primários: os dados são publicados na forma coletada na fonte, com a mais fina granularidade possível, e não de forma agregada ou transformada;

25 Maiores informações em: https://eaves.ca/2009/09/30/three-law-of-open-government-data/.

III) atuais: os dados são disponibilizados o quão rapidamente seja necessário para preservar o seu valor;

IV) acessíveis: os dados são disponibilizados para o público mais amplo possível e para os propósitos mais variados possíveis;

V) processáveis por máquina: os dados são razoavelmente estruturados para possibilitar o seu processamento automatizado;

VI) com acesso não discriminatório: os dados estão disponíveis a todos, sem que seja necessária identificação ou registro;

VII) em formatos não proprietários: os dados estão disponíveis em um formato sobre o qual nenhum ente tenha controle exclusivo;

VIII) livres de licenças: os dados não estão sujeitos a regulações de direitos autorais, marcas, patentes ou segredo industrial. Restrições razoáveis de privacidade, segurança e controle de acesso podem ser permitidas na forma regulada por estatutos.

No âmbito dos países do G8 foram aprovados em junho de 2013, relativamente ao tema, cinco princípios que dispõem no mesmo sentido, conforme se nota:[26]

1. Dados Abertos por *Default*: expectativa de que todos os dados governamentais sejam publicados de forma aberta como padrão, ainda que se reconheça que existem razões legítimas para que alguns dados não possam ser liberados;
2. Qualidade e Quantidade: dados abertos de alta qualidade, que sejam liberados de forma tempestiva, abrangente e precisa. Sempre que possível, dados em sua forma original e na menor granularidade disponível. Informações descritas em linguagem clara, inteligível por todos, e dados descritos de forma que seus usuários tenham informações suficientes para entender limitações analíticas e requisitos de segurança para processar os dados;
3. Utilizável por todos: liberação do máximo de dados de forma gratuita e em formatos abertos, sempre que possível, garantindo que estejam disponíveis para a mais ampla gama de usuários e para a maior variedade de propósitos;
4. Liberação de dados para melhoria da governança: compartilhamento de conhecimentos técnicos e experiências entre países, para que todos possam se beneficiar dos dados abertos, com transparência e documentação on-line sobre coleções de dados, padrões e processos de publicação;
5. Liberação de dados para inovação: incentivo às pessoas, como desenvolve-

26 Disponível em: http://www.brasildigital.gov.br/dados-abertos-e-controle-social.htm.

> dores de aplicativos e organizações da sociedade civil, para extrair valor de dados abertos e promover a formação de uma futura geração de *"Data Innovators"* a partir da liberação de dados em formatos legíveis por máquinas.

Os países que integram a parceria mundial em matéria de dados abertos governamentais podem ser vistos no link https://www.opengovpartnership.org/participants, em que se nota que o Brasil, membro desde 2011, é listado como país com plano de ação em desenvolvimento, contando com 98 compromissos (82 concluídos e 16 em andamento) e cobrindo 15 temas.

Como se verá, a lógica por trás das diretrizes desse movimento terminou por ser em grande medida incorporada na Lei nº 12.527/2011 e em diversos atos normativos federais.

2.2 A incorporação pelo ordenamento jurídico brasileiro

Para além da exigência constitucional de publicidade nos atos da Administração, o ordenamento brasileiro já trazia imposição de transparência, por exemplo, na gestão fiscal (arts. 48, 48-A e 49 da Lei Complementar nº 101/2000).

Com a edição da Lei nº 12.527/2011, porém, foi efetivamente incorporado ao ordenamento brasileiro o tema da política de dados abertos governamentais, como reflexo inclusive dos compromissos assumidos externamente pelo Brasil com outros sete países (África do Sul, Estados Unidos, Filipinas, Indonésia, México, Noruega e Reino Unido) que participaram da formação da Parceria para Governo Aberto (*Open Government Partnership*), parceria esta que hoje congloba quase 80 países.

O histórico desse processo, bem como as perspectivas de desenvolvimento futuro do tema no âmbito da Administração Pública Federal podem ser conferidos no plano de ação nacional para Governo Aberto, que está em sua 3ª edição, editada para o período entre 2016 e 2018, conforme arquivo disponível no link: https://www.opengovpartnership.org/sites/default/files/Brazil_Plano-de-Acao-3_2016-2018.pdf.

Na esteira das diretrizes trazidas pela Lei de Acesso à Informação, foram editados atos normativos infralegais tratando do tema, valendo mencionar, na esfera federal, o Decreto nº 7.724/2012, que regulamenta referido diploma legal, o Decreto nº 8.777/2016, que institui a Política de Dados Abertos do Poder Executivo Federal, e a Instrução Normativa nº 4/2012, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, que institui a

Infraestrutura Nacional de Dados Abertos.[27] Além disso, há atos normativos que, no contexto da regulamentação do controle social de políticas públicas, indiretamente abordam a questão da transparência governamental, a exemplo do Decreto nº 8.243/2014, que institui a Política Nacional de Participação Social e o Sistema Nacional de Participação Social.

Foram criadas iniciativas pontuais relativamente ao tema, notadamente no âmbito da Administração Direta Federal, como a escala Brasil transparente, que traz *ranking* de cumprimento de diversos entes públicos no que toca ao cumprimento da Lei de Acesso à Informação, como se pode ver no link http://www.cgu.gov.br/assuntos/transparencia-publica/escala-brasil-transparente/escala-brasil-transparente.

Além disso, diversos portais oficiais foram criados na esfera federal, a exemplo dos sites http://dados.gov.br/, https://www.governoeletronico.gov.br/ e http://www.governoaberto.cgu.gov.br/, que pretendem dar concreção ao substrato normativo nacional acerca do tema.[28]

Não obstante grande parte desse substrato normativo seja aplicável a toda a Administração Pública (vide art. 1º, parágrafo único, da Lei nº 12.527/2011), o fato é que ainda é deficiente, na prática, sua efetivação nos mais variados órgãos da Administração, notadamente nas esferas alheias à Administração Direta Federal.

2.3 Avanços necessários

A despeito da progressiva absorção das diretrizes de *open data* pelo ordenamento jurídico brasileiro, o fato é que o cenário de abertura de dados ainda é nitidamente insuficiente à luz do que dispõe a Lei de Acesso à Informação.

Nem mesmo no âmbito federal, a despeito da existência de decretos regulamentadores do tema e de sítios oficiais voltados à concretização da proposta, há dados disponibilizados com a abrangência esperada ou na forma adequada, notadamente ao se ter em conta as informações relativas à Administração Indireta.

O fato é que ainda há muito por avançar, nos diversos entes da Administração Indireta e mesmo em órgãos da Administração Direta, com vista a um controle in-

27 Disponível em: https://www.governoeletronico.gov.br/documentos-e-arquivos/3%20-%20IN%2004%2013-04-12.pdf.

28 Foi editada no âmbito da Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão a Resolução nº 2, de 24 de março de 2017, tendo por objeto a regulamentação dos termos de uso do portal brasileiro de dados abertos. Disponível em: http://dados.gov.br/pagina/instrucao-normativa-da-inda.

clusive qualitativo das informações divulgadas abertamente.

O Ministério Público Federal possui papel de destaque nesse cenário, tendo já empreendido esforços exitosos que reforçam a pertinência de alargamento de sua atuação no controle da transparência governamental.

2.4 Atuações do Ministério Público Federal na matéria

Cabe citar alguns exemplos de atuações frutíferas do Ministério Público Federal em matéria de dados abertos governamentais.

Uma atuação amplamente disseminada no território nacional decorreu de iniciativa da 5ª Câmara de Coordenação e Revisão e traduziu-se na busca, em municípios brasileiros, da efetiva disponibilização e alimentação de seus portais de transparência, com esteio sobretudo no regramento dado à matéria pela Lei de Responsabilidade Fiscal, que prevê a possibilidade de suspensão de transferências voluntárias da União em caso de não atendimento à transparência da gestão fiscal. Conforme pode ser visto no portal http://combateacorrupcao.mpf.mp.br/ranking, o projeto tem resultado em notáveis avanços em matéria de transparência de dados municipais.

Outro exemplo que merece ser lembrado é o Termo de Cooperação Técnica assinado entre a Procuradoria Federal dos Direitos do Cidadão (PFDC) e o Fundo Nacional de Desenvolvimento da Educação (FNDE), com vista a garantir mais transparência ao financiamento das políticas públicas de educação.[29] Houve também atuação no FNDE por meio de procedimento administrativo[30] ligado à atuação do Grupo de Trabalho Tecnologia da Informação e Comunicação (GT-TIC), da 3ª CCR. Ambas as atuações resultaram na abertura do acesso a sistemas de informação do FNDE que antes eram de acesso restrito.

No âmbito do GT-TIC da 3ª CCR também tem havido enfrentamento do tema da transparência pública no que toca aos dados pertinentes à atuação do Incra, autarquia responsável por diversas políticas sociais cujos dados não vinham sendo disponibilizados abertamente à consulta pública. Em razão dessa atuação, houve notáveis avanços em matéria de transparência no que toca às políticas públicas sob responsabilidade da autarquia.

29 Informações disponíveis em: http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2015/dezembro/mpf-assina-termo-de-cooperacao-tecnica-para-dar-mais-transparencia-a-dados-da-educacao/ e http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2017/maio/050517-2/.

30 PA nº 1.00.000.002519/2015-61.

Assim, a partir da interlocução de referido grupo de trabalho com o Incra,[31] houve, entre outras melhorias, a implantação, no sítio eletrônico da Instituição, de ferramenta de pesquisa de beneficiários do Programa Nacional de Reforma Agrária, aberta ao acesso de qualquer usuário (http://saladacidadania.incra.gov.br/Beneficiario/ConsultaPublica), permitindo variados critérios de pesquisa, o que enseja um mais adequado controle da política pública.

Por fim, existem ainda diversas atuações oriundas de iniciativas individuais de membros do MPF.

O que se nota, a partir da pluralidade de enfrentamentos sobre o tema, é que a atuação ministerial na temática de dados abertos governamentais tem reflexo no espectro de atribuições de mais de uma Câmara de Coordenação e Revisão (CCR) do Ministério Público Federal.

Por certo, se o foco for o exercício da cidadania e do direito social ao acesso à informação, a temática pode ser afeta à atuação da Procuradoria Federal dos Direitos do Cidadão.

Tomando por escopo, diferentemente, a fiscalização da regularidade do ato administrativo, aí incluso o dever de publicidade, trata-se de questão passível de enfrentamento no âmbito da 1ª CCR.

De outra via, ao se levar em conta o efeito preventivo de atos ilícitos da Administração, sobretudo de corrupção – já que a publicização dos dados facilita o controle de sua regularidade –, trata-se de temática albergada na esfera de atribuições da 5ª CCR.

Por fim, ao tomar como foco o impacto que o acesso a dados (*big data*) pode ter na ordem econômica como um todo, bem como os reflexos possíveis da questão em matéria de proteção de dados pessoais (não passíveis de divulgação), tem-se que a questão pode ser inserida na seara de atuação da 3ª CCR.

Com efeito, a proposta dos dados abertos tem nítidos reflexos não apenas no exercício da cidadania ou na facilitação do controle da Administração, mas também na preservação da própria ordem econômica, na medida em que impede a obtenção privilegiada de informações que podem ter impacto em setores variados da economia, resguardando, a partir do acesso isonômico, a livre concorrência entre os sujeitos do mercado, notadamente daqueles cujas atividades são afetadas em maior ou menor grau pela atuação estatal na economia, seja por meio de serviços públicos, seja por meio de atividades econômicas nas hipóteses em que admitidas (art. 173 do texto constitucional).

31 PA nº 1.00.000.008313/2015-45.

Reforça-se a pertinência do tema com o espectro de atribuições da 3ª CCR quando seu enfrentamento se dá de maneira conjugada com o tema da proteção de dados pessoais.

O fato é que, a despeito das atuações já existentes, ainda há espaço para muitas medidas nesse campo.

2.5 A concretização do dever de transparência

A análise acerca do grau de atendimento às exigências normativas em matéria de transparência de dados governamentais deve ser feita à luz dos critérios já trazidos na legislação, mas sem descurar de particularidades casuísticas inerentes à natureza da atividade desenvolvida pelo órgão público, ou à natureza da informação a ser disponibilizada.

No que toca aos critérios normativos gerais, merece destaque o disposto no art. 8º da Lei de Acesso à Informação, que estipula como dever dos órgãos e entidades públicos a promoção, independentemente de requerimentos, da divulgação de informações de interesse coletivo ou geral pertinentes à respectiva esfera de atribuições, inclusive, de maneira obrigatória (vide § 2º do citado artigo), por meio do sítio oficial na internet, que deverá atender aos seguintes requisitos (conforme § 3º do referido art. 8º):

I. conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
II. possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
III. possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;
IV. divulgar em detalhes os formatos utilizados para estruturação da informação;
V. garantir a autenticidade e a integridade das informações disponíveis para acesso;
VI. manter atualizadas as informações disponíveis para acesso;
VII. indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e

VIII. adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei nº 10.098, de 19 de dezembro de 2000, e do art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008.

Como se nota, mais do que o dever de fornecimento de informações públicas solicitadas, impõe-se ao Poder Público o dever de transparência ativa, traduzido na necessidade de disponibilizar, de maneira aberta e antecipada, o livre acesso, inclusive e especialmente pela internet, de dados pertinentes às atividades da Administração, dever este que resta aclarado pelo rol de direitos estampado no art. 7º do mesmo diploma legal.

No processo de análise das medidas passíveis de serem implementadas pelo órgão público fiscalizado, impõe-se ainda observar a peculiar natureza da atividade desenvolvida – seja com vista à busca da implementação de soluções que permitam maior acesso qualitativo a informações úteis ao cidadão ou mesmo úteis à melhoria do serviço público prestado, seja com vista à avaliação de possíveis limites quanto aos dados passíveis de serem divulgados.

Assim, a própria lei ressalva hipóteses de informações sigilosas, segredo de justiça, segredo industrial, ou mesmo dados pertinentes à vida privada das pessoas.

A atuação ministerial, nesse contexto, deve ser pautada por diagnóstico inicial que leve em conta todos esses aspectos.

O processo de aferição dos contornos dos dados disponibilizados por determinado órgão público pode ser iniciado a partir da simples consulta ao sítio eletrônico do órgão em questão, sendo que o acompanhamento subsequente do tema passa pela realização de diligências comuns à generalidade dos procedimentos de tutela coletiva, notadamente requisições e reuniões, podendo resultar em recomendações, compromissos de ajustamento de conduta ou mesmo na judicialização da questão.

