Lei de proteÃ§Ã£o de dados e a identificaÃ§Ã£o nacional: hÃ¡ antinomias?

A disciplina jurídica dos dados pessoais assenta-se numa tensão entre a garantia da autodeterminação informativa (privacidade/controle) e o reconhecimento da necessidade do tratamento desses dados pelo poder público, especialmente em matéria de segurança e ordem públicas, e também pelo setor privado, face à importância da circulação de dados no mercado.[1]

Claramente inspirada pela regulação europeia relativa aos dados pessoais, a Lei 13.709/2018, que regula a proteção de dados pessoais em âmbito nacional, aspira a conciliação entre a proteção da pessoa, o interesse público e o incentivo ao desenvolvimento econômico e tecnológico, vinculados, em nossas sociedades, à circulação e ao uso da informação.[2]

Antes da promulgação dessa lei, em 14 de agosto último, a tutela desses dados tinha por fundamento normativo o direito à vida privada e à intimidade, consagrados no artigo 5º, X da Constituição e no artigo 21 do Código Civil. A preocupação com essa questão também já se anunciava no Marco Civil da Internet (Lei 12.965/2014), visto que é com as tecnologias da informação que o tratamento de dados pessoais adquire seu alcance atual.[3]

Apesar da aprovação tardia da legislação de proteção de dados pessoais no Brasil, sua utilização é massiva tanto pelo Estado como nas atividades privadas. Um exemplo disso, no setor público, é o recadastramento biométrico, iniciado pelo Tribunal Superior Eleitoral (TSE), já em 2008.[4] Esse trabalho de coleta de dados biométricos dos cidadãos brasileiros expandiu-se, de forma significativa na última década, e inclui a coleta de dados biométricos para renovação de passaporte e da Carteira Nacional de Habilitação.[5]

No ano passado, foi aprovada a Lei 13.444/2017, que dispõe sobre Identificação Civil Nacional (ICN). Essa lei representa um desdobramento importante do projeto iniciado pelo TSE, para fins de identificação dos eleitores brasileiros. Ela pretende não apenas identificar toda a população brasileira com base na biometria, mas também, integrar as bases de dados já existentes para as mais diversas finalidades.

Cumpre, entretanto, indagar sobre a compatibilidade entre esse ambicioso projeto da Identificação Civil Nacional e a proteção de dados pessoais, regulada pela Lei 13.709/2018.

A Lei Geral de Proteção de Dados (LGPD) estabelece como fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o direito ao livre desenvolvimento da personalidade, o desenvolvimento econômico e tecnológico, a livre iniciativa, a livre concorrência e a defesa do consumidor (artigo 2º da Lei 13.709/2018).

Esses fundamentos vêm refletidos nos princípios que regem o tratamento de dados pessoais: princípio da finalidade, da adequação, da necessidade, do livre acesso aos dados por parte dos titulares, da qualidade dos dados, da transparência e da não discriminação (artigo 6º da Lei 13.709/2018). [6]

Assim como na regulação europeia, a lei brasileira protege especialmente os chamados “dados sensíveis” (artigo 5º, II), que revelam informações com risco significativo para privacidade ou que podem dar base para eventual discriminação, dentre os quais os dados biométricos.

A regra para esses dados é a da proibição do tratamento (artigo 11, *caput*), excetuadas as hipóteses expressas em lei: “consentimento específico e em destaque, pelo titular, para finalidades específicas” (artigo 11, I); quando seu tratamento for indispensável para cumprir obrigação legal do controlador dos dados, ou para execução de políticas públicas, realização de estudos e pesquisas, o exercício regular de um direito, proteção da vida ou da incolumidade física do titular dos dados, ou de sua saúde e a segurança (artigo 11, II).

A LGPD é aplicável ao tratamento de dados tanto por pessoas jurídicas de direito público como de direito privado. Assim, o regime geral da tutela dos dados pessoais incide sobre a regulação da Identidade Civil Nacional.

