Privacy by design como princípio do direito à proteção de dados

A problemática em torno da privacidade não envolve mais apenas a feição do "direito a ser deixado só", sem sofrer intervenção de terceiros em suas escolhas existenciais, o "*zero-relationship*"[1]. Essa concepção inicial tem sido mitigada pela crescente consciência de que a privacidade, como direito individual fundamental, retrata um aspecto basilar da realização do livre desenvolvimento da personalidade, incutida na ideia de autodeterminação informada.

No universo digital, dados sobre os cidadãos são captados de muitas formas e a todo momento, sendo irrefutável o desequilíbrio de poder entre os controladores do processamento desses dados, que determinam o quê, o como e o porquê os dados pessoais são processados, e os seus titulares, indivíduos cujas informações pessoais estão em jogo.

Inicialmente, a *privacy by design*[2] se revela no postulado que impulsiona a concepção de que a privacidade deve priorizar a organização, o desenvolvimento e o planejamento das instituições democráticas e ser parte dos deveres e obrigações de todas as operações de sociedades empresárias, notadamente as que utilizam inteligência artificial (IA), exigindo que as organizações adotem padrões especiais e medidas técnicas que assegurem que apenas os dados pessoais necessários sejam processados para cada propósito específico.

Contudo, indo além, é preciso perceber que o princípio *privacy by design* deve ser concebido como um princípio jurídico fundante que assegura a concretização do direito fundamental à proteção de dados, conforme demonstrado, de maneira mais aprofundada, em artigo científico anterior publicado pelos autores, intitulado "Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados"[3], produzido no âmbito do Grupo de Pesquisas Institucionais "Novas Tecnologias, Inteligência Artificial, Direito e Democracia", vinculado ao Programa de Pós-graduação Stricto Sensu em Direito da Universidade do Estado do Rio de Janeiro, de modo que a presente coluna se revela uma espécie de resenha da publicação mencionada e dos trabalhos desenvolvidos no âmbito da pesquisa publicada.

Ao investigar sua origem, verifica-se que a privacidade desde a concepção de um sistema computacional não é conceito novo em termos de proteção de dados. É a filosofia proposta academicamente por Ann Cavoukian[4], a Comissária de Informação e Privacidade, nos anos 1990 no Canadá, e reconhecida como a principal criadora do conceito de *privacy by design* (PbD). Diante de sistêmicos desafios tecnológicos, a PbD fornece uma visão holística e uma perspectiva preventiva da proteção de dados.

Sua aplicação atravessa toda a estrutura do negócio, de ponta a ponta, visando atingir uma soma positiva na interação, mutuamente benéfica, entre privacidade e tecnologia e se embasa em sete pilares: (i) um projeto proativo, não reativo, não repressivo e sim preventivo; (ii) a privacidade de dados como configuração-padrão, instituída em sistemas de tecnologia da informação e comunicação (TIC) como paradigma de práticas negociais; (iii) a privacidade incorporada na arquitetura do projeto; (iv) a funcionalidade completa como soma positiva, e não soma-zero, sem haver neutralidade ou opacidade; (v) a segurança e a proteção de todo o ciclo de vida dos dados e do desenvolvimento tecnológico; (vi) garantia de escolha, controle e transparência como ferramentas essenciais à confiança no uso de dados, além de fundamental à *accountability*; (vii) centralização das normas regulatórias em integridade, confidencialidade, disponibilidade e segurança dos dados em benefício de seus titulares.

Embora a privacidade exija que as informações de identificação pessoal sobre os indivíduos sejam protegidas contra o acesso não autorizado, para o qual fortes medidas de segurança são essenciais, faz-se mister reconhecer que a privacidade envolve muito mais que garantir acesso seguro aos dados. Privacidade pressupõe controle, permitindo que os titulares mantenham controle individual sobre as informações de identificação pessoal em relação à coleta, análise, armazenamento, uso, manipulação e divulgação[5].

Apesar da clareza e importância das diretrizes da PbD, a Lei Geral de Proteção de Dados (LGPD) institui, de modo ainda muito tímido, uma perspectiva preventiva de proteção à privacidade de dados *by design*, tanto no inciso VIII do artigo 6º, ao tratar das "medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais", quanto no parágrafo 2º do artigo 46, que versa sobre "as medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução".