O fato é que o ordenamento jurídico brasileiro atual fornece elementos que dão peso e exigibilidade à atuação ministerial em face da Administração em matéria de transparência de dados.

2.6 Resultados esperados

A adequada observância dos deveres de transparência pública tem o condão não apenas de viabilizar o desejável controle social da coisa pública, mas também de facilitar o trabalho exercido pelo próprio Ministério Público e por outros órgãos com atuação institucional no controle da Administração – prevenindo atos de corrupção e ilícitos administrativos –, além de representar mecanismo de potencialização da participação democrática da população na condução de medidas governamentais de interesse geral da sociedade.

A ampla divulgação de matérias afetas a políticas públicas permite ainda maior previsibilidade e isonomia quanto à repercussão de atos administrativos na ordem econômica, evitando uso de informações privilegiadas em detrimento da livre concorrência, por exemplo.

Os resultados possíveis de uma adequada observância dos deveres de transparência pública são, pois, plúrimos.

E, desde que haja suficiente atenção à necessidade de resguardo de certas situações não passíveis de ampla divulgação, esses resultados são eminentemente positivos à sociedade.

No que toca ao espectro de situações não passíveis de ampla divulgação, demanda maior cuidado a necessidade de adequada proteção de dados de caráter pessoal.

2.7 A compatibilização do dever de transparência com a proteção de dados pessoais

A imposição, ao Poder Público, da ampla divulgação de informações afetas a suas atividades traz como contrapartida a questão atinente aos limites do que pode ser divulgado em matéria de dados pessoais deste ou daquele cidadão.

Ao mesmo tempo que o texto constitucional traz o princípio da publicidade dos atos da Administração (art. 37, *caput*) e o direito fundamental de acesso à informação (inciso XXXIII do art. 5º; inciso II do § 3º do art. 37; e § 2º do art. 216), resguarda também os direitos à intimidade e à privacidade (art. 5º, X e LX; e art. 93, IX, segunda parte) – do que deflui a necessidade de compatibilização desses valores.

Exatamente por esse motivo, a Lei de Acesso à Informação (Lei nº 12.527/2011) traz (art. 6º) a um só tempo a necessidade de assegurar a gestão transparente da informação – propiciando amplo acesso a ela e sua divulgação – e a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, au-

tenticidade, integridade e eventual restrição de acesso.

Mais recentemente, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018, com entrada em vigor prevista para fevereiro de 2020) veio trazer regramento mais detalhado acerca do tema, notadamente quanto ao tratamento de dados pessoais pelo Poder Público.

O tratamento de dados pessoais pelo Poder Público independe do consentimento do titular quando for indispensável para o cumprimento de obrigação legal ou para a execução de políticas públicas legalmente previstas (art. 11, II, LGPD). Isso não se aplica a empresas públicas e sociedades de economia mista que atuem em regime de concorrência – visto que nesse caso têm o mesmo tratamento dispensado às pessoas jurídicas de direito privado.

De outro lado, o tratamento de dados pessoais por entes públicos deve ser sempre atrelado ao atendimento de sua finalidade pública e à persecução do interesse público, devendo haver ainda explicitação das hipóteses em que realizam referido tratamento – com especificação dos procedimentos e práticas usados.

Além disso, o uso compartilhado de dados pessoais pelo Poder Público deve sempre respeitar os princípios de proteção de dados pessoais, especificados no art. 6º da LGPD.

A atuação do Ministério Público Federal na temática do acesso público a dados governamentais deve levar em conta essa necessidade de compatibilização do dever de transparência com o dever de proteção a dados pessoais – zelando pelo cumprimento do dever de publicidade sempre que a questão analisada indicar a preponderância do interesse público no acesso à informação, sem deixar de observar, tanto quanto possível e recomendável à luz dos contornos do caso concreto, o cuidado de resguardar informações pessoais que não interessem à sociedade, mas digam preponderantemente respeito à intimidade e à privacidade das pessoas envolvidas.

Não se ignora que, em matéria de atos da Administração Pública, ganha maior peso o dever de transparência, até porque nessa seara não costuma haver, em regra, situações de afetação à intimidade e à privacidade.

Assim, a Lei de Acesso à Informação preconiza como diretriz norteadora dos atos administrativos a observância da publicidade como preceito geral e do sigilo como exceção (art. 3º, I), deixando clara a opção pelo fomento ao desenvolvimento da cultura de transparência na Administração Pública (inciso IV do citado art. 3º) e pelo desenvolvimento do controle social da Administração Pública (inciso V do mesmo artigo).

Isso não significa, claro, que não haja preocupação quanto à proteção dos dados pessoais, até porque, a depender de sua natureza, sua divulgação pode representar

afetação não apenas à vida privada, mas também trazer vulnerabilidade à própria segurança das pessoas atingidas.

Exatamente por isso, a Lei de Acesso à Informação regulamenta em seu artigo 31 o tratamento das informações pessoais nos seguintes termos:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
> I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
> II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.
> § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.
> § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:
> I – à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
> II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
> III – ao cumprimento de ordem judicial;
> IV – à defesa de direitos humanos; ou
> V – à proteção do interesse público e geral preponderante.
> § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.
> § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

O Decreto nº 7.724/2012 regulamenta mais detalhadamente o tema em seus arts. 55 a 62.

Falaremos em sequência de uma situação concreta em que se faz presente a problemática do cotejo entre acesso a informações de interesse público e proteção de dados pessoais.

2.7.1 Cadastros negativos e a proteção de dados pessoais

Tema delicado relativo ao cotejo entre dados pessoais e transparência pública diz respeito à publicização de listagem de pessoas com responsabilização reconhecida por determinados atos ilícitos, ou mesmo de pessoas impedidas do acesso a determinados direitos ou políticas públicas.

Um primeiro exemplo a ser mencionado é o da lista de empregadores que submeteram trabalhadores à condição análoga à de escravo,[32] tema objeto de regulamentação pela Portaria Interministerial MTPS/MMIRDH nº 4, de 11/5/2016.

Conforme se depreende da leitura do ato normativo em questão, há divulgação pública da listagem de pessoas físicas ou jurídicas autuadas em ação fiscal que tenha identificado trabalhadores submetidos a condições análogas à de escravo. A inclusão em referida lista somente ocorre após o trânsito em julgado da apuração na esfera administrativa, sendo que os nomes permanecem na lista pelo período de dois anos, durante o qual há monitoramento. Em caso de assinatura de termo de ajustamento de conduta – que conta com a participação do Ministério Público do Trabalho –, o nome do compromissário é colocado em lista diversa, sendo que há cláusulas mínimas a constarem em eventual TAC, incluindo medidas preventivas e reparadoras de natureza variada.

Nota-se que a divulgação dos dados pessoais numa tal situação é justificada pela natureza da informação – tratando-se de ilícitos de ocorrência reconhecida em regular processo administrativo, com contraditório e ampla defesa –, não se tratando, pois, de informação relativa à vida privada das pessoas envolvidas, já que são públicos os processos em que apurada sua responsabilidade.

O § 4º do art. 31 da Lei de Acesso à Informação dá margem à existência de um tal cadastro "negativo", ao dispor que não é possível a invocação da restrição de acesso a informações atinentes à vida privada, honra e imagem de pessoas com o

32 O cadastro em questão é divulgado no link: http://trabalho.gov.br/component/content/article?id=4428.

intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido.

No caso, a publicização do cadastro de empregadores autuados é ínsita ao processo de enfrentamento jurídico do problema da exploração de trabalhadores, notadamente em razão do efeito preventivo que a publicidade traz, evitando novos ilícitos – de maneira, pois, consentânea com o interesse público subjacente ao tema.

Outra situação de cadastro negativo que merece ser mencionada e que também se afiguraria legítima e admissível é ligada ao disposto no art. 2º, § 7º, da Lei nº 8.629/1993, que prevê a exclusão, do Programa de Reforma Agrária do Governo Federal, dos beneficiários ou pretendentes que participarem de invasões ou esbulhos de imóveis rurais em fase de vistoria ou avaliação para fins de reforma agrária, ou que esteja sendo objeto de desapropriação, excluindo ainda do Programa participantes de invasão de prédios públicos ou de atos de violência real.

O Ministério Público Federal em Pernambuco ajuizou ação civil pública relativa ao tema (autos nº 0804835-55.2017.4.05.8300), buscando a implantação, pelo Incra, de banco de dados de pessoas inseridas na situação de impedimento indicada.

Embora na ação em referência não haja pedido de divulgação dos integrantes de referido banco de dados, não se vê óbice a que haja publicização da listagem, desde que somente daqueles com participação já apurada após regular contraditório e observância do devido processo legal – ainda que a apuração em questão tenha se dado apenas na esfera administrativa.

A abertura do acesso a referido cadastro permitiria amplo controle, por exemplo, quanto a possíveis beneficiários cujo ingresso no Programa de Reforma Agrária foi indevido.

Os exemplos indicados demonstram como, a depender dos contornos do caso concreto e do interesse público subjacente à informação a ser divulgada, justifica-se a abertura mesmo de dados pessoais por parte da Administração, ainda que representem, do ponto de vista do titular desses dados, situação negativa (por exemplo, situação que possa lhes afetar a imagem pessoal).

Não se deve perder de vista, porém, que mesmo quando justificada a abertura de informações pessoais, essa divulgação deve ser limitada ao que for essencial ao resguardo do interesse público envolvido – por exemplo, divulgar apenas dados suficientes a evitar homonímias.[33] Com isso se evitaria o risco, que não pode

33 Esse o padrão adotado, por exemplo, pelo Incra na divulgação dos assentados no Programa Nacional de Reforma Agrária, nos resultados da ferramenta de pesquisa nominal, disponibilizada no sítio eletrônico da instituição. Além do nome completo, os resultados apontam apenas os três primeiros dígitos do CPF, o que se afigura suficiente para permitir o controle da política pública sem expor desnecessariamente dados pessoais dos beneficiários.

ser desprezado, de uso criminoso das informações pessoais por parte de terceiros mal-intencionados.

2.8 Conclusões

O tema dos dados abertos governamentais, notadamente quando conjugado à necessidade de proteção de dados pessoais, adquire significativo relevo diante do quadro de transformação das comunicações sociais, intensificado pelo avanço das tecnologias digitais.

A perspectiva de progressiva disseminação do uso do ambiente virtual como espaço de interlocuções sociais múltiplas e variadas, inclusive perante a Administração, reforça a necessidade de detido acompanhamento do tema por parte do Ministério Público Federal, não apenas quanto ao cumprimento, pelo Poder Público, do dever de transparência em sua atuação, mas também quanto ao resguardo de medidas adequadas de proteção de dados pessoais dos envolvidos.

3 A IDENTIFICAÇÃO CIVIL NACIONAL E A PROTEÇÃO DE DADOS PESSOAIS

Manoel Antonio Gonçalves da Silva

3.1 Introdução

A Lei nº 13.444, de 11 de maio de 2017, dispõe sobre a Identificação Civil Nacional e o respectivo Documento Nacional de Identificação (DNI), tendo como escopo, consoante seu art. 1º, identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.

É certo que a Lei nº 7.116/1983 já regulava a expedição de carteiras de identidade pelos estados, assegurando a validade nacional de tais documentos, todavia os problemas do modelo de identificação civil até então adotado se mostraram numerosos, tornando inadiável a implementação de um registro civil moderno e unificado.

Há no Brasil uma histórica ineficiência do Poder Público em registrar, manter e acessar informações que identifiquem os indivíduos de maneira desburocratizada, confiável e de fácil interoperabilidade entre os diversos órgãos governamentais. Essa ineficiência, ao cabo, traduz-se em dispêndio de recursos e transtornos de diversas ordens tanto para a Administração Pública quanto para o cidadão.

A título de exemplo, destaquem-se os inúmeros documentos de que deve dispor o cidadão para se identificar (CPF, RG, CNH, Carteira Profissional, Título de Eleitor, passaporte etc.), a falta de confiabilidade de tais documentos – frequentemente objeto de falsificação – e a rotineira e injustificável exigência de certidões para comprovação de dados pessoais perante órgãos públicos, pois muito embora o Poder Público já disponha das informações, objeto da certidão, as tem de maneira desorganizada e inacessível a seus diversos órgãos.

As inconsistências no sistema de identificação também são responsáveis por viabilizar a prática de fraudes, cuja prevenção e repressão são difíceis tarefas para os órgãos incumbidos deste mister. Não raro, um mesmo indivíduo dispõe de mais

de uma identificação civil[34], utilizando-se das falhas do sistema de identificação para se furtar às suas responsabilidades civis e criminais. Nesse ambiente favorável à criminalidade, multiplicam-se também as vítimas do uso indevido de dados pessoais[35].

Após a adoção de diversas nomenclaturas e de duas décadas de tentativas de implementação da identificação civil unificada, a Lei nº 13.444/2017 surgiu com o desafio de pavimentar a via da modernização do sistema nacional de identificação. Porém, na aplicação da nova legislação, não deve o operador do Direito atentar exclusivamente para o escopo legal de viabilizar a absorção dos avanços tecnológicos relacionados à identificação civil, deve também atentar para a preservação de direitos fundamentais historicamente conquistados e para os contornos assumidos por esses direitos face aos avanços da modernidade.

É fato que para a criação de um sistema de identificação civil de dimensão nacional e atual do ponto de vista tecnológico, a Lei nº 13.444/2017, como era de se esperar, instituiu as bases legais para a formação de uma vultosa base de dados pessoais, a Base de Dados da Identificação Civil Nacional (BDICN), a demandar a proteção da lei, dos órgãos e agentes da Administração Pública responsáveis pelo tratamento[36] desses dados, do Ministério Público Federal e dos demais órgãos e entidades responsáveis pela defesa de direitos e garantias fundamentais.

Para compreender a dimensão e a relevância da BDICN, cabe transcrever parte do art. 2º da Lei nº 13.444/2017:

> Art. 2º A ICN utilizará:
> I – a base de dados biométricos da Justiça Eleitoral;
> II – a base de dados do Sistema Nacional de Informações de Registro Civil (Sirc), criado pelo Poder Executivo federal, e da Central Nacional de Informações do Registro Civil (CRC Nacional), instituída pelo Conselho Nacional de Justiça, em cumprimento ao disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009;

34 TUROLLO JR., Reynaldo. Repórter tira carteira de identidade em 9 estados. **Folha de São Paulo**, 13 out. 2013. Disponível em: https://www1.folha.uol.com.br/cotidiano/2013/10/1355762-reporter-tira-carteira-de-identidade-em-9-estados.shtml. Acesso em: 22 jul. 2019.

