COLEÇÃO LGPD EM MOVIMENTO

8 temas chave de implementação: uma visão multissetorial

DataPrivacyBR Research

Observatório

FICHA TÉCNICA

O Data Privacy Brasil é um espaço de intersecção entre a escola Data Privacy Ensino e a Associação Data Privacy Brasil de Pesquisa. Este relatório foi produzido exclusivamente pela Associação Data Privacy Brasil de Pesquisa, entidade civil sem fins lucrativos sediada em São Paulo.
A organização dedica-se à interface entre proteção de dados pessoais, tecnologia e direitos fundamentais, produzindo pesquisas e ações de incidência perante o sistema de Justiça, órgãos legislativos e governo. A partir de uma Política de Financiamento Ético e Transparência, a associação realiza pesquisas de interesse público que buscam reforçar a gramática de direitos fundamentais e ampliar a cultura de proteção de dados pessoais no Brasil e no Sul Global. A Associação integra a Coalizão Direitos na Rede, a Rede-Iberoamericana de Proteção de Dados Pessoais e o Conselho Consultivo da Sociedade Civil da Sociedade da Informação (CSISAC) da Organização para Cooperação e Desenvolvimento Econômico (OCDE). A Associação Data Privacy Brasil de Pesquisa também representa a sociedade civil perante o Conselho Nacional de Proteção de Dados Pessoais da Autoridade Nacional de Proteção de Dados (ANPD).

Para mais informações sobre a organização, impacto de seus projetos e como pesquisas são apoiadas, visite www.dataprivacybr.org.

ORGANIZADORES
Bruno Bioni e Mariana Rielli

AUTORES
Bruno Bioni, Mariana Rielli, Júlia Mendonça, Iasmine Favaro, Thais Aguiar, Pedro Martins.

COMO CITAR
BIONI, Bruno; RIELLI, Mariana (Org). Coleção LGPD em movimento - 8 temas chave de implementação: uma visão multissetorial. Associação Data Privacy Brasil de Pesquisa. 2022.

DIREÇÃO

Bruno Bioni e Rafael Zanatta

COORDENAÇÃO GERAL DE PROJETOS

Mariana Rielli e Marina Meira

LÍDER DE PROJETOS

Johanna Monagreda

ANALISTA DE INCIDÊNCIA

Vinícius Silva

PESQUISADORES

Gabriela Vergili, Hana Mesquita, Helena Secaf, Jaqueline Pigatto, Júlia Mendonça, Marina Garrote, Mikael Servilha, Nathan Paschoalini, Pedro Saliba e Thaís Aguiar

ADMINISTRATIVO E COMUNICAÇÃO

Camila Dias, Erika Jardim, Fabrício Sanchez, Gustavo Reis, Júlio Araújo, Layanne Gayofato, Rafael Guimarães, Roberto Junior, João Paulo Vicente, Victor Scarlato e Willian Oliveira

APOIO

Meta

IMPRENSA

Para esclarecimentos sobre o documento e entrevistas, entrar em contato com a Associação pelo e-mail imprensa@dataprivacybr.org

PREFÁCIO

A aprovação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) em agosto de 2018 após cerca de 10 anos de debates travados em diferentes fóruns e por uma multiplicidade de atores não colocou um ponto final nas discussões - e dúvidas - sobre o tema no Brasil. Muito ao contrário, foi a partir desse marco que a privacidade e a proteção de dados pessoais começaram a galgar ainda mais espaço na agenda pública brasileira, onde hoje têm um lugar indiscutível.

Por um lado, desde agosto de 2018 foi possível observar uma explosão de proposições no legislativo federal sobre o tema, seja com o objetivo de alterar a própria LGPD, ou para dispor sobre privacidade e proteção de dados em outras normas[1]. Por outro, é evidente que os debates sobre a interpretação e a aplicação da própria LGPD, especialmente a partir de sua vigência parcial em setembro de 2020, apenas cresceram e se aprofundaram nesse período.

Além de se tratar de uma lei transversal, com profundos impactos sobre os mais diversos setores, o aspecto geral da LGPD também ajuda a explicar a efervescência de discussões sobre seus significados, interpretações e boas práticas. Por exemplo, há dispositivos que expressamente requerem regulamentação por parte da Autoridade Nacional de Proteção de Dados (ANPD), como aqueles relacionados a relatórios de impacto à proteção de dados, à figura do encarregado ou a alguns direitos dos titulares.