No entanto, compreende-se que o princípio da privacidade desde a concepção deve ser levado a sério em toda sua força expansiva e originária, como um importante fundamento para assegurar de modo prático o direito à proteção de dados. Isso porque, não se olvida que muitos são os riscos existentes à privacidade

e à segurança dos dados pessoais.

Com efeito, a inteligência artificial pode ser considerada uma das tecnologias mais disruptivas do século XXI, uma poderosa ferramenta que auxilia na solução de problemas e também cria outros novos. Porém, como outras tendências disruptivas, o direito demora a acompanhar os avanços tecnológicos[6]. A IA é empregada na dimensão algorítmica, com capacidade de processamento massivo de dados e de estabelecer hiperconexões, porém sua linguagem não alcança a consciência hermenêutica, restringindo-se à dimensão lógico-formal das manifestações humanas[7].

Os algoritmos permitem traçar perfis psicográficos – por *profiling* ou perfilização – dos usuários da internet e, por conseguinte, viabilizam mudanças sofisticadas e imperceptíveis do comportamento de consumidores, espectadores e até de eleitores, comprometendo a privacidade e a autonomia na tomada de suas decisões. Tecnologias refinadas de manipulação algorítmica progrediram a ponto de os usuários não identificarem que foram influenciados.

Nesse contexto, é preciso considerar que na Sociedade da Exposição[8], existem diversificadas concepções de privacidade[9] sendo constantemente vilipendiadas por "algoritmos de destruição matemática", termo este cunhado por Cathy O´Neil[10], sendo elas: a) *informational privacy*; b) *decisional privacy*; c) *behavioral privacy*; d) *physical privacy*, o que demanda uma abordagem holística e compreensiva sobre a matéria.

Assim, a mitigação de riscos e a exigência de segurança no tratamento de dados pessoais, reforça a necessária eficácia normativa e a imprescindível efetividade regulatória concreta do princípio *privacy by design*, a qual implica na sua compreensão como princípio normativo implícito, concebido como resultado da projeção hermenêutica do direito fundamental à privacidade e à intimidade (artigo 5º, X, da Constituição) e à inviolabilidade do sigilo de dados (artigo 5º, XII, da Constituição), devendo atuar como fundamento de validade e vetor interpretativo (fechamento de sentido) para as regras e processos que dele se originam e regulamentam seu campo material de aplicação[11].

Uma vez compreendido como norma, o princípio *privacy by design* deve estar na raiz e incidir sobre os sistemas instalados desde sua gênese, bem como sobre toda regulamentação legal e os procedimentos práticos que lhe assegurem efetividade.

Em outras palavras, o princípio PbD deve nortear e validar as inúmeras ações que envolvem otratamento de dados no âmbito das instituições e das corporações, tais como a) celebrar compromissoorganizacional documentado com os padrões mínimos de proteção de dados, incluindo culturacorporativa, práticas comerciais e serviços comerciais; b) nomear um diretor de proteção de dados(DPO), se aplicável, ou contratar um consultor de proteção de dados; c) estabelecer uma estrutura deproteção de dados, com criptografia e pseudonimização; d) criar e documentar um sistema demanutenção de registros para o processamento de dados; e) formular um sistema de gerenciamento deriscos, incluindo o gerenciamento de *compliance* (artigo 50 da LGPD); f) atualizar o treinamento decontrole de privacidade para os funcionários que lidam com dados pessoais de clientes e funcionários; g)usar mecanismos de autoavaliação e autorregulação para auditar e monitorar a implementação dossistemas mencionados; h) estabelecer medidas de segurança que visem minorar e evitar incidentes eviolações à privacidade de dados.

Assim, além de se observar esse *checklist* inicial e as disposições legais, deve ser considerada a garantia da privacidade a partir do padrão principiológico by design para todo o ciclo de vida do tratamento de dados, em especial nas empresas que utilizam Inteligência Artificial avançada em seus produtos e serviços e compromisso com suas diretrizes de validar as informações (fechamento de sentido) para as regras que dele se originam.