35 HOMEM é preso por engano no DF por crime que irmão cometeu. **G1**, 5 dez. 2017. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/homem-e-preso-por-engano-no-df-por-crime-que-irmao-cometeu.ghtml. Acesso em: 22 jul. 2019.

36 Conforme esclarece Laura Schertel Mendes (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor** – Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.), "utiliza-se a expressão 'tratamento de dados pessoais' para designar as operações técnicas que podem ser efetuadas sobre os dados pessoais, de modo informatizado ou não, com a finalidade de se refinar a informação, tonando-a mais valiosa ou útil".

> III – outras informações, não disponíveis no Sirc, contidas em bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou disponibilizadas por outros órgãos, conforme definido pelo Comitê Gestor da ICN.

Os dois primeiros incisos do citado artigo já abrangem um volume considerável de dados (registro de nascimento, registro de casamento, impressões digitais, dados relativos ao eleitor, número do CPF, padrões biométricos da face etc.), mas o inciso III vai além, trazendo cláusula aberta, que possibilita ao Comitê Gestor da ICN definir a inclusão de inúmeros outros dados na BDICN. Sendo assim, apenas para citar os dados mais alinhados com o escopo de unificação da base de dados de identificação dos cidadãos, é possível antever a inclusão na BDICN do Número de Identificação Social (NIS), do número de Programa de Integração Social (PIS), do número de Programa de Formação do Patrimônio do Servidor Público (Pasep), do número do Cartão Nacional de Saúde (CNS), do número do Título de Eleitor, do número do documento de identidade profissional expedido por órgão ou entidade legalmente autorizado, do número da Carteira de Trabalho e Previdência Social (CTPS), do número da Carteira Nacional de Habilitação (CNH), do número do Certificado Militar, entre outros[37].

Como é possível perceber, a BDICN tem o potencial de se tornar uma das maiores bases de dados que o Poder Público manterá a respeito dos cidadãos brasileiros, cuja importância se revela não apenas no volume de dados pessoais que agregará, mas também na sensibilidade de uma parte considerável desses dados.

É cediço que o tema da proteção de dados pessoais, embora não seja algo novo, vem progressivamente ocupando a pauta dos noticiários, do mercado, da Academia e dos Poderes Públicos.

As possibilidades incontáveis de utilização de dados pessoais há muito foram percebidas pelo mercado, a ponto de tais dados representarem o principal ativo de algumas das maiores empresas do Vale do Silício[38]. Escândalos envolvendo vaza-

37 Já há previsão da possibilidade de inclusão destes números na carteira de identidade expedida pelos estados, conforme Decreto nº 9.278/2018. Dessa forma, a simples inclusão da base de dados dos institutos de identificação dos estados e do Distrito Federal, prevista no inciso III da Lei nº 13.444/2017, determinaria a automática inclusão de todos estes dados na BDICN, acaso já constantes das bases de dados estaduais.

38 Laura Schertel Mendes (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor** – Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.) ressalta: "Diante da importância que o conhecimento sobre os consumidores adquiriu na economia atual, os dados pessoais tornaram-se capital essencial para o sucesso de inúmeros negócios. Assim, no contexto da economia de produção flexível, emerge uma verdadeira 'indústria de bancos de dados', nos termos de Daniel Solove [SOLOVE, Daniel. The digital person, 2004, p. 19], cuja finalidade principal é a de propiciar aos

mentos e o mau uso desses dados se tornaram rotineiros[39], tendo o recente caso envolvendo o Facebook e a Cambridge Analytica demonstrado que a manipulação de dados pessoais tem potencial de causar danos de dimensões antes inimagináveis, indo além da esfera jurídica dos titulares dos dados[40].

A crescente preocupação com a questão determinou recente reforma nas regras de proteção de dados da União Europeia[41], obrigando empresas do mundo inteiro a se adequarem para continuar fazendo negócios dentro do bloco sem sofrerem pesadas multas. Na esteira da *General Data Protection Regulation* (GDPR), ampliou-se no Brasil a discussão sobre o tema e acelerou-se a aprovação da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados)[42], que trouxe avanços na matéria de proteção de dados pessoais e com isso também tornou o Estado brasileiro mais apto ao intercâmbio de dados no plano internacional[43].

É certo que no Brasil diversas leis já tratavam do tema, abordando questões específicas, sem maior sistematização da matéria. Além disso, o direito à proteção de dados pessoais, também conhecida como autodeterminação informativa[44], deve ser observado como uma especificação de direitos fundamentais já consolidados e que encontram tutela constitucional na proteção da dignidade da pessoa humana, dos direitos à liberdade, à privacidade, à intimidade, à honra e à imagem[45].

---

setores interessados os dados pessoais de categorias de consumidores, por meio da comercialização ou cessão. O resultado é a ampla circulação das informações pessoais na sociedade, gerando benefícios aos setores envolvidos, mas também grandes riscos aos consumidores, cujos dados são coletados, processado e transferidos"

39 Sobre o famoso caso da NSA, surgido a partir das revelações de Edward Snowden: https://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat.

40 Na matéria publicada no jornal britânico "*The Guardian*", revelou-se que a Cambridge Analytica colaborou com a equipe que trabalhou na eleição de Donald Trump e no Brexit, analisando dados de milhões de usuários do Facebook para criar um software capaz de prever e influenciar a escolha dos eleitores (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election).

41 Disponível em: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

42 SANCIONADA com vetos lei geral de proteção de dados pessoais. **Senado notícias**, 15 ago. 2018. Disponível em: https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 22 jul. 2019.

43 A título de exemplo, confira-se: http://www.mpf.mp.br/pgr/noticias-pgr/mpf-se-aproxima-da-eurojust-em-reuniao-interinstituciona.

44 Nomenclatura utilizada na decisão de 1983 sobre a "Lei do Censo" pelo Tribunal Constitucional Alemão, é que se trata de direito que não se basta nas faculdades negativas, ou seja, impeditivas da ação de outrem, mas sim, que exige a presença de uma série de faculdades positivas, que permitam ao indivíduo exercer efetivo controle sobre o uso dos seus dados (FERREIRA DA SILVA, Carlos Bruno. **Proteção de Dados e Cooperação Transnacional**: Teoria e Prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes Editores, 2014, p. 16). O termo foi adotado na Lei Geral de Proteção de Dados (art. 2º, II, da Lei nº 13.709/2018).

45 Importante pontuar que, muito antes da existência de leis específicas para a proteção de dados pessoais no Brasil, o Supremo Tribunal Federal já relacionava o direito ao acesso às informações de caráter pessoal, registradas em órgãos do Estado, à autonomia individual e à privacidade, conforme pode ser observado no voto do ministro Celso de Melo, relator para acórdão no RHD nº 22/DF, julgado em 19/9/91, no qual destaca que "A garantia de acesso a informações de caráter pessoal, registra-

Pois bem. Feita essa breve contextualização, cabe destacar que o presente trabalho possui como escopo a análise da proteção constitucional, legal e regulamentar da BDICN, destacando-se as normas específicas, bem como outras normas que poderão oferecer subsídios para a proteção do referido banco de dados. Buscar-se-á, ademais, apontar, algumas omissões da Lei nº 13.444/2017, sem a pretensão de esgotar a matéria, eis que, por se tratar de lei recente no ordenamento, muitas outras questões hão de surgir com o decorrer do tempo. Dessa forma, a familiarização com a problemática envolvendo a proteção de dados pessoais, a partir de um enfoque mais específico, poderá auxiliar o leitor a solucionar as questões de ordem prática vindouras, sejam elas relacionadas à BDICN, sejam relacionadas aos inúmeros outros bancos de dados pessoais mantidos pelo Poder Público.

3.2 Histórico da Lei nº 13.444/2017

A tentativa de modernizar e unificar o registro civil dos brasileiros não é algo recente, dela tendo se ocupado, de longa data, autoridades públicas dos Poderes Legislativo e Executivo, no que se fizeram acompanhar, recentemente, do Poder Judiciário Eleitoral.

A novel legislação derrogou a Lei nº 9.454/1997, a qual prevê a criação do Registro de Identidade Civil-RIC e foi regulamentada treze anos após sua publicação, pelo Decreto nº 7.166/2010, sem nunca ter chegado a ser de fato implementada.

das em órgãos do Estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade". Já no STJ, no Recurso Especial 22.337/RS, o magistral voto do relator min. Rui Rosado de Aguiar (Quarta Turma, julgado em 13/2/1995) destaca: "A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce e ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, algumas providências já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível das garantias fundamentais, com o direito de autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do ombudsman, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação (HESSEMER. **Proteção de Dados**. Palestra proferida na Faculdade de Direito da UFRGS, 22 nov. 1993). No Brasil, a regra do art. 5º, inc. X, da Constituição de 1888, é um avanço significativo: 'São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação'.

Vejamos os fatos que marcaram as idas e vindas na tentativa de implementar uma identificação civil unificada[46]:

1995: Vários projetos tramitam no Congresso Nacional sobre a identificação civil com o objetivo de modernizar o padrão brasileiro.

1997: O projeto mais completo entre os que tratavam do tema é aprovado e dá origem à Lei nº 9.454/1997. O Ministério da Justiça cria então grupo de trabalho, composto por vários órgãos da Administração Pública Federal para propor a regulamentação da Lei nº 9.454/1997 e implantar o novo sistema de identificação civil no país. O trabalho chega a ser concluído, mas não é enviado à Presidência da República para as providências necessárias.

2009: A Lei nº 9.454/1997 é derrogada pela Lei nº 12.058/2009, que modificou alguns aspectos da legislação, especialmente quanto a prazos.

2010: Em 5 de maio, é publicado o Decreto nº 7.166/2010, que regulamente a Lei nº 9.454/1997. É criado o Comitê Gestor composto por representantes de vários órgãos da Administração Pública Federal com a incumbência de estudar e propor processo ideal para implantação do RIC. Em solenidade, em 30 de dezembro, o então presidente Lula faz o lançamento oficial do RIC, com a distribuição dos primeiros cartões. O de número 1 foi para o próprio presidente.

2011: Já na Gestão Dilma Rousseff, começa o projeto-piloto que visava emitir 2 milhões de RICs no Brasil. O programa não é integralmente cumprido.

2012: O Ministério da Justiça anuncia a suspensão do RIC para reavaliação de todo o projeto.

2015: A Justiça Eleitoral apresenta à presidência da República a proposta de criação do Registro Civil Nacional (RCN). A gestão do banco de dados e a emissão ficariam a cargo da Justiça Eleitoral. É então elaborado no âmbito do Poder Executivo e apresentado ao Congresso Nacional o Projeto de Lei nº 1.775/2015, propondo a criação do RCN e a revogação da Lei nº 9.454/1997.

2017: Após sofrer modificações no Congresso Nacional e vetos parciais pela presidência da República, já na Gestão Temer, o PL nº 1.775/2015 dá origem à Lei nº 13.444/2017, criando a Identificação Civil Nacional (ICN), sem revogação expressa da Lei nº 9.454/1997.

46 LINHA do tempo com as etapas do Projeto RIC. **Revista Idigital**, ano 6, n. 20, p. 64-65, jan./fev./mar./abr. 2015. Disponível em: https://issuu.com/infoliocom/docs/rev20. Acesso em: 4 ago. 2017.

3.3 A escassez de normas sobre proteção de dados na Lei nº 13.444/2017

O texto final da Lei nº 13.444/2017 é merecedor de algumas críticas, notadamente em razão de ter se omitido diante da necessidade de criação de normas para a proteção dos dados pessoais que integrarão a BDICN.

Em verdade, seus únicos dispositivos que podem ser diretamente relacionados à proteção de dados pessoais são os a seguir transcritos:

> Art. 2º [...]
> § 1º A base de dados da ICN será armazenada e gerida pelo Tribunal Superior Eleitoral, que a manterá atualizada e adotará as providências necessárias para assegurar a integridade, a disponibilidade, a autenticidade e a confidencialidade de seu conteúdo e a interoperabilidade entre os sistemas eletrônicos governamentais.
> [...]
> Art. 4º É vedada a comercialização, total ou parcial, da base de dados da ICN.

Em razão da necessidade de se assegurar a proteção dos dados da BDICN, a 3ª Câmara de Coordenação e Revisão do Ministério Público Federal, por meio do Grupo de Trabalho – Tecnologia da Informação e Comunicação (GT-TIC), vem acompanhando a questão desde o desenvolvimento dos trabalhos que resultariam na elaboração do Projeto de Lei nº 1.775/2015, até a publicação da Lei nº 13.444/2017[47].

Ainda durante sua tramitação do Projeto de Lei nº 1.775/2015, foi direcionada ao Congresso Nacional uma Nota Técnica pelo GT-TIC, apontando os principais problemas identificados no texto do projeto. Embora alguns desses problemas tenham sido corrigidos ainda durante a processo legislativo, boa parte deles remanesceram no texto legal.

As omissões da Lei nº 13.444/2017, todavia, não representam problemas insuperáveis, sendo certo que em parte foram supridas pela própria regulamentação da BDICN. Além disso, é possível fazer uso de outras normas de proteção de dados constantes no ordenamento para a solução de eventuais controvérsias.

47 PA 1.00.000.002518/2015-17.

3.4 A regulamentação da BDICN

3.4.1 A Resolução do TSE nº 23.526/2017 e as Resoluções nºs 1, 2 e 3 do Comitê Gestor da ICN

A Resolução do TSE nº 23.526, de 26 de setembro de 2017, dispõe sobre a formação e a operacionalização da BDICN.

Os seus arts. 3º e 4º regulamentam o art. 2º da Lei nº 13.444/2017, já transcrito linhas acima. Note-se que o art. 4º especifica apenas os dados básicos que comporão a base de dados, devendo-se atentar para o fato de que os dados sobre filiação e os dados biométricos (fotografia e digitais) seriam posteriormente classificados como dados sensíveis pela Lei nº 13.709/2018, em seu art. 5º, II.

> Art. 4º A BDICN será armazenada e gerida pelo TSE (Lei nº 13.444/2017, art. 2º, § 1º) e composta dos seguintes dados básicos:
> I – identificador único (número ICN);
> II – nome civil;
> III – nome social;
> IV – sexo;
> V – data de nascimento;
> VI – filiação;
> VII – naturalidade;
> VIII – CPF;
> IX – fotografia;
> X – digitais;
> XI – situação do registro;
> XII – origem do dado.

O parágrafo 3º do art. 4º, por sua vez, supre uma das omissões da Lei nº 13.444/2017, ao estipular que "quaisquer inserções e atualizações na BDICN deverão gerar histórico e ter identificação de origem, para controle, depuração e auditoria". A previsão mostra-se um tanto tímida, mas a questão será resolvida de maneira mais definitiva com a entrada em vigor da Lei Geral de Proteção de Dados, aplicável à BDICN, conforme se verá adiante.