Deve-se destacar, no entanto, que a LGPD excetua de seu campo de incidência o tratamento de dados, por pessoa jurídica de direito público, “… realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais”, cuja proteção deverá ser objeto de lei específica (artigo 4º).

Em suma, os dados armazenados na base da ICN estão protegidos pela LGPD. Em princípio, a dispensa do consentimento para coleta, armazenamento e uso desses dados está baseada no artigo 11, II da LGPD, que autoriza o tratamento de dados pelo poder público para execução de políticas públicas e prestação de serviços públicos. Ao lado dessas hipóteses, a previsão da lei da ICN quanto ao uso dos dados para o fim de persecução criminal, poderia encontrar guarida no artigo 4º da LGPD.

Entretanto, ao examinarmos a forma como foi regulada a utilização e compartilhamento dos dados biométricos coletados pelo TSE, e os que serão coletados para fins de identificação civil, emerge, mais claramente, a questão de sua compatibilidade com a tutela jurídica de dados pessoais e o direito à privacidade, bem como com as garantias constitucionais típicas de um Estado de Direito.[7]

A previsão de um regime mais brando para a proteção de dados pessoais em matéria de segurança pública e nacional é elemento comum da regulação, também, no plano internacional.[8] Do mesmo modo, a execução de políticas públicas e serviços públicos ou o interesse público constituem hipóteses, de um modo geral, de dispensa de consentimento para tratamento de dados pessoais.[9] Isso não significa, porém, uma licença para um uso amplo e compartilhamento indiscriminado entre órgãos públicos.

Na LGPD, veda-se o compartilhamento de dados sensíveis, com exceção de "… dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos." (artigo 11, II, "b"). O artigo 23 da lei, por sua vez, estabelece os parâmetros para o tratamento de dados pessoais pelo poder público: deve ser realizado para uma finalidade pública, norteada pelo interesse público, e com o objetivo de executar suas competências legais ou atribuições legais do serviço público.

Não há, portanto, uma autorização para o compartilhamento generalizado de dados pessoais, muito menos os sensíveis, como os biométricos. Ainda assim, é de notar que a vinculação ao "interesse público" e a finalidade de "execução de políticas e serviços públicos" dá margem a uma interpretação extensiva que permitiria o compartilhamento dos dados em nome da "eficiência da administração pública" e da "segurança pública".

Outro ponto importante a ser destacado é ao dever do ente público responsável pelo tratamento de dados, mesmo nos casos de dispensa do consentimento, de respeito aos direitos dos titulares de dados e aos princípios da LGPD (artigo 18). Dentre esses princípios, interessam, especialmente, para este debate, o da finalidade e o da adequação, que exigem que o compartilhamento dos dados da ICN, pelo TSE, passe por um controle de compatibilidade com as finalidades admitidas em lei (artigo 6º, I e II da Lei 13.709/2018).

Por fim, a questão mais delicada a ser enfrentada diz respeito ao compartilhamento dos dados pessoais sensíveis, inclusive os biométricos, com as polícias Federal e Civil, para fins de investigação criminal. Nos termos da lei que cria a base de dados da ICN, utilizando-se dos dados biométricos do cadastro eleitoral, está prevista a plena integração dessa base com as bases de dados de identificação criminal (artigo 3º).

Com isso, franqueia-se aos órgãos de segurança pública acesso irrestrito aos dados pessoais, dentre eles os biométricos, coletados, de toda a população, para fins de identificação civil.

A pretensão de que essa base de dados alcance toda a população é explícita, como se vê da portaria do Ministério da Saúde, publicada em fevereiro de 2018, que determina a identificação palmar de todos os recém-nascidos brasileiros, juntamente com a identificação biométrica de sua mãe, de forma obrigatória (Portaria 248/2018).