Ao mesmo tempo, a LGPD incide sobre áreas que são um "mundo" em si mesmo, como relações de trabalho ou a proteção de crianças e adolescentes. Assim, dúvidas sobre a aplicação de bases legais, por exemplo, vêm temperadas com reflexões sobre outros elementos tradicionais do direito, como o poder diretivo do empregador ou o princípio constitucional do melhor interesse da criança.

1 O projeto Privacidade e Proteção de Dados no Congresso Nacional, lançado pela Associação Data Privacy Brasil de Pesquisa em 2021, descreve esse quadro quantitativa e qualitativamente. Em relação a números, até dezembro de 2021, 675 proposições sobre privacidade e proteção de dados foram propostas na Câmara dos Deputados e Senado Federal, sendo que mais da metade delas foram propostas após agosto de 2018, mês de aprovação da LGPD. Disponível em: <https://www.observatorioprivacidade.com.br>.

Mais de dois anos após a aprovação da LGPD, foi instalada em novembro de 2020 a Autoridade Nacional de Proteção de Dados (ANPD), que imediatamente publicizou sua agenda regulatória para os anos de 2021 e 2022, ressaltando as prioridades temáticas sobre as quais deve se debruçar no período.

Desde então, a ANPD deu início a vários processos - com participação pública por meio de tomadas de subsídio, consultas públicas e audiências públicas - e avançou na agenda em temas como pequenas e médias empresas, comunicação de incidentes de segurança e seu processo sancionatório. Muitos pontos, entretanto, seguem em aberto e o debate não tem hora para acabar.

Com tudo isso em mente, ainda em setembro de 2020, a Associação Data Privacy Brasil deu início à série de webinars "**LGPD em movimento**", apoiada pelo Meta[2] no âmbito do Observatório da Privacidade e Proteção de Dados. O nome da série procura justamente captar esse momento singular no qual se forjam e se disputam diferentes interpretações do conjunto de normas da LGPD. Um momento de efervescência para o que se convencionou chamar de dogmática jurídica, umas das principais marchas que dá ritmo ao campo do direito.

A partir do objetivo de contribuir com o debate público qualificado sobre temas particularmente críticos da interpretação da LGPD, e buscando seguir a lógica de discussões multissetoriais que marcou a tramitação da própria lei, de lá para cá foram realizados 8 (oito) webinars sobre os seguintes temas: i) Transferência Internacional de Dados; ii) LGPD e crianças e adolescentes; iii) LGPD e a base legal de execução do contrato; iv) LGPD e decisões automatizadas; v) LGPD e os direitos dos titulares; vi) Legítimo Interesse; vii) Responsabilidade civil na LGPD e; viii) Relatórios de Impacto à Proteção de Dados.

Além de transmitir os debates ao vivo e disponibilizá-los posteriormente em uma playlist do canal do Data Privacy Brasil no Youtube, ao longo desse percurso a equipe também produziu pequenos ensaios, que resumem cada webinar e pontuam as principais reflexões trazidas pelos participantes[3]. A maioria desses ensaios foi publicada a cada mês no blog do Observatório e agora todos eles foram revisados e

2 Todos os financiamentos recebidos pela Associação são balizados por sua Política de Financiamento Ético e Transparência. Com o objetivo central de resguardar a autonomia da organização e suas pesquisas, a Política prevê, dentre outros pontos, a revisão por um comitê externo para avaliação de potenciais financiamentos de valor superior a R$ 200.000,00, a fim de se identificar potenciais ou reais conflitos de interesse. Disponível em: <https://www.dataprivacybr.org>.

3 Agradecemos a participação e contribuição de todos os painelistas, que nomeamos com as afiliações que possuíam à época de sua participação nos webinários: Giovanna Carloni (CIPL), Paula Pedigoni (USP), Mário Viola (CMPF - European University Institute), Bárbara Simão (IDEC), Juliana Domingues (SENACOM), Daniela Cravo (ESDM), Raíssa Moura (Head Legal Incognia), Daniel Dias (FGV-RJ Direito), Crisleine Yamaji (FEBRABAN), Flávia Lefèvre (Intervozes), Mauro Sobrinho (Secretaria de Governo Digital), Juliana Sakai (Transparência Brasil), Vanessa Butalla (Serasa Experian), Enrico Roberto (FDUSP), Camila Nagano (iFood), Marcel Leonardi (Leonardi Advogados), Luciana Xavier - (UFPR), Renato Santa Rita (Proteste Brasil), Camila Camargo (Andersen Ballão Advocacia), Chiara de Teffé (Ibmec), Elora Fernandes (UERJ), Isabella Henriques (Instituto Alana) , Ralf Sauer (Comissão da UE), Gabriela Zanfir (Future of Privacy Forum), Bojana Bellamy (CIPL), Luiza Brandão (IRIS) e Renato Leite Monteiro (Twitter).