Outro aspecto positivo da Resolução é o fato de trazer uma clara distinção entre

os órgãos que estão autorizados a enviar dados para compor a BDICN[48] e os órgãos públicos ou instituições privadas que terão apenas acesso ao BDICN[49]. Estes últimos terão acesso à BDICN exclusivamente para fins de identificação e autenticação do cidadão.

Também tratam especificamente da proteção de dados da BDICN, os seguintes dispositivos da Resolução nº 23.526/2017.

> Art. 10. O uso dos dados da BDICN obriga quem os tenha obtido a citar a fonte e a assumir a responsabilidade pela manipulação inadequada dos dados obtidos.
> Art. 11. Os órgãos da administração pública que tiverem acesso à BDICN deverão observar as normas e os procedimentos específicos que garantam a segurança, proteção e confidencialidade dos dados.
> Art. 12. Às empresas eventualmente contratadas para a execução de serviços que envolvam a BDICN, é vedada a utilização de quaisquer dados ou informações resultantes da base de dados para fins diversos do serviço contratado, sob pena de imediata rescisão do contrato e sem prejuízo de outras sanções administrativas, civis e criminais.
> Art. 13. Em situações excepcionais, em que haja risco iminente de dano ao Estado ou a terceiros, o TSE poderá suspender cautelarmente o acesso de qualquer órgão da administração pública à BDICN.

O art. 10 é manifestação dos princípios da transparência, da responsabilização e da prestação de contas, descritos na LGPD, art. 6º, VI e X. No art. 11, os princípios a serem observados são os da qualidade dos dados e da segurança (art. 6º, VII e V, da LGPD). Já o art. 12 é manifestação dos princípios da finalidade[50], adequação, responsabilização e prestação de contas (art. 6º, I, II e X, da LGPD). Por fim, o art. 13 é corolário do princípio da prevenção (art. 6º, VII, da LGPD).

Note-se que a Resolução nº 23.526/2017 buscou incorporar ao seu texto normas que encerram princípios regentes da proteção de dados pessoais, tendo sido mais atenta às demandas atuais de proteção de dados que a Lei nº 13.444/2017.

48 Mencionados nos arts. 3º, III, 5º, 6º, 8º, I, 9º.

49 Sobre os quais se referem os art. 8º, II

50 Um exemplo de violação ao princípio da finalidade, passível de ocorrência também em relação aos dados da BDICN, pode ser visto no acórdão do TJSP (AC 355.607.4/0-00, Rel. Des. Carlos Augusto De Santi Ribeiro), em que uma empresa de comércio varejista foi obrigada a indenizar o autor por ter fornecido a particular dados cadastrais daquele, inclusive quanto a seus rendimentos, o que foi utilizado para mover ação de alimentos em face do demandante.

Além da Resolução nº 23.526/2001, é importante lembrar que há previsão na Lei nº 13.444/2017 de criação de um Comitê Gestor da ICN, a quem caberá (art. 5º, § 2º):

> I – recomendar:
> a) o padrão biométrico da ICN;
> b) a regra de formação do número da ICN;
> c) o padrão e os documentos necessários para expedição do Documento Nacional de Identidade (DNI);
> d) os parâmetros técnicos e econômico-financeiros da prestação do serviço de conferência de dados que envolvam a biometria;
> e) as diretrizes para administração do Fundo da Identificação Civil Nacional (FICN) e para gestão de seus recursos;
> II – orientar a implementação da interoperabilidade entre os sistemas eletrônicos do Poder Executivo federal e da Justiça Eleitoral;
> III – estabelecer regimento.

Até o momento, o Comitê Gestor da ICN editou três resoluções. A Resolução nº 1/2017 estabelece o Regimento Interno do Comitê Gestor, a Resolução nº 2/2017 estabelece o CPF como número de uso público da Identificação Civil Nacional[51] e a Resolução nº 3/2017 estabelece os padrões biométricos da ICN[52].

51 Há ainda a previsão de criação de um outro número, de uso interno, para controle de unicidade, vinculado a um registro biométrico individualizado e a um CPF (art. 2º da Resolução nº 2/2017).

52 O COMITÊ GESTOR DA IDENTIFICAÇÃO CIVIL NACIONAL, no uso da atribuição que lhe confere o art. 5º, § 2º, inciso I, alínea a e inciso II da Lei 13.444/2017, resolve:
Art. 1º Recomendar o padrão biométrico da Identificação Civil Nacional e orientar a implementação da interoperabilidade entre os sistemas eletrônicos que acessarão a Base de Dados da Identificação Civil Nacional.§ Os procedimentos de captura dos dados biométricos dos cidadãos, para fins de composição da Base de Identificação Civil Nacional (BDICN), e de intercâmbio de dados biométricos devem seguir os seguintes padrões:
I – Coleta rolada dos 10 (dez) dedos das mãos;
II – ANSI-INCITS 378/2004: Padrão de minúcias de impressões digitais para intercambio de dados;
III – ICAO 9303: padrão de documentação adotado pela *International Civil Aviation Organization*, no que diz respeito à imagem facial;
IV – ISO/IEC FCD 19794: definições de formatos padrão para intercâmbio de dados biométricos, dentre os quais o ISO/UEC FCD 19794-2 e ISO/UEC FCD 19794-4 (padrões de impressão digital) ISO/IEC FCD 19794-5 (padrões de imagem facial);
V – ANSIINIST ITL 1-2000 e ANSI/NIST ITL 2-2008 - Padrão de dados para troca de dados de digitais;
VI – WSQ Versão 3.1: padrão de algoritmo de compressão e armazenamento de imagens de impressões de digitais;
VII – CBEFF (*common biometric exchange formats framework*) : padrão de intercâmbio de dados biométricos;
Art. 2º Esta Resolução entra em vigor na data de sua publicação.

3.4.2 O Decreto nº 9.278/2018

Muito se discutiu, durante a elaboração da Lei nº 13.444/2017, qual seria o papel dos órgãos estaduais de identificação civil diante da instituição do Documento Nacional de Identificação. O Decreto nº 9.278/2018 parece ter trazido a resposta, ao modificar a regulamentação da Lei nº 7.116/2018, a qual assegura validade nacional às carteiras de identidade e regula sua expedição.

Perceba-se que o Decreto trata do documento expedido pelos estados e não do futuro Documento Nacional de Identificação previsto na Lei nº 13.444/2017, mas sua análise é de fundamental importância para a compreensão da BDICN e do Documento de Identificação Nacional, já que o principal objetivo da edição de novo decreto regulamentador para a Lei nº 7.116/1983 foi conciliar o antigo sistema de identificação com o novo modelo traçado pela Lei nº 13.444/2017, inclusive com a integração das respectivas bases de dados. Vejamos:

> Art. 5º A Carteira de Identidade conterá:
> [...]
> VI – fotografia, no formato 3X4cm, a assinatura e a impressão digital do polegar direito do identificado;
> [...]
> §4º Para fins do disposto no inciso VII do *caput*, padrões biométricos seguirão as recomendações do Comitê Gestor da Identificação Civil Nacional – ICN.
> [...]
> Art. 4º Na expedição da Carteira de Identidade será realizada a validação biométrica com a Base de Dados da ICN para aferir a conformidade com o Documento Nacional de Identificação – DNI.
> Parágrafo único. O disposto no *caput* e no inciso I do § 1º do art. 8º está condicionado à existência de compartilhamento de dados entre o órgão de identificação e o Tribunal Superior Eleitoral.

Como se pode ver do parágrafo único do art. 4º, a integração dos dois sistemas, no que se refere à biometria, ficou condicionada à existência de compartilhamento de dados entre o órgão de identificação e o Tribunal Superior Eleitoral.

Infelizmente o Decreto não estipula prazo para que essa integração ocorra, não sendo demais lembrar que essa integração, caso seja estabelecida da maneira correta, é uma eficiente forma de evitar fraudes, pois será capaz de detectar a expe-

dição de documentos de identificação diferentes para os mesmos padrões biométricos, ou seja, um mesmo indivíduo possuindo mais de uma carteira de identidade com dados qualificativos diferentes (nome, idade, filiação, naturalidade), e também evitar que dois indivíduos diferentes compartilhem de uma mesma identificação, em outros termos, impedir que uma pessoa assuma a identidade de outra.

Outras mudanças interessantes estabelecidas no Decreto nº 9.278/2018 encontram-se nos arts. 8º e 9º, *in verbis*:

> Art. 8º Será incluído na Carteira de Identidade, mediante requerimento:
> I – o número do DNI;
> II – o Número de Identificação Social - NIS, o número no Programa de Integração Social - PIS ou o número no Programa de Formação do Patrimônio do Servidor Público - PASEP;
> III – o número do Cartão Nacional de Saúde;
> IV – o número do Título de Eleitor;
> V – o número do documento de identidade profissional expedido por órgão ou entidade legalmente autorizado;
> VI – o número da Carteira de Trabalho e Previdência Social;
> VII – o número da Carteira Nacional de Habilitação;
> VIII – o número do Certificado Militar;
> IX – o tipo sanguíneo e o fator Rh;
> X – as condições específicas de saúde cuja divulgação possa contribuir para preservar a saúde ou salvar a vida do titular; e
> XI – o nome social.
> § 1º A comprovação das informações de que tratam os incisos I a VIII do *caput* será feita por meio, respectivamente:
> I – da validação biométrica com a base de dados da ICN;
> II – dos cartões de inscrição no NIS, no PIS ou no PASEP;
> III – do Cartão Nacional de Saúde;
> IV – do Título de Eleitor;
> V – do documento de identidade profissional expedido por órgão ou entidade legalmente autorizado;
> VI – da Carteira de Trabalho e Previdência Social;
> VII – da Carteira Nacional de Habilitação;
> VIII – do Certificado Militar;
> IX – do resultado de exame laboratorial; e

> X – do atestado médico ou documento oficial que comprove a vulnerabilidade ou a condição particular de saúde que se deseje preservar, nos termos do inciso X do *caput*.
> § 2º Em substituição aos documentos de que tratam os incisos I a VIII do *caput*, será aceita a apresentação de documento de identidade válido para todos os fins legais do qual constem as informações a serem comprovadas.
> § 3º A comprovação pelo interessado das informações de que tratam os incisos II a X do *caput* será dispensada na hipótese do órgão de identificação ter acesso às informações por meio de base eletrônica de dados de órgão ou entidade públicos.
> § 4º O nome social de que trata o inciso XI do *caput*:
> I – será incluído:
> a) mediante requerimento escrito do interessado;
> b) com a expressão "nome social";
> c) sem prejuízo da menção ao nome do registro civil no verso da Carteira de Identidade; e
> d) sem a exigência de documentação comprobatória; e
> II – poderá ser excluído por meio de requerimento escrito do interessado.
> § 5º O requerimento de que trata a alínea "a" do inciso I do § 4º será arquivado no órgão de identificação, juntamente com o histórico de alterações do nome social.
> Apresentação dos documentos mencionados na Carteira de Identidade
> Art. 9º A Carteira de Identidade fará prova de todos os dados nela incluídos e dispensará a apresentação dos documentos que nela tenham sido mencionados.

Note-se que a solução adotada pelo Poder Público Federal para a constante crítica sobre a necessidade de se possuírem inúmeros documentos de identificação foi, a princípio, permitir a inclusão dos dados dos diversos documentos de identificação na Carteira de Identidade, estabelecendo que, neste caso, esta fará prova de todos os outros documentos cujos dados estejam nela incluídos, sem a necessidade de apresentação destes.

É importante notar, todavia, que não é descartada a necessidade de elaboração dos documentos previstos no art. 8º, sendo fácil perceber que a confecção dos documentos previstos nos incisos II a VIII permanece obrigatória, a exemplo do

Certificado Militar, da CNH e do Título de Eleitor. No quadro atual, portanto, o Documento Nacional de Identificação, além de não excluir a necessidade da elaboração dos inúmeros documentos de identificação impostos aos brasileiros, torna-se mais um documento, a somar-se aos demais.

Não se descarta, todavia, que o objetivo final seja a integração de todos esses sistemas, de maneira que os dados necessários à identificação dos indivíduos perante os diferentes órgãos expedidores dos documentos previstos no art. 8º passem a integrar, automaticamente, o Documento Nacional de Identificação (DNI) ou a Carteira de Identidade (CI), tornando desnecessária a elaboração de diversos documentos. Em verdade, um importante passo foi dado nessa direção, ao instituir-se que os órgãos de identificação estadual poderão utilizar como número do registro geral o número de inscrição no CPF (art. 5º, § 1º). Isso porque a Lei nº 13.444/2017 parece buscar a convergência dos diversos documentos de identificação para o uso do mesmo número de inscrição, o do CPF (art. 9º e 11 da Lei nº 13.444/2017).

Cabe destaque, ainda, à autorização expressa de inclusão do nome social na Carteira de Identidade (§ 4º), que segue na esteira do Decreto nº 8.727/2016, o qual prevê o uso do nome social por travestis ou transexuais no âmbito da Administração Pública Federal Direta, Autárquica e Fundacional.

Por fim, destaque-se que o Decreto nº 9.278/2018 faculta a expedição da Carteira de Identidade em meio eletrônico, mas sem prejuízo da expedição em meio físico (art. 11). Portanto, haverá a expedição do DNI apenas por meio eletrônico, mas a CI, ao menos por enquanto, continuará sendo expedida em meio físico, ainda que possua também uma versão digital.

3.5 Outras normas aplicáveis na proteção da BDICN

O ordenamento jurídico nacional dispõe de diversas normas relacionadas à proteção de dados pessoais, dispersas em dispositivos constitucionais, legais e infralegais.

Na Constituição Federal, é possível citar os seguintes dispositivos relacionados à proteção de dados:

- Art. 1º, III; e
- Art. 5º, X, XII, XXXIII, XXXIV, "b", LXXII e LXXVII.

A tutela constitucional da dignidade da pessoa humana, da liberdade, da privacidade, da intimidade, da honra e da imagem, bem como a disciplina constitucional do *habeas data*, deverá sempre orientar o operador do Direito na proteção de dados pessoais.