O compartilhamento integral das bases de dados de identificação civil para fins de persecução penal amplia, de forma preocupante, a possibilidade de coleta e armazenamento de dados pessoais dos cidadãos, pelo Poder Público, com fundamento na segurança pública.

Por força do artigo 5º, LVIII da Constituição Federal, a identificação criminal, mediante registro fotográfico e recolha de dados datiloscópicos, só é permitida nas hipóteses previstas em lei, especialmente, em caso de ausência ou imprecisão da identificação civil e da necessidade justificada, e autorizada por decisão judicial fundamentada (Lei 12.037/2009).

A Lei 12.654/2012, que criou a base de perfis genéticos para fins de investigação criminal, restringe, por sua vez, a inclusão compulsória desses dados apenas a pessoas condenadas pela prática de crimes hediondos ou dolosos e violentos contra a pessoa (artigo 9º-A). Ademais, essas informações estão protegidas pelo sigilo e pelo dever de observância do princípio da finalidade (artigo 5º-A).

Com a lei que cria a base de dados da ICN, ao contrário, há uma previsão de compartilhamento indiscriminado entre a identificação civil, especialmente a partir de dados biométricos, e as bases de dados destinadas à persecução criminal.

Embora a relativização do direito à proteção de dados em matéria de segurança pública também esteja presente no regulamento europeu, percebe-se uma maior preocupação em definir os limites do tratamento de dados pessoais pelo Poder Público. A legitimidade desse tratamento está condicionada à existência de previsões legais, no âmbito do direito interno de cada Estado-membro, e "que constituam uma medida necessária e proporcionada numa sociedade democrática" (artigo 23), para salvaguardar os objetivos referidos no artigo 23º, 1, dentre os quais "a segurança do Estado e a segurança pública".

No Brasil, entretanto, a significativa ampliação das hipóteses de coleta compulsória e utilização não autorizada pelos titulares dos dados, por parte do Poder Público, em nome da segurança pública, foi promovida com base em uma autorização genérica para o acesso a dados coletados para fins de identificação civil.

A legitimidade dessa autorização pode, contudo, ser questionada, especialmente com a promulgação da Lei Geral de Proteção de Dados. Isto porque, a despeito exclusão feita nessa do tratamento de dados em matéria de segurança pública e nacional, os dados coletados e integrados às bases da ICN, foram obtidos para fins de identificação civil e eleitoral. A alteração de sua finalidade para identificação criminal não pode ser justificada, de forma automática, pelo interesse da segurança pública.

A crescente demanda de tratamento de dados pessoais dos cidadãos e estrangeiros na área da segurança pública, perceptível não apenas no Brasil, mas no plano internacional, tem conduzido a uma relativização da proteção dos dados pessoais e da privacidade.[10]

No Brasil, os altos índices de violência e a insegurança generalizada coloca a segurança pública dentre as principais preocupações da população brasileira.[11] Esse cenário, aliado à aposta na tecnologia como vetor inexorável de desenvolvimento, constitui um ambiente favorável ao afrouxamento dos limites à coleta e utilização de dados pessoais pelo poder público.

É preciso, contudo, estar atento aos riscos de autoritarismos e violação não apenas de direitos, em sua dimensão individual (proteção de dados pessoais e privacidade), mas também das garantias inextrincáveis do Estado Democrático de Direito.

Referências bibliográficas

CASTRO. C. S. e. O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro. In: Derecho Constitucional Para El Siglo XXI. Actas Del VIII Congreso Iberoamericano De Derecho Constitucional, vol. 1, 2006, pp. 1639-1662.

_____. **Direito da informática, privacidade e dados pessoais.** Coimbra: Almedina, 2005.

CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção Jurídica de Dados Pessoais: a intimidade sitiada entre o Estado e o Mercado. **Revista da Faculdade de Direito UFPR**, n. 47. Curitiba, 2008, p. 141–153.