compilados nessa publicação, que apresenta um quadro mais completo do acúmulo da série LGPD em movimento.

Além dos ensaios em si, a equipe incluiu referências e comentários sobre eventuais novidades que tenham surgido sobre os temas discutidos ou sobre casos concretos mencionados pelos painelistas à época de cada webinar. Assim, a publicação constrói um retrato bastante rico do estado da arte do debate jurídico sobre os temas à época de cada evento, com reflexões e questionamentos que perduram, e também atualiza alguns pontos de acordo com desenvolvimentos posteriores e materiais de referência para aprofundamento.

Esperamos que aproveite a leitura!

Por Bruno Bioni & Mariana Rielli

SÉRIE LGPD EM MOVIMENTO

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Webinar realizado no dia **10 de setembro de 2020**

POR *Bruno Bioni, Iasmine Favaro e Mariana Rielli*

Recentemente, no caso conhecido como Schrems II, o Tribunal de Justiça da União Europeia (TJUE) invalidou o Escudo de Privacidade, ou EU-US Privacy Shield, que regulamentava a transferência internacional de dados entre Estados Unidos e Europa. O Privacy Shield foi criado, em 2015, para substituir o International Safe Harbor Privacy Principles, que também foi anulado em um processo movido pelo ativista Max Schrems.

No primeiro webinário do projeto "LGPD em movimento", organizado pelo Observatório da Privacidade e da Proteção de Dados, o tema da transferência internacional de dados foi discutido por especialistas de diferentes áreas, que propuseram soluções, problemáticas e impacto da invalidação do Privacy Shield.

Em ambos processos, Schrems denunciou o aparato legal criado para a transferência internacional de dados entre EUA e UE, alegando que o nível de *adequacy* entre os países não seria suficiente para garantir a proteção de dados pessoais dos titulares europeus. O primeiro (Schrems I) ocorreu após Edward Snowden ter tornado públicos os detalhes de programas estadunidenses de vigilância em massa, revelando o uso de dados não só de americanos, mas também de estrangeiros, para fins diversos dos da transferência internacional.

Gabriela Zanfir, do Future of Privacy Forum afirmou que, no período em que atuou no European Data Protection Supervisor (EPDS), após a invalidação do Safe Harbor, o foco da autoridade europeia era o de desenvolver um novo acordo, propondo o aparato jurídico necessário para que a transferência internacional de dados fosse segura para os titulares. No entanto, como observado, o Privacy Shield também foi invalidado pela Corte Europeia. Mas qual a diferença entre a primeira e a última decisão?

O que mudou com os casos Schrems I e II?

Como mencionado, ambos os processos trataram de falhas na adequação da legislação de proteção de dados americana com relação à europeia, mas o caso Schrems II, na prática, tem uma repercussão muito maior sobre o dia-a-dia das empresas que têm como atividade a transferência internacional de dados. Isso porque a decisão do caso Schrems II não apenas invalidou o Privacy Shield, como também determinou que, embora válidas, as cláusulas contratuais padrão aprovadas pela Comissão Europeia - um outro mecanismo para a transferência internacional - podem vir a ser consideradas falhas para o exercício do direito à proteção de dados dos cidadãos europeus.