As seguintes leis também dispõem de normas de proteção de dados:

- Decreto-Lei nº 2.848/1940 (Código Penal), arts. 153, § 1º-A, 154-A e 313-A;
- Decreto-Lei nº 3.689/1941 (Código de Processo Penal), arts. 13-A e 13-B;
- Lei nº 7.116/1983 (Assegura validade nacional às Carteiras de Identidade) e Decreto nº 9.278/2018, que a regulamenta;
- Lei nº 7.232/1984 (Dispõe sobre a Política Nacional de Informática, e dá outras providências);
- Lei nº 8.078/1990 (Código de Defesa do Consumidor), arts. 43, 72 e 73;
- Lei nº 9.472/1997 (Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995);
- Lei nº 9.507/1997 (Lei do *Habeas Data*);
- Lei nº 9.296/1996 (Lei de Interceptação Telefônica);
- Lei nº 7.492/1986 (Define os crimes contra o sistema financeiro nacional), art. 18 (considera crime a violação do dever de sigilo das instituições financeiras);
- Lei nº 9.504/1997 (Estabelece normas para as eleições);
- Lei nº 10.406/2002 (Código Civil), arts. 20 e 21;
- Lei nº 12.414/2011 (Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito);
- Lei nº 12.527/2011 (Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências);
- Lei nº 12.654/2012 (Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 – Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências);

- Lei nº 12.737/2012 (Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências);
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Há também um vasto rol de decretos e resoluções com normas sobre proteção de dados. Vejamos alguns:

- Decreto nº 3.505/2000 (Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal);
- Portaria nº 5/2002 da SDE/MJ, art. 1º, I e II;
- Instrução CVM nºs 380/2002 (Estabelece normas e procedimentos a serem observados nas operações realizadas em bolsas e mercados de balcão organizado por meio da rede mundial de computadores e dá outras providências);
- Decreto nº 4.489/2002 (Regulamenta o art. 5º da Lei Complementar nº 105, de 10 de janeiro de 2001, no que concerne à prestação de informações à Secretaria da Receita Federal do Ministério da Fazenda, pelas instituições financeiras e as entidades a elas equiparadas, relativas às operações financeiras efetuadas pelos usuários de seus serviços);
- Instrução CVM nº 461/2007 (Disciplina os mercados regulamentados de valores mobiliários e dispõe sobre a constituição, organização, funcionamento e extinção das bolsas de valores, bolsas de mercadorias e futuros e mercados de balcão organizado);
- Resolução CFM nº 1.821/2007 (Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde);
- Decreto nº 6.029/2007 (Institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências);
- Decreto nº 6.135/2007 (Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal e dá outras providências);
- Decreto nº 6.425/2008 (Dispõe sobre o Censo Anual da Educação);
- Decreto nº 6.523/2008 (Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para fixar normas gerais sobre o Serviço de Atendimento ao Consumidor – SAC);

- Resolução Normativa ANS – RN nº 305/2012 (Estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar – Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde; revoga a Resolução Normativa – RN nº 153, de 28 de maio de 2007 e os arts. 6º e 9º da RN nº 190, de 30 de abril de 2009);
- Decreto nº 7.962/2013 (Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico);
- Resolução CMN nº 4.474/2016 (Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente);
- Resolução Bacen nº 4.480/2016 (Dispõe sobre a abertura e o encerramento de contas de depósitos por meio eletrônico e dá outras providências);
- Decreto nº 8.789/2016 (Dispõe sobre o compartilhamento de bases de dados na administração pública federal);
- Decreto nº 8.764/2016 (Institui o Sistema Nacional de Gestão de Informações Territoriais e regulamenta o disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009);
- Decreto nº 8.777/2016 (Institui a Política de Dados Abertos do Poder Executivo federal);

Esse microssistema, com a edição da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), ainda em período de vacância, adquiriu considerável robustez, pois esse diploma legal explicitou uma vasta base principiológica que rege a proteção de dados. Por serem tais princípios corolários de direitos e garantias fundamentais previstos na Constituição Federal, sua aplicação independe do termo final da vacatio legis, previsto para fevereiro de 2020.

É importante destacar que a disciplina de proteção de dados pessoais trazida pela LGPD se aplicará à BDICN. Observe-se o que diz o referido texto legal:

> 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 fundamen-

> tais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> [...]
> Art. 3º Esta Lei aplica-se 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, desde que:
> I – a operação de tratamento seja realizada no território nacional;
> II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do *caput* do art. 4º desta Lei.

Perceba-se que, em condições normais, a BDICN estará abrangida pelos três incisos do art. 3º, pois a operação de tratamento se dará no Brasil e será de dados coletados no território nacional, sobre indivíduos localizados no território nacional.

É necessário ressaltar que a formação de bancos de dados para identificação civil não se confunde com nenhuma das finalidades arroladas nos incisos do art. 4º, não se tratando, pois, de exceção à aplicação da LGPD. Vejamos:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II – realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III – realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV – provenientes de fora do território nacional e que não sejam objeto

> de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º 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.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do *caput* deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do *caput* deste artigo poderá ser tratada por pessoa de direito privado.

Outras normas de proteção de dados aplicáveis na proteção da BDICN e que merecem, no ponto, maior destaque, são as que tipificam crimes.

Como a base de dados da ICN será armazenada e gerida pelo Tribunal Superior Eleitoral[53], há atribuição do Ministério Público Federal para a persecução penal de diversos delitos envolvendo o referido banco de dados[54]. Entre tais delitos podem ser citados os previstos nos seguintes dispositivos:

- art. 153, § 1º-A c/c § 2º, do Código Penal[55];

53 Art. 2º, § 1º, da Lei nº 13.444/2017.

54 Art. 109. Aos juízes federais compete processar e julgar: [...]
IV – os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral; [...]

55 § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

- art. 154-A c/c art. 154-B do Código Penal[56];
- art. 313-A do Código Penal[57];
- art. 325 do Código Penal[58].

Além dos crimes acima citados, que estariam relacionados ao banco de dados da ICN, caberá ainda ao MPF a persecução dos crimes de falsidade envolvendo o Documento Nacional de Identificação, seja por violação ao disposto no art. 297 do CP (falsificação de documento público), seja por violação ao disposto no art. 299 do CP (falsidade ideológica). Isso porque o aludido documento deverá ser expedido pela Própria Justiça Eleitoral ou mediante sua certificação, conforme dispõe o art. 8º, § 3º, da Lei nº 13.444/2017.

Neste ponto, vale a pena lembrar que a jurisprudência nacional se pacificou no sentido de que o delito de falsificação é absorvido pela prática da fraude quando nela se exaure, sempre que não se identifique maior potencialidade lesiva no delito de falsificação, tal qual orienta o Enunciado nº 17 da Súmula do STJ[59]. Neste caso específico, pouca relevância haveria quanto ao órgão responsável pela emissão do documento, pois a identificação do órgão ao qual este foi apresentado é que assumirá maior importância para determinar a competência estadual ou federal para julgamento do delito. É o que dispõe outro verbete sumular do STJ, o de número 546.

Não obstante, tratando-se da falsificação de DNI, é pouco provável que se conclua, no caso concreto, que a potencialidade lesiva da falsificação se esgotou na prática de um único delito, pois o documento de identificação falso pode servir à prática de inúmeras fraudes.

§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

56 Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012)
Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

57 Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

58 Art. 325. Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena – detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
§ 1º Nas mesmas penas deste artigo incorre quem:
I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;
II – se utiliza, indevidamente, do acesso restrito.
§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

59 Súmula 17: Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido.

3.6 Principais omissões da Lei nº 13.444/2017 na proteção da BDICN

Uma vez compreendidos os principais subsídios normativos para a solução das controvérsias envolvendo a proteção de dados da BDICN, cabe enumerar algumas omissões da Lei nº 13.444/2017 e indicar como eventuais dúvidas surgidas a partir dessas omissões podem ser resolvidas, de maneira a preservar o direito à autodeterminação informativa.

3.6.1 Regra geral de proteção de dados

A Lei da Identificação Civil Nacional deveria ter estabelecido expressamente que a formação e tratamento da BDICN se submete ao direito à proteção de dados dos indivíduos afetados e às suas faculdades inerentes.

A ausência de informação expressa e clara no texto legal a respeito da necessidade de compatibilizar seus dispositivos ao direito à proteção de dados obviamente não representa óbice para o exercício desse direito. É de se destacar, todavia, que a melhor técnica legislativa recomenda que informações como esta sejam incorporadas ao texto legal, a fim de evitar dúvidas e reforçar a necessidade de proteção do direito individual tutelado quando da aplicação da lei. A título de exemplo, é o que faz o Marco Civil da Internet, *in literis*:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> [...]
> II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> [...]
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> [...]
> II – proteção da privacidade;
> III – proteção dos dados pessoais, na forma da lei;

Ademais, como já visto, a posterior edição da Lei Geral de Proteção de Dados, com previsão de aplicação ao tratamento de dados por órgãos públicos trouxe mais luz à questão.

3.6.2 Registro do operador e das operações de tratamento de dados

A previsão quase sem ressalvas[60] de acesso ao banco de dados da ICN pelo Poder Executivo da União, dos estados, do Distrito Federal e dos municípios (art. 3º) se mostra temerosa ao não estabelecer a necessidade de registro das operações de tratamento e de seu operador.

Pecou gravemente o legislador nesse ponto. É extremamente necessário que leis que instituem bancos de dados pessoais estipulem a forma como se dará o controle de acesso e registro de cada operação de tratamento de dados, gravando-se, por exemplo, número do terminal, horário e finalidade da operação.

A questão poderia ter sido resolvida da forma como fez a Lei nº 12.414/2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, a qual assevera, em seu art. 9º, § 4º:

> O gestor deverá assegurar, sob pena de responsabilidade, a identificação da pessoa que promover qualquer inscrição ou atualização de dados relacionados com o cadastrado, registrando a data desta ocorrência, bem como a identificação exata da fonte, do nome do agente que a efetuou e do equipamento ou terminal a partir do qual foi processada tal ocorrência.

Não tendo a Lei nº 13.444/2017 estabelecido qualquer regra a esse respeito, coube à Resolução do TSE nº 23.526/2017 solucionar a questão, estipulando:

> Art. 4º A BDICN será armazenada e gerida pelo TSE (Lei nº 13.444/2017, art. 2º, § 1º) e composta dos seguintes dados básicos: [...]
> § 3º Quaisquer inserções e atualizações na BDICN deverão gerar histórico e ter identificação de origem, para controle, depuração e auditoria.
> [...]
> Art. 7º O TSE garantirá acesso à BDICN aos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e ao Ministério Público, de forma gratuita, exceto quanto às informações eleitorais (Lei nº

60 A única restrição prevista expressamente no dispositivo diz respeito às informações eleitorais.

> 13.444/2017, art. 3º).[...]
> Parágrafo único. Para ter acesso à BDICN, o interessado deverá solicitar ao TSE o seu credenciamento.

Ademais, o art. 6º da LGPD, ao discorrer sobre o princípio da transparência, em seu inciso VI, garante aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

3.6.3 Acesso limitado à necessidade de cada órgão público

Não restou explicitado que o acesso ao BDICN deve ser limitado à necessidade de cada órgão público.

A medida não obstaria o uso das informações pelos agentes públicos que de fato delas necessitam e seria capaz de prevenir os desvios de finalidade que o acesso universalizado e ilimitado potencializam[61].

A Resolução do TSE nº 23.526/2017 trata da questão, tendo vedado o acesso a dados biométricos e eleitorais a outros órgãos públicos e enumerado as finalidades únicas de atualização da base de dados, identificação e autenticação do cidadão. A Resolução indicou ainda os órgãos que teriam acesso à BDICN[62]. Vejamos:

> Art. 8º O acesso à BDICN poderá ser realizado das seguintes formas, observado o disposto no art. 31 da Lei nº 12.527/2011:
> I – por meio de serviços eletrônicos disponibilizados pelo TSE, para fins de atualização das bases de dados da administração pública;
> II – por meio de serviços eletrônicos disponibilizados pelo TSE à administração pública e às instituições privadas, para fins de identificação e autenticação do cidadão.
> § 1º Dados biométricos e eleitorais não serão disponibilizados pelo

61 A título de exemplo, vale conferir como o Decreto nº 8.764/2016 (Institui o Sistema Nacional de Gestão de Informações Territoriais e regulamenta o disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009). Trata da questão, no *caput* de seu art. 3º, *in literis*: "O acesso pelos usuários às informações armazenadas no Sinter deverá ser efetuado observado o limite de suas competências, do sigilo fiscal e das demais hipóteses legais de sigilo e de restrição ao acesso a informações".

62 É de se observar que o Decreto nº 8.789/2016 prevê hipóteses bastante amplas para o compartilhamento de bases de dados mantidos pela Administração Pública Federal, porém, além de a BDICN não ser mantida pelo Executivo Federal, com a Resolução do TSE nº 23.526/2017, esta base de dados passou a ter regras próprias para o seu compartilhamento, aplicando-se o princípio da especialidade.

> TSE (Lei nº 13.444/2017, art. 3º, *caput* e § 1º).
> § 2º Os direitos de acesso à BDICN e os dados dela obtidos não poderão ser transferidos ou cedidos a terceiros.
> Art. 9º Para atendimento ao inciso I do art. 8º, os serviços de atualização de dados serão disponibilizados aos órgãos públicos que:
> I – tiverem como missão institucional a identificação do cidadão;
> II – fornecerem os atributos básicos do cidadão cujo registro for objeto de atualização;
> III – fornecerem a biometria e o CPF do cidadão cujo registro for objeto de atualização; ou
> IV – possuírem acordo de cooperação técnica firmado com o TSE para fornecimento de dados da BDICN.

É de se elogiar, também, a abordagem da questão feita pela LGPD, por ter estabelecido no rol de princípios do art. 6º os princípios da finalidade[63], da adequação, da necessidade, da responsabilização e prestação de contas.

> Art. 5º Para os 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;
> 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;

63 Um outro exemplo de norma de proteção de dados pessoais que determina a observância do princípio da especialidade pode ser vista no art. 6º do Decreto nº 6.425/2008, que diz: "Ficam assegurados o sigilo e a proteção de dados pessoais apurados no censo da educação, vedada a sua utilização para fins estranhos aos previstos na legislação educacional aplicável".

> [...]
> 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.

O art. 26 fecha a questão de maneira ainda mais clara, enunciando:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

3.6.4 Previsão de acesso gratuito e irrestrito a dados próprios

Outra injustificável omissão do legislador se refere à ausência de previsão de acesso gratuito e irrestrito dos cidadãos aos próprios dados, assim como da obrigatoriedade de pronta resposta a pedidos de correção de dados equivocados. Quanto a esse ponto, a Resolução do TSE nº 23.526/2017 também se silenciou.

A ausência de previsão específica, embora merecedora de críticas, novamente não haverá de limitar o direito do titular dos dados, pois tal direito se encontra tutelado pela disciplina constitucional e legal do *habeas data*[64], pela disciplina constitucional e legal do direito de acesso à informação[65], assim como pela Lei Geral do Processo Administrativo[66].