DONEDA, D. **A proteção dos dados pessoais como um direito fundamental.** Revista Espaço Jurídico. vol. 12. n. 2. Joaçaba: Unoesc, 2011, pp. 91-108.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

TRIBUNAL SUPERIOR ELEITORAL. **TSE e Polícia Federal vão compartilhar banco de dados biométricos**. Disponível em <http://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos>. Acesso em setembro de 2018.

**Esta coluna é produzida pelos membros e convidados da Rede de Pesquisa de Direito Civil Contemporâneo (USP, Humboldt-Berlim, Coimbra, Lisboa, Porto, Roma II-Tor Vergata, Girona, UFMG, UFPR, UFRGS, UFSC, UFPE, UFF, UFC, UFMT, UFBA, UFRJ e UFAM).*

[1] Cf.: CORRÊA, Adriana Espíndola; GEDIEL, José Antônio Peres. Proteção Jurídica de Dados Pessoais: a intimidade sitiada entre o Estado e o Mercado. *Revista da Faculdade de Direito UFPR*, 47. Curitiba, 2008, p. 141–153.

[2] Cf.: GDPR, considerando 7.

[3] Como explica Danilo Doneda, a proteção de dados pessoais antes da LGPD baseava-se em diplomas legais esparsos, como no CoÌ•digo de Defesa do Consumidor (Lei 8.078/90), a Lei de*Habeas Data* (Lei 9.507/1997), a Lei do Cadastro Positivo (Lei 12.414/2011) e a Lei de acesso à Informação(Lei 12.527/2011). Sobre o tema conferir: DONEDA, D. *A proteção dos dados pessoais como um direito fundamental.* Revista Espaço Jurídico. vol. 12. n. 2. Joaçaba: Unoesc, 2011,p. 103 e ss.

[4] Resolução 22.688/07/TSE.

[5] Resolução 249 de 27/08/2007 do CONTRAN – Conselho Nacional de Trânsito e artigo 20, VI do Decreto 5.978/2006, com a redação dada pelo Decreto 8.374/2014.

[6] Esses princípios foram inspirados na regulação europeia de direito de proteção de dados. Sobre o sentido dos princípios do tratamento de dados, no direito europeu: CASTRO, Catarina Sarmento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005, pp. 229 e ss.

[7] Antes mesmo da promulgação da Lei 13.444/2017, em 2010, já havia sido firmado um Acordo de Cooperação Técnica entre o TSE e o Ministério da Justiça, a fim de permitir a transferência de dados biométricos. Essa parceria foi estabelecida com o objetivo de contribuir com eventuais investigações criminais. Em 2017, novo acordo, agora com fundamento na Lei que havia sido recém-promulgada, foi firmado entre o TSE e a Polícia Federal (*TSE e Polícia Federal vão compartilhar banco de dados biométricos***.** Disponível em <http://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos >. Acesso em setembro de 2018).

[8] O GDPR, assim como já previsto na Diretiva anterior, autoriza os Estados-membros limitarem o alcance dos direitos e obrigações desse regulamento, tanto para a garantia da segurança pública como para defesa nacional Na América Latina, podemos mencionar a Lei 25.326/2000, que dispõe sobre a proteção dados na Argentina e a *Ley Federal de Protección de datos personales en posesión de los particulares* do México; ambas estabelecem exceções à proteção de dados pessoais nessas matérias.

[9] Idem

[10] CASTRO. C. S. e. O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de setembro. In: *Derecho Constitucional Para El Siglo XXI*. Actas Del VIII Congreso Iberoamericano De Derecho Constitucional, vol. 1, 2006, pp. 1639-1662.

[11] Recente pesquisa publicado pela Confederação Nacional da Indústria indica que 38% dos brasileiros aponta a segurança pública como um dos principais problemas do país (CNI. *Retratos da sociedade brasileira*, Ano 7, n.41 – BrasiÌ•lia : CNI, 2018, p. 05. Disponível em: Acesso em: 17.12.2018).