Em resumo, o TJUE decidiu que, ainda que as cláusulas padrão possam ser utilizadas como medida de salvaguarda para garantir os padrões mínimos de segurança e proteção de dados, elas não são absolutas e devem estar sujeitas a uma análise da prática e legislação do país destino, sendo responsabilidade do controlador observar tais eixos: "*o Tribunal salienta, em particular, que essa decisão impõe ao exportador de dados e ao destinatário dos dados a obrigação de verificar, antes de qualquer transferência, se esse nível de proteção é respeitado no país terceiro em causa e se a decisão exige que o destinatário informe o exportador de dados de qualquer incapacidade de cumprir as cláusulas-padrão de proteção de dados, sendo este último, por sua vez, obrigado a suspender a transferência de dados e/ou rescindir o contrato com o primeiro.*"

Embora a decisão seja aplicável apenas às relações entre Estados Unidos e a União Europeia, ela suscita discussões mais amplas, por exemplo: Quais medidas poderiam ser tomadas para que a transferência internacional de dados pudesse continuar acontecendo também entre outros países que não apresentem um alto grau de *adequacy* com a legislação europeia? Quais seriam os impactos econômicos da decisão?

Entraves e reflexões acerca da invalidação do EU-US Privacy Shield

Em primeiro lugar, cabe dizer que a decisão do TJUE no caso Schrems II trouxe à tona a discussão que já ocorre há muito acerca da função dual da legislação de proteção de dados pessoais. A primeira – e evidente – função é a de proteção do direito fundamental à proteção de dados pessoais. A segunda, por outro lado, é a de ser um elemento facilitador de trocas econômicas, estimulando a inovação. Como apontou Bojana Bellamy, as leis de proteção de dados funcionam em um contexto econômico que não diz respeito apenas à proteção dos titulares dos dados, e cabe às organizações que discutem o tema a capacidade de equilibrar a função dual da legislação, para que o fluxo internacional de dados possa continuar existindo, mas através de mecanismos que protejam os cidadãos.

Sob esse aspecto, a transferência internacional de dados é um dos temas mais relevantes para as leis de proteção de dados, porque é ela que permite que não apenas as Big Techs, mas também startups que, desde sua concepção são globais, funcionem ao realizar operações diárias de transferência internacional para manter o seu desempenho.

A esse respeito ainda persistem estratégias regulatórias que forçam o armazenamento de dados pessoais em uma localização específica, como o caso da Rússia, que implementou lei específica para data *localization*. O tema foi amplamente debatido no Brasil durante o processo de formulação do Marco Civil da Internet e, conforme demonstra o relatório de aprovação do Deputado Federal Alessandro Molon, o armazenamento forçado dos dados em determinada localização não foi aprovado, sendo que sociedade civil e empresas brasileiras e estrangeiras votaram contra a aprovação da medida. Dever-se-ia dar menor relevância para a localização dos dados e maior relevância para a adequação dos diferentes países aos critérios mínimos de proteção aos direitos fundamentais, como o da proteção de dados pessoais. A painelista Luiza Brandão iniciou a sua fala no webinário frisando exatamente esse ponto, ao afirmar a importância da convergência e harmonização entre diferentes países e reuniões, não apenas para facilitar os fluxos de dados, mas também para que se garantam níveis apropriados de proteção de dados.

Nesse sentido, a Convenção 108 do Conselho da Europa/CoE, que pode ser aderida inclusive por países não-membros do CoE, é o principal instrumento de direito internacional para que haja essa convergência normativa. Por outro lado, Luiza destacou que o caso Schrems II aponta para uma imediata necessidade de criação de padrões internacionais de proteção de dados que olhem para o sistema como um todo, levando em consideração não apenas como os dados são tratados pelas empresas, mas também com atenção ao acesso governamental a dados, de forma a garantir os padrões de proteção de dados pessoais estabelecidos, ponto também ressaltado pelos demais painelistas.

Nessa perspectiva, como apontou Rauf Sauer, é importante estabelecer padrões internacionais de proteção de dados pessoais sobre como governos podem acessar dados para fins de segurança pública, persecução criminal e outros fins legítimos. Desde o caso Schrems I, esse permanece sendo o principal calcanhar de aquiles para que haja um livre fluxo informacional transfronteiriço – terminologia amplamente utilizada pela OCDE.

Outro mecanismo, apontado por Bruno Bioni como meio eficiente de transferência internacional de dados no Setor Privado são as Binding Corporate Rules (BCRs). Se validadas pelos órgãos reguladores, cria-se uma espécie de zona intra-organizacional segura para o fluxo de dados. Por exemplo, empresas e entidades de um mesmo grupo econômico podem trocar dados entre si, ainda que o destino seja um país sem um nível de proteção de dados adequado.