Aliás, a LGPD, ao abordar a questão, apenas declara o aludido direito, em seu art. 6º, IV, ao instituir que as atividades de tratamento de dados pessoais deverão observar o princípio do livre acesso consistente na "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"; mas quanto aos prazos e à forma de exercício desse direito, faz remissão à Lei do *Habeas Data*, à Lei de Acesso à Informação e à Lei Geral do Processo Administrativo.

64 Art. 5º, LXXII, da CF, e Lei nº 9.507/1997.

65 Art. 5º, XXXIII, da CF, e Lei nº 12.527/2011.

66 Lei nº 9.784/1999.

Em julgamento recente, a Primeira Turma do Supremo Tribunal Federal teve oportunidade de decidir sobre o acesso a dados pessoais mantidos pela Administração Fazendária, sendo plenamente possível transpor os argumentos ali tecidos para outros bancos de dados mantidos pelo Poder Público. Confira-se a emenda do julgado:

> EMENTA: DIREITO CONSTITUCIONAL E TRIBUTÁRIO. AGRAVO INTERNO EM RECURSO EXTRAORDINÁRIO. ACESSO À INFORMAÇÃO CONTIDA EM ÓRGÃO DE ADMINISTRAÇÃO FAZENDÁRIA. DIREITO DO CONTRIBUINTE. 1. O Supremo Tribunal Federal, ao julgar o RE 673.707-RG, sob a relatoria do Ministro Luiz Fux, assentou que o contribuinte tem direito de obter informações contidas nos registros da Receita Federal do Brasil ou qualquer outro órgão de Administração Fazendária de outras entidades estatais, tendo em vista tratar-se de dados pessoais relativos ao próprio requerente, e que não comprometem a segurança da sociedade ou do Estado. 2. Agravo interno a que se nega provimento. (RE nº 601766 AgR/MG, Relator Min. ROBERTO BARROSO, julgamento em 29/09/2017, Primeira Turma)

3.6.5 Emissão gratuita da primeira via do DNI

Por fim, embora a questão não diga respeito, diretamente, à tutela do direito à proteção de dados, é preciso chamar a atenção para o fato de que um importante dispositivo foi suprimido do projeto de lei pelo veto presidencial. Ao suprimir o § 2º do art. 8º do texto legal, que previa a emissão gratuita da primeira via do documento, justificou-se a Presidência da República com o argumento de que a previsão representaria considerável impacto orçamentário à União e que uma futura regulamentação da lei estabeleceria os critérios da gratuidade "em função dos públicos".

O referido veto, no entanto, vai na contramão de importante conquista alcançada com a edição da Lei nº 12.687/2012, que, alterando a Lei nº 7.116/1983, impôs a gratuidade da emissão da primeira via das carteiras de identidade expedidas pelos estados. Acaso não haja a referida previsão no decreto regulamentador, de garantia da gratuidade da primeira via do DNI ao menos às classes mais carentes, não há dúvidas de que, com a progressiva substituição das atuais carteiras de identidade pelo DNI, haverá grave risco de que o exercício de direitos fundamentais de cidadãos de classes menos favorecidas seja cerceado.

3.7 Conclusão

Não há dúvidas de que a Lei nº 13.444/2017 veio em boa hora e viabiliza esperados avanços para o sistema de identificação dos cidadãos brasileiros. Porém, ao se avançar no uso de novas tecnologias, é natural que surjam também novos desafios. Portanto, é necessário estar atento às fragilidades até então inexistentes e às novas formas de violação de direitos individuais, buscando-se novos mecanismos de defesa desses mesmos direitos. No caso da Lei nº 13.444/2017, merece especial atenção a recém-criada Base de Dados da Identificação Civil Nacional, bem como as inúmeras formas de mau uso das informações ali contidas. Felizmente, na esteira do desenvolvimento tecnológico, a legislação nacional também tem avançado quanto à proteção de dados pessoais, em um movimento a ser acompanhado de perto pelos órgãos incumbidos de preservar esse direito.

4 A PROTEÇÃO PELO MPF DOS DADOS PESSOAIS DOS USUÁRIOS DA INTERNET

Alexandre Assunção e Silva

4.1 Conceito de dados pessoais

De acordo com a Convenção de Strasbourg (1981), informação pessoal é aquela relativa a uma pessoa identificada ou identificável. É proveniente de seus atos, dados de consumo e opiniões que o indivíduo manifesta, apresentando uma ligação concreta com o indivíduo.

O Decreto nº 8.771/2016, ao regulamentar a Lei nº 12.965/2014, tratou do conceito de dados pessoais no seu art. 14, inciso I: "dado pessoal – dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa." A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) foi bem mais sintética ao conceituar dados pessoais, no art. 5º, I: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

Parcela da doutrina trata os dados pessoais como direito de propriedade. Os dados pessoais são tutelados como direitos da personalidade, pois são emanações imediatas desta.

Entre os dados pessoais encontram-se os dados sensíveis, informações que, se conhecidas e processadas, prestam-se a uma potencial utilização discriminatória ou lesiva, particularmente mais intensa e que apresenta maiores riscos potenciais que a média. Exemplos: dados sobre raça, credo político, religioso, opções sexuais, histórico médico, dados genéticos. A análise de dados sensíveis apresenta elevado potencial lesivo aos titulares. Mas mesmo dados não considerados sensíveis, submetidos a tratamento, podem levar à discriminação.

4.2 Criação de perfis

Sabe-se que empresas de tecnologia monitoram as atividades do consumidor quando conectado à internet – incluindo as pesquisas que ele fez, as páginas que ele visitou e o conteúdo consultado – com a finalidade de fornecer publicidade dirigida aos interesses individuais desse consumidor.

Grandes empresas de tecnologia da internet, como o Google, coletam dados pessoais dos usuários de seus serviços, para fins comerciais, principalmente. Os dados são tratados com o auxílio de métodos estatísticos e técnicas de inteligência artificial, com o fim de sintetizar hábitos, preferências pessoais e outros registros. A partir disso são criados perfis para cada usuário (*profiling*) que possibilitam o envio seletivo de mensagens publicitárias de um produto a seus potenciais compradores.

Redes sociais on-line como o Facebook também realizam o tratamento de dados pessoais dos seus usuários. A rede social permite a seus usuários gerar um perfil público, alimentado por dados e informações pessoais, dispondo de ferramentas que permitem a interação com outros usuários afins ou não ao perfil publicado. A rede social é um intermediário que acumula informações pessoais sobre os usuários.

Os clientes de redes sociais são aqueles que efetivamente contratam a rede social mediante retribuição, não os usuários, mas empresas que apresentam interesse na base de dados e na relação de usuários, para oferecer publicidade focada em grupos.

As possibilidades oferecidas a uma pessoa são fechadas (encaixotadas) em torno de presunções realizadas por ferramentas de análise comportamental, guiando dessa forma suas escolhas futuras. A publicidade específica tem o efeito colateral de uniformizar padrões de comportamento, diminuindo o rol de escolhas apresentadas a uma pessoa.

A elaboração de perfis pode levar à negativa de acesso a determinado bem ou serviço (negativa de acesso a site porque o consumidor acessou sites de proteção ao crédito), bem como preços diferentes a consumidores diversos conforme o seu perfil (*adaptative pricing*).

Daí porque é fundamental o consentimento prévio do usuário de internet, autorizando o tratamento de seus dados pessoais. O endereço de e-mail, por exemplo, é um dado de caráter pessoal que não deve ser compartilhado sem autorização expressa. Os e-mails não são informações públicas e, portanto, somente podem ser objeto de tratamento no caso de haver consentimento.

4.3 Direitos dos usuários da internet

Os direitos e garantias dos usuários da internet encontram-se no art. 7º da Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet. Estão transcritos a seguir:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV – não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V – manutenção da qualidade contratada da conexão à internet;
> VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da

> relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII – acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Note-se que dos treze incisos que compõem os direitos e garantias dos internautas, enumerados no art. 7º do Marco Civil da Internet, nove dizem respeito à proteção dos dados pessoais (incisos I, II, III, VI, VII, VIII, IX, X). Os demais tratam da não suspensão da conexão à internet, salvo por débito (inciso IV); qualidade do serviço (inciso V), direito à informação sobre as políticas de uso (inciso XI); acessibilidade (inciso XII); e aplicação do Código de Defesa do Consumidor (inciso XIII).

Os três primeiros incisos do art. 7º da Lei nº 12.965/2014 tratam da inviolabilidade do fluxo das comunicações realizadas pela internet e do sigilo das comunicações privadas armazenadas. Alguém só pode ser monitorado, ou seja, ter suas conversas travadas por e-mail interceptadas, por exemplo, se houver autorização judicial (inciso II). Além disso, caso o celular de alguém seja apreendido para investigação de um crime, as conversas via WhatsApp ou outro meio de comunicação, nele armazenadas, só podem ter o sigilo levantado por ordem judicial (inciso III). Caso essas garantias não sejam respeitadas, a pessoa lesada terá o direito de ser indenizada pelos danos materiais e morais decorrentes de sua violação (inciso I), e a prova eventualmente colhida será considerada ilícita.

O direito a informações claras e completas nos contratos de prestação de serviços, já bastante conhecido no direito do consumidor, é expressamente apontado na primeira parte do inciso VI, com destaque para o regime de proteção aos registros de conexão e registros de acesso a aplicações de internet. O Decreto nº 8.771/2016, que regulamentou a Lei nº 12.965/2014, trouxe mais detalhes sobre como deve ocorrer essa proteção:

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
> I – o estabelecimento de controle estrito sobre o acesso aos dados me-

> diante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
> II – a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
> III – a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e
> IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.
> [...]
> Art. 16. As informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais.

O inciso VII declara que os dados pessoais só podem ser fornecidos a terceiros, como sites parceiros dos provedores de conexão ou aplicação, se houver consentimento livre expresso e informado. O usuário tem o direito de negar a transferência de seus dados, como o histórico de navegação, a terceiros.

Além disso, é preciso que haja informações claras sobre coleta, uso, armazenamento, tratamento e proteção dos dados, na forma do inciso VIII, que só poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam proibidas e estejam especificadas nos termos de uso. Não deve ser admitido "o consentimento genérico para o tratamento de dados pessoais, porém somente quando é especificada sua finalidade, bem como não seria cabível sua interpretação extensiva para hipóteses fora das expressamente previstas."[67]

De acordo com o inciso IX, a coleta, o uso, o armazenamento e qualquer tratamento de dados pessoais[68] só pode ocorrer mediante consentimento expresso e

67 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 383.

68 O Decreto nº 8.771/2016, no art. 14, inciso II, esclarece que constitui tratamento de dados pessoais qualquer operação realizada com esses dados, "como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução,

destacado do interessado. Isso quer dizer que o tratamento dos dados precisa ser autorizado em janela específica, sendo insuficiente o consentimento geral fornecido no momento da adesão aos termos de uso e à política de privacidade da empresa. O consentimento concedido em janela específica permite que o usuário o revogue posteriormente, sem que deixe de ter acesso ao serviço.

A forma de exclusão definitiva dos dados pessoais, exigida pelo inciso X do art. 7º da Lei nº 12.965/2014, foi regulamentada no art. 13 do Decreto nº 8.771/2016, a seguir:

> Art. 13. *Omissis.*
> [...]
> § 2º Tendo em vista o disposto nos incisos VII a X do *caput* do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
> I – tão logo atingida a finalidade de seu uso; ou
> II – se encerrado o prazo determinado por obrigação legal.

São princípios comuns de garantia do cidadão no uso de dados pessoais (*fair information principles*):

> 1 – não deve existir um sistema de armazenamento de dados pessoais cuja existência seja mantida em segredo.
> 2 – deve existir um meio para o indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma elas são utilizadas.
> 3 – deve existir um meio para o indivíduo evitar que a informação a seu respeito, colhida para determinado fim, seja utilizada para outros propósitos sem o seu conhecimento.
> 4 – deve existir um meio para o indivíduo corrigir ou retificar informações a seu respeito.
> 5 – toda organização que estruture, mantenha ou utilize dados pessoais deve garantir a confiabilidade dos dados e evitar o mau uso destes.

transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração."

Ainda que se trate de uma empresa estrangeira sem filial no Brasil, ela estará obrigada a respeitar os direitos previstos no art. 7º da Lei nº 12.965/2014, que cuidam da proteção de dados pessoais, desde que os dados sejam coletados em território nacional, em terminal localizado no Brasil, e o serviço seja ofertado ao público brasileiro, nos termos do art. 11, §§ 1º e 2º, da referida lei:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

4.4 Aplicação do CDC

Está pacificado na jurisprudência que as empresas que fornecem aplicativos da internet estão sujeitas às normas de defesa do consumidor, mesmo que não haja uma remuneração direta paga pelo usuário, pois no caso há uma remuneração indireta, que se dá por meio da obtenção de vantagens econômicas pelo oferecimento de serviços gratuitos. Sobre a existência de relação de consumo, segue decisão do Superior Tribunal de Justiça no RESP nº 1.193.764 – SP:

> DIREITO CIVIL E DO CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO SITE PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. CIÊNCIA DA EXISTÊNCIA DE

> CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA. *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. [...]* (grifo nosso)

Além disso, a própria Lei nº 12.965/2014 manda aplicar a legislação de defesa do consumidor nas relações firmadas pela internet, nos termos do art. 7º, inciso XIII: "aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.". Desse modo, além dos direitos previstos expressamente no Marco Civil da Internet, o internauta possui toda a gama de direitos previstos no Código de Defesa do Consumidor. Por exemplo, os Termos de Serviço e a Política de Privacidade das empresas que operam na internet são equiparados a contratos de adesão, pois por meio deles o usuário adere ao serviço. Assim, qualquer limitação de direitos, como o compartilhamento de dados pessoais, deve ser informada de maneira clara e destacada, pois constitui limitação do direito à privacidade, na forma do art. 54, §§ 3º e 4º do Código de Defesa do Consumidor:

> Art. 54. *Omissis.*
> § 3º Os contratos de adesão escritos serão redigidos em termos claros e com caracteres ostensivos e legíveis, cujo tamanho da fonte não será inferior ao corpo doze, de modo a facilitar sua compreensão pelo consumidor.
> § 4° As cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão.