Isso porque os algoritmos representam graves perigos a princípios constitucionais anteriores ao advento da IA, como privacidade, autonomia, igualdade, devido processo legal e ao Estado de Direito, haja vista a manipulação oculta e a influência opaca de desejos e preferências de consumidores e eleitores, sendo cada vez mais eficazes com o amplo poder de persuasão obtido a partir da mineração de dados.

A tecnologia persuasiva reforça uma noção originária da área da psicologia: o "reforço intermitente positivo", implementando, de forma inconsciente no usuário, uma reprogramação neurolinguística do humano pela máquina.

Apesar desses perigos, não se verifica um real senso de urgência para enfrentá-los e superá-los, ainda que haja tempo. Para tanto, a incorporação jurídica do *privacy by design* justifica a adoção de salvaguardas da privacidade, de ponta a ponta, nos projetos computacionais desenvolvidos e no tratamento de dados, a fim de que as sociedades empresárias absorvam as diretrizes do PbD em seus valores corporativos e empreguem o discurso pragmaticamente, como diferencial capaz de reforçar sua responsabilidade, desde a concepção do projeto, com ética (*ethics by design*), segurança (*security by design*) e compromisso com sua força jurídico-normativa.

A inclusão do PbD à ordem jurídica brasileira e à agenda de *compliance* para o desenvolvimento de novas tecnologias da informação e das comunicações (TIC), com foco no *technological enforcement*, deve conduzir a proteção proativa de dados a um patamar autoexecutável, em perspectiva preventiva, em que pese os desafios de ordens técnica, informacional, regulatória e mercadológica, que devem ser superados a partir de uma tutela promocional dos direitos da personalidade e das garantias fundamentais[12].

Por todo o exposto, defende-se a concepção do princípio fundante do *privacy by design* como princípio

jurídico-constitucional a partir do qual se deve construir todo o arcabouço regulatório do direito fundamental à proteção de dados, de modo originário, integrado e transparente em todo o processo de arquitetura tecnológica.

[1] RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 81.

[2] O termo privacy, como conceito jurídico moderno, originou-se na sociedade burguesa estadunidense através da obra de dois juristas, no final do século XIX, Samuel Warren e Louis Brandeis, que, atentos aos avanços tecnológicos, teriam sido os pioneiros a tratar do tema em famoso artigo intitulado The Right to Privacy, publicado em 1890 pela Harvard Law Review. (WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. Harvard Law Review, v.4, n.5, 1890, p. 193-220. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warrenbrandeis.pdf. Acesso em: 06.09.2020).

[3] MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. In: Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 2020.

[4] CAVOUKIAN, Ann, CHANLIAU, Marc. Privacy and security by design: a convergence of paradigms. Disponível em: http://www.ipc.on.ca/images/Resources/pbd-convergenceofparadigms.pdf. Acesso em: 16.08.2020.

[5] MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. In: Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 2020.

[6] MANHEIN, Karl M.; KAPLAN, Lyric. Artificial Intelligence: Risks to Privacy and Democracy (October 25, 2018). In: 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper nº. 2018-37. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016. Acesso em: 30 jul. 2020.

[7] MARRAFON, Marco Aurelio. Filosofia da Linguagem e limites da IA na Interpretação Jurídica. In: Revista Consultor Jurídico, 2019. Disponível em: https://www.conjur.com.br/2019-jul-22/constituicao-poder-filosofia-linguagem-limites-ia-interpretacao-juridica. Acesso em: 16 ago. 2019.

[8] RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 41-42.

[9] CASTELLITTO, Anita L. Allen. Understanding privacy: the basics. Disponível em: https://www.law.upenn.edu/cf/faculty/aallen/workingpapers/pli2007.pdf. Acesso em: 16 ago. 2020.

[10] O-NEIL, Cathy. Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia. Trad. por Rafael Abraham. 1ª ed. São Paulo: Ed. Rua do Sabão, 2020.

[11] Sobre o conceito de princípio jurídico em uma leitura hermenêutica no contexto do constitucionalismo contemporâneo, conferir: MARRAFON, Marco Aurélio. Hermenêutica, sistema constitucional e aplicação do direito. 2ª ed. Florianópolis: Emais, 2018. p. 198-206.

[12] MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. In: Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 2020.

Date Created
19/07/2021