Também, uma ferramenta indicada por Renato Leite Monteiro como possibilidade de preservação

do fluxo internacional de dados é o artigo 33, inciso IX da Lei Geral de Proteção de Dados, que trata da hipótese de a transferência se dar para atender a execução de um contrato e que, portanto, independe da iniciativa da Autoridade Nacional da Proteção de Dados e políticas de governo. Esse pode ser o caso, por exemplo, do compartilhamento de dados realizado por empresas aéreas, que demandam o fluxo transfronteiriço de dados pessoais para executar o contrato estabelecido entre o titular dos dados e a empresa.

E no Brasil?

Com a invalidação do EU-US Privacy Shield e a relativização das cláusulas-padrão como hipótese para a transferência internacional, fica ainda mais evidente a necessidade da instalação de uma Autoridade Nacional de Proteção de Dados (ANPD) robusta e independente. Isto porque, havendo tal arranjo institucional, abre-se espaço para que o Brasil seja reconhecido como um país com nível adequado de proteção de dados.

Com isso, empresas e outros agentes de tratamento de dados podem transferir dados para cá sem ter que se valer de outros instrumentos, os quais detêm, via de regra, um alto custo. Em poucas palavras, diminuem-se as barreiras de entrada para que atores da indústria nacional atuem em escala global e possam manter grande parte das suas atividades de tratamento de dados no país.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- A ANPD foi instalada em novembro de 2020 e conta com uma Coordenação-Geral de Relações Institucionais e Internacionais;
- Um pouco depois do webinar, o European Data Protection Board aprovou um conjunto de recomendações sobre transferências internacionais pós-Schrems II. Em junho de 2021, as recomendações foram complementadas.
- Também em junho de 2021, a Comissão Europeia adotou dois novos conjuntos de Cláusulas Contratuais Padrão - um para uso entre controladores e operadores e um para transferências internacionais.

Para aprofundar...

- MARQUES, Fernanda Mascarenhas. Cláusulas-padrão contratuais como autorizadoras para a transferência internacional de dados: alternativas em casos de ausência de decisão e adequação. **Revista do Advogado**. Ano 39. Nº 144. Novembro de 2019.
- AQUINO, Theófilo Miguel; MARQUES, Fernanda Mascarenhas. O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo. *In*: BIONI, Bruno Ricardo; DONEDA, Danilo; MENDES, Laura Schertel; JUNIOR, Otávio Luiz Rodrigues; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. São Paulo: Editora Forense, 2021. p. 299-319.
- INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. Projeto Governança Global da Internet, Conflitos de Leis e Jurisdição.

SÉRIE LGPD EM MOVIMENTO

LGPD E A PROTEÇÃO DE CRIANÇAS E ADOLESCENTES

Webinar realizado no dia 01 de outubro de 2020

POR *Bruno Bioni, Iasmine Favaro e Mariana Rielli*

A pandemia do coronavírus, que assolou o Brasil e o mundo desde março de 2020, teve impactos sobre o tema da proteção de dados pessoais, em geral. No caso de dados de crianças e adolescentes, práticas como o ensino à distância em razão da necessidade do isolamento social tornaram obrigatório para a maioria das pessoas dessa faixa etária o fornecimento de dados pessoais, a fim de, por exemplo, utilizar plataformas de streaming e videoconferência.

Ao mesmo tempo, o surgimento do TikTok, nova rede social com mais de 65 milhões de usuários no Brasil, incitou polêmicas ao ser acusado de violar a privacidade e utilizar inadequadamente dados de crianças menores de 13 anos, o que também demonstra a urgência do debate sobre a proteção de dados das crianças e adolescentes.

Diante desse quadro, e levando ainda em consideração as questões deixadas em aberto pela LGPD em relação à disciplina do tratamento de dados de crianças e adolescentes, o OPPD selecionou essa temática para o segundo webinário da série "LGPD em movimento: temas chave de implementação". Seu objetivo foi explorar mais a fundo, dentre outros elementos, quais são os limites do tratamento de dados pessoais de crianças e adolescentes e quais bases legais podem ser adequadamente empregadas para legitimar o uso desses dados, que merecem proteção especial.

Bases legais: quais se adequam ao tratamento de dados de crianças e adolescentes?

Cresce, cada dia mais, o investimento global em publicidade digital voltada para crianças, com previsão de 1,7 bilhões de dólares até 2021, compondo 37% de todo o valor aplicado em publicidade no mundo. A intensificação massiva dos investimentos demonstra que o direcionamento de publicidade a

crianças e adolescentes é um "negócio" muito lucrativo para as empresas.