4.5 Atuação do Ministério Público Federal

Cabe ao Ministério Público Federal zelar pela proteção dos direitos do consumidor e dos usuários de provedores e aplicativos da internet, na forma do art. 6º, VII, letra "c", *in fine*, e letra "d", da Lei Complementar nº 75/1993, com a adoção das medidas judiciais e extrajudiciais cabíveis:

> Art. 6º Compete ao Ministério Público da União:
> [...]
> VII – promover o inquérito civil e a ação civil pública para:
> [...]
> c) a proteção dos interesses individuais indisponíveis, *difusos e coletivos*, relativos às comunidades indígenas, à família, à criança, ao adolescente, ao idoso, às minorias étnicas e ao *consumidor*; (grifo nosso)

Conforme o art. 8º da Lei nº 12.965/2014, são nulas de pleno direito as cláusulas contratuais que impliquem ofensa ao sigilo das comunicações privadas:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no *caput*, tais como aquelas que:
> I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

A Lei nº 8.078/1990, Código de Defesa do Consumidor (CDC), admite expressamente a legitimidade do Ministério Público para propor ação anulatória de cláusulas contratuais abusivas ou ilegais:

> Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:
> [...]
> § 4° É facultado a qualquer consumidor ou entidade que o represente requerer ao Ministério Público que ajuíze a competente ação para ser declarada a nulidade de cláusula contratual que contrarie o disposto neste código ou de qualquer forma não assegure o justo equilíbrio entre direitos e obrigações das partes.

Os direitos dos usuários da internet classificam-se como direitos coletivos, pois pertencem ao conjunto de pessoas que usam a internet. Segundo o art. 81, inciso

II, da Lei nº 8.078/1990 (CDC), são interesses ou direitos coletivos os "transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base". A vastidão e a quantidade de usuários da internet, milhões em todo o Brasil, comprovam a natureza coletiva desse direito. Por exemplo, se os Termos de Uso e Privacidade de determinado aplicativo violar a privacidade de seus usuários, a pretensão de pedir que o Poder Judiciário declare a nulidade dessa cláusula se enquadra como defesa de direito coletivo, pois os usuários do aplicativo constituem grupo de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base, podendo a ação coletiva ser proposta pelo MPF.

A internet tem uma inegável finalidade social, estando diretamente relacionada ao pleno exercício da cidadania, como dispõe a Lei nº 12.965/2014:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I – o reconhecimento da escala mundial da rede;
> II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III – a pluralidade e a diversidade;
> IV – a abertura e a colaboração;
> V – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI – a finalidade social da rede.

Se o próprio Marco Civil da Internet reconhece a finalidade social da rede, não se pode negar a legitimidade do MPF em defesa dos usuários da internet, quer se considere tais direitos de natureza coletiva, quer como direitos individuais homogêneos com relevância social.[69]

69 Nesse sentido: "seja para a defesa de interesses difusos, ou coletivos *stricto sensu* ou, ainda, de interesses individuais homogêneos, detém a Instituição ministerial legitimidade ativa para propor a respectiva ação coletiva. Não há gradação valorativa entre os diversos tipos de interesses supraindividuais tutelados pelo Código, a justificar qualquer distinção quanto a sua legitimação para agir. Pode haver, sim, diferentes níveis de danosidade, efetiva ou potencial, a partir de uma mesma realidade supraindividual. Mas, desde que se trate de lesão a algum, a vários, ou a todos os tipos de interesses transindividuais, cuja tutela se reveste de relevância social, porquanto intrinsecamente vulneráveis e carecedores de organização representativa, configurados estarão o interesse de agir e a legitimidade ad causam do Ministério Público." (MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. **Comentários ao código de defesa do consumidor**. 3. ed. São Paulo: RT, 2010, p. 1321).

4.6 Competência da Justiça Federal

A Política Nacional de Proteção e Defesa do Consumidor é desempenhada pelo Ministério da Justiça por meio da Secretaria Nacional de Defesa do Consumidor (Senacon). Dessa forma, diante do descumprimento de normas de proteção aos usuários da internet, às quais se aplica o direito do consumidor, em escala nacional, compete à Senacon adotar providências para apurar e punir a empresa responsável, na forma do art. 18 do Decreto nº 8.771/16, transcrito a seguir: "Art. 18. A Secretaria Nacional do Consumidor atuará na fiscalização e na apuração de infrações, nos termos da Lei nº 8.078, de 11 de setembro de 1990."

O interesse direto de órgão fiscalizador federal, com a Senacon, faz a Justiça Federal competente para o julgamento de eventual ação coletiva demanda, conforme jurisprudência do STJ:

> PROCESSUAL CIVIL. ADMINISTRATIVO. AÇÃO CIVIL PÚBLICA. DEMANDA COLETIVA. DIREITO DO CONSUMIDOR. SERVIÇO DE TELEFONIA MÓVEL. PARTICIPAÇÃO DA ANATEL. COMPETÊNCIA DA JUSTIÇA FEDERAL. OAB/PE E ADECCON/PE. PRELIMINARES DE ILEGITIMIDADE ATIVA, FALTA DE INTERESSE DE AGIR E IMPOSSIBILIDADE JURÍDICA DO PEDIDO AFASTADAS. QUALIDADE DEFICIENTE DOS SERVIÇOS DE TELEFONIA MÓVEL COMPROVADA POR RELATÓRIO DA ANATEL E OUTROS DOCUMENTOS. DANOS MORAIS COLETIVOS RECONHECIDOS PELO TRIBUNAL DE ORIGEM. PEDIDO PARA QUE O STJ EXAMINE O CUMPRIMENTO DA OBRIGAÇÃO DE FAZER. IMPOSSIBILIDADE. NECESSIDADE DE REEXAME DO CONTEXTO FÁTICO-PROBATÓRIO. SÚMULA 7/STJ.
>
> 1. Na hipótese dos autos, quanto à questão relacionada à competência, *o Superior Tribunal de Justiça possui a orientação no sentido de que a atividade fiscalizatória exercida por entidade reguladora, in casu a Anatel, aliada à legitimidade ad causam do Ministério Público Federal para figurar no polo ativo da demanda, define a competência da Justiça Federal para processamento e julgamento do feito.* (REsp 1.479.316/SE, Rel. Ministro Humberto Martins, Segunda Turma, julgado em 20/8/2015, DJe 1/9/2015).
>
> [...]
>
> 11. Agravo Regimental não provido. (STJ, AgRg no REsp 1502179 / PE, Relator Ministro HERMAN BENJAMIN, SEGUNDA TURMA, DJe 19/12/2016)(grifo nosso)

Dessa forma, havendo violação aos direitos e garantias dos usuários da internet, a Senacon deverá apurar tal infração. Nos casos de omissão da Senacon, terá o MPF competência para demandar à Justiça Federal para proteger esses direitos. Mas mesmo diante da atuação da Senacon, se o MPF reconhecer que ela é insatisfatória, poderá propor ação coletiva para garantir a efetividade dos direitos previstos na Lei nº 12.965/2014.

4.7 A nova Lei Geral de Proteção de Dados Pessoais (LGPDP)

Em 15 de agosto de 2018 foi publicada a Lei nº 13.709/2018, que trata da proteção de dados pessoais no Brasil. Mas até ela entrar em vigor, o que só acontecerá em 16 de agosto 2020 (vinte e quatro meses após a data de sua publicação na forma do seu art. 65, II), o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet (MCI) continuarão a ser as principais normas disponíveis para aqueles que tiverem seus dados pessoais violados.

Quando começar a valer, a LGPDP revogará as normas do MCI que protegem os dados dos usuários da internet, presentes principalmente no art. 7º, incisos VII, VIII, IX e X?

Acreditamos que não.

Não houve revogação expressa, pela LGPDP, dos artigos do MCI que protegem os dados dos usuários da internet. Pelo contrário. O art. 60 da nova lei, reconhecendo indiretamente a permanência das normas do MCI, alterou a redação do art. 7º, inciso X, para incluir uma referência expressa à LGPDP:

> Art. 7° *Omissis.*
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei *e na que dispõe sobre a proteção de dados pessoais.* (em destaque a parte acrescentada pela LGPDP)

Embora a Lei nº 13.709/2018 se aplique inclusive nos meios digitais, segundo dispõe seu art. 1º,[70] o MCI é uma lei especial, que trata exclusivamente da internet,

70 Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pes-

enquanto a LGPDP é uma lei geral. Aplica-se, então, a regra do art. 2º, § 2º, da Lei de Introdução ao Direito Brasileiro, que diz: "A lei nova que estabelecer disposições gerais ou especiais a par das existentes não revoga nem modifica a anterior".

De qualquer modo, a LGPDP aplicar-se-á também às relações havidas na internet, suprindo omissões e incompletudes do MCI, para uma melhor proteção do usuário. A LGPDP trouxe novos conceitos de grande relevância no ambiente digital, tais como dado pessoal sensível[71], anonimização[72], além de explicar o que deve ser entendido por consentimento[73].

"Foi ainda reconhecido o direito de petição à Autoridade Nacional, conforme o art. 18, § 1º, da LGPDP: "O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional."

Isso não impede a atuação conjunta de órgãos de defesa do consumidor, nos termos do § 8º do mesmo artigo, segundo o qual: "O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor."

A aplicação das sanções previstas na LGPDP compete, contudo, somente à Autoridade Nacional de Proteção de Dados pessoais, na forma do art. 55-K, abaixo:

> Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública. (Incluído pela Lei nº 13.853, de 2019)
>
> Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação. (Incluído pela Lei nº 13.853, de 2019)

soa 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.

71 Art. 5º Para os fins desta Lei, considera-se:
II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

72 XI – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

73 XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Será possível uma atuação articulada entre os órgãos com competência sancionatória que envolvem proteção de dados, a exemplo da Senacon, em nível federal, e os Procons, em nível estadual.

Por fim, é possível a atuação de organismos privados, como o Instituto Brasileiro de Defesa do Consumidor (Idec), que tem legitimidade para defender em juízo os direitos dos consumidores.

Segue quadro comparativo entre o Marco Civil da Internet e a LGPDP:

Quadro comparativo sobre proteção de dados pessoais no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais

Marco Civil da Internet	Lei Geral de Proteção de Dados Pessoais
Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.	Art. 3º Esta Lei aplica-se 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, desde que: I – a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019) III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do *caput* do art. 4º desta Lei.

Quadro comparativo sobre proteção de dados pessoais no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais

Marco Civil da Internet	Lei Geral de Proteção de Dados Pessoais
Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; [...] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei. § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. [...] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

Quadro comparativo sobre proteção de dados pessoais no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais

Marco Civil da Internet	Lei Geral de Proteção de Dados Pessoais
Art. 7º *Omissis.* VIII –informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;	Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I – finalidade específica do tratamento; II – forma e duração do tratamento, observados os segredos comercial e industrial; III – identificação do controlador; IV – informações de contato do controlador; V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI – responsabilidades dos agentes que realizarão o tratamento; e VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações. § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Quadro comparativo sobre proteção de dados pessoais no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais

Marco Civil da Internet	Lei Geral de Proteção de Dados Pessoais
Art. 7º *Omissis.* VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;	Art. 7º *Omissis.* § 5º O controlador que obteve o consentimento referido no inciso I do *caput* deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. Art. 11. *Omissis.* [...] § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências. § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (Redação dada pela Lei nº 13.853, de 2019) I - a portabilidade de dados quando solicitada pelo titular; ou (Incluído pela Lei nº 13.853, de 2019) II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo. (Incluído pela Lei nº 13.853, de 2019)

Quadro comparativo sobre proteção de dados pessoais no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais

Marco Civil da Internet	Lei Geral de Proteção de Dados Pessoais
Art. 7º *Omissis.* [...] X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;	Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II – fim do período de tratamento; III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Quadro comparativo sobre proteção de dados pessoais no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais

Marco Civil da Internet	Lei Geral de Proteção de Dados Pessoais
Art. 7º *Omissis.* VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;	Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I – confirmação da existência de tratamento; II – acesso aos dados; III – correção de dados incompletos, inexatos ou desatualizados; IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

5 A PROTEÇÃO DE DADOS PESSOAIS NAS ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO DE INFRAÇÕES PENAIS

Alexandre Assunção e Silva

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais, que entrará em vigor em agosto de 2020, estabelece diversas regras que visam proteger a privacidade, o desenvolvimento da personalidade e outros direitos fundamentais dos indivíduos cujos dados pessoais sejam objeto de tratamento.

Tratamento de dados, segundo a própria Lei nº 13.709/2018, 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.

Embora abranja qualquer manipulação de dados realizada por pessoas físicas e jurídicas, de direito público ou privado, o art. 4º, III, da Lei nº 13.709/2018 exclui do seu âmbito de aplicação algumas atividades, entre as quais as de investigação e repressão de delitos, senão vejamos:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> [...]
> III – realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou

Todavia, ainda que a LGPDP pareça retirar, num primeiro momento, tais operações de tratamento do seu campo de proteção, a própria LGPDP traz dispositivos que visam assegurar alguns direitos àqueles que tiverem seus dados pessoais manipulados para fins de repressão penal. O § 1º do art. 4º é o primeiro deles. Diz o seguinte:

> Art. 4º *Omissis*.
> § 1º 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, a LGPDP exige que a legislação específica que regule o tratamento de dados para fins de investigação e repressão de delitos preveja medidas proporcionais e estritamente necessárias para atender o interesse público, devendo ser obedecidos os princípios gerais de proteção e os direitos do titular previstos na LGPDP.

Uma das normas que regula a manipulação de dados possíveis de serem utilizados na investigação e repressão de infrações penais é a Lei nº 12.965/2014, o Marco Civil da Internet que em seu art. 13 determina que sejam armazenados os dados de conexão à internet de todos os usuários no país, pelo prazo de 1 (ano). Esses dados podem identificar a autoria de crimes praticados pela Web. Com igual propósito, o art. 15 do Marco Civil da Internet determina que sejam guardados os registros de acesso a aplicações da internet, pelo prazo de 6 (seis) meses.

Outra situação na qual os órgãos de repressão penal guardam e processam dados pessoais é a prevista na Lei nº 12.037/2009, que criou o banco de dados de perfis genéticos para auxiliar na descoberta de infrações penais. Dispõe o art. 5º-A:

> Art. 5º-A. Os dados relacionados à coleta do perfil genético deverão ser armazenados em banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia criminal.
> § 1º As informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos.
> § 2º Os dados constantes dos bancos de dados de perfis genéticos terão caráter sigiloso, respondendo civil, penal e administrativamente

> aquele que permitir ou promover sua utilização para fins diversos dos previstos nesta Lei ou em decisão judicial.
> § 3º As informações obtidas a partir da coincidência de perfis genéticos deverão ser consignadas em laudo pericial firmado por perito oficial devidamente habilitado.

Esses bancos de dados precisarão respeitar os princípios gerais de proteção e os direitos do titular previstos na LGPDP. Os referidos princípios encontram-se arrolados no art. 6º.[74]

Como decorrência da aplicação desses princípios, as polícias devem garantir, por exemplo, livre acesso e consulta sobre a forma e a duração do tratamento de dados, bem como sobre quais dados estão sendo manipulados (art. 6º, IV).