Por outro lado, também é nocivo para os seus alvos, na medida em que, como aponta a Senacon, crianças de até sete anos não são capazes de distinguir a publicidade de um conteúdo comum e, até os doze anos, não compreendem o caráter persuasivo das publicidades, sendo, dessa forma, mais vulneráveis do que adultos.

Nesse sentido, Isabella Henriques, do Instituto Alana defendeu, citando a recomendação da Academia Americana de Pediatria, que a publicidade direcionada ao público infantil é questionável per se, e que a utilização de dados pessoais de crianças e adolescentes para fins de publicidade comportamental deve ser absolutamente repudiada. Isso, segundo Isabella, decorre de uma leitura sistemática do quadro normativo brasileiro:

NORMA	REFERÊNCIA
Constituição Federal	**Art. 227** – É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.
Constituição Federal	**Art. 5º, X** – 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;
Convenção Sobre os Direitos da Criança (UNICEF)	Todas as ações relativas à criança, sejam elas levadas a efeito por instituições públicas ou privadas de assistência social, tribunais, autoridades administrativas ou órgãos legislativos, devem considerar primordialmente o melhor interesse da criança.
Estatuto da Criança e do Adolescente	O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, idéias e crenças, dos espaços e objetos pessoais.
Estatuto da Criança e do Adolescente	**Art. 71** – A criança e o adolescente têm direito à informação, cultura, lazer, esportes, diversões, espetáculos e produtos e serviços que respeitem sua condição peculiar de pessoa em desenvolvimento.

NORMA	REFERÊNCIA
Código Civil	**Art. 11** – Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
Lei Geral de Proteção de Dados	**Art. 14** – O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
Lei Geral de Proteção de Dados	**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; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável

Como é possível observar no quadro, existem princípios, que lidos em harmonia com as previsões da Lei Geral de Proteção de Dados, devem ser respeitados quando praticada a atividade de tratamento de dados de crianças e adolescentes. Um dos exemplos é, como prevê a Convenção Sobre os Direitos da Criança da ONU, a Constituição brasileira e a própria LGPD, o *princípio do melhor interesse*, que determina que qualquer atividade que envolva crianças deve ter como prioridade o seu melhor interesse e, de forma alguma, poderá prejudicá-las. Tal constatação traz uma nova camada de complexidade e um elemento adicional que deve ser analisado no estudo das bases legais aplicáveis ao tratamento de dados de crianças e adolescentes.

Deste modo, como apontou Isabella Henriques, ainda que haja o consentimento parental específico e destacado, previsto no art. 14 da LGPD, se ele eventualmente contrariar o melhor interesse da criança, ele não se sustentará como base legal e a prática do tratamento pode ser considerada abusiva. Essa é uma constatação importante porque, seja por falta de conhecimento adequado sobre determinada tecnologia ou plataforma ou até por má-fé, o recurso exclusivo à vontade de pais e responsáveis pode não ser suficiente para garantir uma proteção integral e, então, o princípio do melhor interesse funciona como uma salvaguarda contra eventuais danos causados à criança e ao adolescente.

Além das implicações do princípio do melhor interesse, o Webinário também foi marcado por uma das discussões mais presentes no marco da LGPD e os direitos das crianças e adolescentes: seria o consentimento a única base legal aplicável? Ou haveria alternativas, como a equiparação dos dados de crianças e adolescentes a dados sensíveis e a consequente aplicação das bases legais do art. 11?

Segundo Elora Fernandes, da UERJ, especificamente para o setor público, três bases legais são frequentemente utilizadas para além do consentimento: para fins de políticas públicas, para fins de pesquisa e para a tutela da saúde. Para a pesquisadora, essas bases podem ser adequadamente utilizadas pelo setor público, mas também são passíveis de invalidação a partir do princípio do melhor interesse das crianças e adolescentes.

Adiante, as outras painelistas também abordaram a questão de quais bases legais podem ser aplicadas para o tratamento de dados de crianças e adolescentes, levando-se em consideração, por exemplo, a disciplina do Regulamento Geral de Proteção de Dados europeu (GDPR), em que há a possibilidade de aplicação de todas as bases legais, inclusive, do legítimo interesse.