Ademais, ainda serão observados os direitos do titular previstos na LGPDP. Estes estão localizados no capítulo III da Lei nº 13.709/2018, que correspondem aos arts. 17 a 22.[75] Essa gama de direitos favorecerá bastante quem tiver seus dados

74 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

75 Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.
Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I – confirmação da existência de tratamento;
II – acesso aos dados;
III – correção de dados incompletos, inexatos ou desatualizados;
IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)
VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

pessoais utilizados numa investigação criminal.

Uma das principais características do tratamento realizado para fins de investigação penal é a desnecessidade de consentimento. O investigado, obviamente, não precisa concordar que seus dados sejam coletados, armazenados ou processados, sob pena de inviabilizar a investigação. Isso decorre do próprio sistema de proteção de dados instituído pela LGPDP, ao não prever o consentimento para "o cumprimento de obrigação legal ou regulatória pelo controlador" (art. 7º, II).

Contudo, o suspeito de um crime pode acessar os dados (art. 18, II) e solicitar a

VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I – comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento. (Redação dada pela Lei nº 13.853, de 2019)
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do *caput* deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.
Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
I – em formato simplificado, imediatamente; ou
II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.
§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.
§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:
I – por meio eletrônico, seguro e idôneo para esse fim; ou
II – sob forma impressa.
§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.
§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do *caput* deste artigo para os setores específicos.
Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
Art. 22. 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.

correção de informações incompletas, inexatas ou desatualizadas (art. 18, III), o que em nada prejudica, e até ajuda, na elucidação do delito. Dados anonimizados igualmente podem ser acessados pelo titular, como os armazenados pelos provedores de conexão à internet (administradores de sistema autônomo) e provedores de aplicativos de internet.

Outro dispositivo da LGPDP que se aplica às investigações criminais é o § 2º do art. 4º:

> § 2º É vedado o tratamento dos dados a que se refere o inciso III do *caput* deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

A vedação imposta acima não traz maiores complicações para a atividade de investigação e repressão de infrações penais, pois ainda que a guarda de dados determinada pelo caso do Marco Civil da Internet seja realizada por pessoa jurídica de direito privado (provedor de conexão ou aplicativo), tal procedimento encontra-se sob fiscalização do Poder Público. Quanto ao Banco Nacional de Perfis Genéticos, ele foi instituído na unidade de perícia oficial do Ministério da Justiça e é administrado por perito criminal federal habilitado, designado pelo ministro de Estado da Justiça. Em seguida, continua o § 3º do art. 4º da LGPDP:

> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

A Autoridade Nacional poderá fiscalizar os bancos de dados utilizados para investigação de delitos, emitindo recomendações para uma melhor proteção aos dados pessoais dos acusados. O § 4º do art. 4º, por fim, diz o seguinte:

> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do *caput* deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público. (Redação dada pela Lei nº 13.853, de 2019)

Essa norma, de aplicação necessária ao tratamento de dados realizado para apurar infrações penais, poderá entrar em conflito com a Lei nº 12.965/2014.

O armazenamento dos dados de conexão à internet e dos registros de acesso a aplicações da internet é feito por pessoas jurídicas de direito privado (empresas fornecedoras de conexão e aplicativos). Todos os dados de conexão ficam guardados nessas empresas (ou em "nuvens"), disponíveis para uso das autoridades que atuam na repressão penal, via requisição do Poder Judiciário, por meio do procedimento previsto no art. 22 da Lei nº 12.965/2014.

A existência de oposição entre o Marco Civil da Internet e a LGPDP dependerá do que se entende por "totalidade dos dados pessoais". Se o objetivo da LGPDP é impedir que uma mesma pessoa jurídica guarde os dados e depois venha a recuperá-los, não haverá desavença, pois a recuperação dos dados anonimizados e posterior uso dar-se-á pela Polícia e pelo Ministério Público. Os dados não serão tratados em sua totalidade por pessoa jurídica de direito privado, mas parte por ela (armazenamento) e parte pelo Poder Público (processamento e avaliação).

Porém, se a LGPDP tem por finalidade evitar que qualquer fase do tratamento, mesmo o armazenamento, seja totalmente de responsabilidade de empresa privada, então haverá um claro choque entre o que determinam os arts. 13 e 15 do Marco Civil da Internet e o § 4º do art. 4º da LGPDP.

A exceção trazida pela nova redação do § 4º dada pela lei n. 13.853/2019, autorizando a empresa privada a tratar os dados de forma integral desde que seu capital seja integralmente constituído pelo Poder Público, pouco altera a situação, vez que os dados de conexão à internet são armazenados por pessoas jurídicas formadas com capital privado (administradores do sistema autônomo e provedores de aplicação da internet), e não por empresas públicas. A Autoridade Nacional de Proteção de Dados Pessoais, poderá solucionar tal questão por meio do uso da competência prevista no § 3º acima mencionado.

REFERÊNCIAS

BALL, James; SCHNEIER, Bruce. Explaining the latest NSA revelations – Q&A with internet privacy experts. **The Guardian**, Sept. 2013. Disponível em: https://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat.

BELLEIL, Arnaud. **@-privacidade.** O mercado de dados pessoais: protecção da vida privada na idade da internet. Lisboa: Instituto Piaget, 2001.

BENDA, Ernst. Dignidad Humana y Derechos de la Personalidad. *In*: BENDA, Ernst; MAIHOFER, Werner; VOGEL, H; HESSE, Konrad; HEYDE, Wolfgang. **Manual de derecho constitucional**. Madrid: Marcial Pons, 2001.

_____. Dignidad Humana y Derechos de la Personalidad. *In*: BENDA, Ernst; MAIHOFER, Werner; VOGEL, H; HESSE, Konrad; HEYDE, Wolfgang. **Manual de derecho constitucional**. Madrid: Marcial Pons, 2001.

BOBBIO, Norberto. **O futuro da democracia**. São Paulo: Paz e Terra, 2004.

BRASIL. Decreto-Lei nº 2.848/1940, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**: Seção 1, Rio de Janeiro, 1940, p. 23911, 31 dez. 1940.

_____. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Promulgada em 5 de outubro de 1988.

_____. **Lei nº 9.507/1997, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.

_____. **Lei nº 9.784/1999, de 29 de janeiro de 1999**. Regula o processo administrativo no âmbito da Administração Pública Federal.

_____. **Decreto nº 6.425/2008, de 4 de abril de 2008**. Dispõe sobre o Censo Anual da Educação.

_____. **Lei nº 11.977/2009, de 7 de julho de 2009**. Dispõe sobre o Programa Minha Casa, Minha Vida – PMCMV e a regularização fundiária de assentamentos localizados em áreas urbanas; altera o Decreto-Lei no 3.365, de 21 de junho de 1941, as Leis nos 4.380, de 21 de agosto de 1964, 6.015, de 31 de dezembro de 1973, 8.036, de 11 de maio de 1990, e 10.257, de 10 de julho de 2001, e a Medida Provisória no 2.197-43, de 24 de agosto de 2001; e dá outras providências.

_____. **Lei nº 12.527/2011, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

_____. **Decreto nº 8.771/2016, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

_____. **Decreto nº 8.764/2016, de 10 de maio de 2016**. Institui o Sistema Nacional de Gestão de Informações Territoriais e regulamenta o disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009.

_____. **Decreto nº 8.789/2016, de 29 de junho de 2016**. Dispõe sobre o Compartilhamento de Bases de Dados na Administração Pública Federal.

_____. **Lei nº 13.444/2017, de 11 de maio de 2017**. Dispõe sobre a Identificação Civil Nacional (ICN).

_____. **Decreto nº 9.278/2018, de 5 de fevereiro de 2018**. Regulamenta a Lei nº 7.116, de 29 de agosto de 1983, que assegura validade nacional às Carteiras de Identidade e regula sua expedição.

_____. **Lei nº 13.709/2018, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

BRASIL. Ministério da Economia. Secretaria de Trabalho. **Ministério publica Cadastro de Empregadores que tenham submetido trabalhadores a condições análogas às de escravo**. Disponível em: http://trabalho.gov.br/component/content/article?id=4428.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. **Resolução nº 2, de 24 de março de 2017**. Aprova os Termos de Uso do Portal Brasileiro de Dados Abertos. Disponível em: http://wiki.dados.gov.br/GetFile.aspx?File=%2fComiteGestor%2fResolu%c3%a7%c3%b5es%2fresolucao-cginda-2-24-3-2017%2cpdf.pdf .

BRASIL. Superior Tribunal de Justiça. Súmula nº 17. Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, e por este absorvido. **Diário de Justiça**: seção três, Brasília, DF, 28 nov. 1990.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.526, de 26 de setembro de 2017**. Dispõe sobre a formação e a operacionalização da base de dados da identificação civil nacional (icn), prevista na Lei nº 13.444/2017.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles havested for Cambridge Analytica in major data breach. **The Guardian**, Mar. 2019. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

CASTELLS, Manuel. **El Poder de la Identidad**. Barcelona: Alianza Editorial, 1997. (La era de la información: economía, sociedad y cultura, v. II).

_____. **A Sociedade Em Rede**. São Paulo: Paz e Terra, 2007. (A Era da Informação: Economia, Sociedade e Cultura, v. 1).

CONDE ORTIZ, Concepción. **La protección de datos personales**: un derecho autónomo con base en los conceptos de intimidad y privacidad. Madrid: Dykinson, 2005.

DE LA CUEVA, Pablo Lucas Murillo. **El derecho a la autodeterminación informativa**: la protección de los datos personales frente al uso de la informática. Madrid: Tecnos, 1990.

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

EAVES.CA. The Three Laws of Open Government Data. Disponível em: https://eaves.ca/2009/09/30/three-law-of-open-government-data/.

EUROPEAN COMISSION. **2018 reform of EU data protection rules**. Disponível em: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

FERREIRA, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor** – Linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

FERREIRA DA SILVA, Carlos Bruno. **Proteção de Dados e Cooperação Transnacional**: Teoria e Prática na Alemanha, Espanha e Brasil. Belo Horizonte: Arraes Editores, 2014.

FOUCAULT, Michel. **Vigiar e punir**: história da violencia nas prisoes. Petrópolis: Vozes, 2004.

FROOMKIN, A. Michael. The Death of Privacy?. **Stan. L. Rev.**, v. 52, p. 1461-1543, may 2000.

GARCÍA-BERRIO HERNÁNDEZ, Teresa. **Informática y libertades**: la protección de datos personales y su regulación en Francia y España. Murcia: Servicio de Publicaciones de la Universidad de Murcia, 2003.

GRIMMELMANN, James. Saving Facebook. **Iowa Law Review**, v. 94, p. 1137-1206, 2009.

HASSEMER. **Proteção de Dados**. Palestra proferida na Faculdade de Direito da UFRGS, 22 nov. 1993.

HOMEM é preso por engano no DF por crime que irmão cometeu. **G1**, 5 dez. 2017. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/homem-e-preso-por-engano-no-df-por-crime-que-irmao-cometeu.ghtml.

HOFFMANN-RIEM, Wolfgang (Hrsg.). **Verwaltungsrecht in der Informationsgesellschaft**. Baden-Baden: Nomos-Verl.-Ges., 2000.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman v.; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. 3. ed. São Paulo: RT, 2010.

MINISTÉRIO PÚBLICO FEDERAL. Procuradoria Federal dos Direitos do Cidadão. **MPF assina termo de cooperação técnica para dar mais transparência a dados de Educação**. Disponível em: http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2015/dezembro/mpf-assina-termo-de-cooperacao-tecnica-para-dar-mais-transparencia-a-dados-da-educacao/.

_____. **PFDC se reúne com equipe do FNDE para acompanhar ações pactuadas em Termo de Cooperação Técnica em 2015**. 5 maio 2017. Disponível em: http://pfdc.pgr.mpf.mp.br/informativos/edicoes-2017/maio/050517-2/.

MPF se aproxima da Eurojust em reunião interinstitucional. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/mpf-se-aproxima-da-eurojust-em-reuniao-interinstitucional.

PÉREZ LUÑO, Antonio E. Informática y libertad. Comentario al artículo 18.4 de la Constitución. **Revista de Estudios Políticos**, n. 24, p. 31-53, nov. 1981.

_____. **Derechos humanos, estado de derecho y constitución**. Madrid: Tecnos, 2005.

PETERSEN, Stefanie. **Grenzen des Verrechtlichungsgebotes im Datenschutz**. Münster; Hamburg [u.a.]: Lit, 2000.

REVISTA IDIGITAL, ano 6, n. 20, p. 64/65. Disponível em https://issuu.com/infoliocom/docs/rev20. Acesso em: 4 ago. 2017.

RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**. Rio de Janeiro: Editora Renovar, 2008.

SANCIONADA com vetos lei geral de proteção de dados pessoais. **Senado Notícias**, 15 ago. 2018. Disponível em: https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais.

SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO. **Instrução Normativa nº 4, de 12 de abril de 2012**. Institui a Infraestrutura Nacional de Dados Abertos – INDA. Disponível em: https://www.governoeletronico.gov.br/documentos-e-arquivos/3%20-%20IN%2004%2013-04-12.pdf.

SEMINÁRIO INTERNACIONAL BRASIL 100% DIGITAL: INTEGRAÇÃO E TRANSPARÊNCIA A SERVIÇO DA SOCIEDADE. Disponível em: http://www.brasildigital.gov.br/dados-abertos-e-controle-social.htm.

TÉLLEZ AGUILERA, Abel. **Nuevas tecnologías, intimidad y protección de datos**: con estudio sistemático de la Ley Orgánica 15-1999. Madrid: Edisofer, 2001.

TINNEFELD, Marie-Theres; EHMANN, Eugen; GERLING, Rainer W. **Einführung in das Datenschutzrecht**: Datenschutz und Informationsfreiheit in europäischer Sicht. München; Wien: Oldenbourg, 2005.

TUROLLO JR., Reynaldo. Repórter tira carteira de identidade em 9 estados. **Folha de S.Paulo**, 13 out. 2013. Disponível em: https://www1.folha.uol.com.br/cotidiano/2013/10/1355762-reporter-tira-carteira-de-identidade-em-9-estados.shtml.

TROPER, Michel. **A filosofia do direito**. São Paulo: Martins Editora, 2008.

VÁZQUEZ, Javier Barnes. Sobre el procedimiento administrativo: evolución y perspectivas. *In*: _____ (coord.). **Innovación y reforma en el derecho administrativo**. Sevilla: Derecho Global, 2006.

MPF

Ministério Público Federal