Segundo Chiara de Teffé, o GDPR caminhou bem no assunto relativo ao tratamento de dados de sujeitos dessa faixa etária. No Brasil, o paradigma em todo tratamento de informações de crianças e adolescentes deverá ser sempre o princípio do melhor interesse, conforme preconiza o caput do art. 14 da LGPD. Teffé entende ser possível o diálogo do art. 14 com as bases legais dispostas nos artigos 7º e 11 da LGPD, porém afirma ser necessário adotar especial atenção com a hipótese do legítimo interesse, que só poderia ''caber'' em situações excepcionais, devidamente justificadas. A tutela do crédito deveria ser afastada nesse caso, segundo a pesquisadora e professora. Salientou também a relevância de se conferir uma proteção ampliada para os dados sensíveis de crianças e adolescentes, havendo a feitura de relatórios de impacto e cuidado adicional com a lógica do privacy by design.

Isabella Henriques, por outro lado, defendeu a equiparação, em todas as hipóteses, dos dados de crianças e adolescentes aos dados sensíveis e apontou que "se nós consideramos aqui no Brasil que o legítimo interesse é possível, vamos abrir uma possibilidade de análises subjetivas que vão ser muito complexas, na casuística. Na prática, estaremos possibilitando uma violação constante dos direitos da criança e do adolescente. A base do legítimo interesse conflita com o melhor interesse."

Para Elora Fernandes, caberá à Autoridade Nacional de Proteção de Dados harmonizar a interpretação do melhor interesse com o rol de bases legais mais adequado, assim como fez o ICO, autoridade britânica de proteção de dados, que, em diretrizes específicas para tratamento de dados de crianças e adolescentes, desaconselhou o emprego da base legal do legítimo interesse, na medida em que nela o interesse está mais ligado ao sujeito que realiza o tratamento e não ao titular, o que tende a ferir o melhor interesse das crianças e adolescentes. Sobre a questão do melhor interesse, ainda, o ICO criou um código de conduta para serviços online (Age Appropriate Design Code) que ajuda a parametrizar sua aplicação.

Complementando o debate sobre o tema das bases legais, a painelista Camila Camargo partiu do pressuposto de que, especificamente no ambiente escolar, há um desafio central de tradução dessas

preocupações para o dia-a-dia de pais, crianças e educadores, em um sentido que é também cultural. Além disso, levantou questionamentos relevantes, como a possibilidade de se considerar eventual legítimo interesse por parte de escolas e outras instituições de ensino, inclusive porque, por definição, elas devem defender os interesses de seus estudantes em um sentido mais amplo. No mesmo sentido, destacou a camada adicional de complexidade acrescida pela ampla gama de obrigações legais a que instituições de ensino estão sujeitas, por força de normas como a Lei de Diretrizes e Bases da Educação Nacional, o que coloca esses atores, especificamente, em uma constante busca por equilíbrio e harmonização diante das mudanças trazidas pela LGPD.'

Em conclusão, o debate do uso de dados infantis está no topo da agenda e evidencia posições diferentes em torno de temas comuns, como a aplicação das bases legais ao tratamento dos dados desses indivíduos. Quando devidamente instalada, a Autoridade Nacional de Proteção de Dados poderá ser instada a se posicionar sobre o tema e formular interpretações e recomendações, a exemplo de outras autoridades ao redor do mundo. Mas deverá fazê-lo em harmonia com todo o quadro normativo existente para a proteção das crianças e adolescentes, cujo cerne é a garantia do seu melhor interesse.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- A ANPD ainda não se debruçou especificamente sobre o tema. Apesar disso, o Instituto Alana divulgou contribuição que apresentou à Consulta Pública da ANPD sobre a aplicação da LGPD para agentes de pequeno porte, com foco na proteção de dados de crianças e adolescentes.
- O comitê dos direitos das crianças da ONU publicou o Comentário Geral 25 (Children 's rights in relation to the digital environment), do qual a Associação Data Privacy de Pesquisa participou da 2º consulta pública, em novembro de 2020.
- Sobre a discussão envolvendo as bases legais aplicáveis, foi realizado o Data Debate "Proteção de crianças e adolescentes na LGPD: desafios interpretativos", que tratou sobre o tema a partir de um texto do mesmo nome de autoria Elora Fernandes e Filipe Mendon.
- O Age Appropriate Design Code da ICO foi traduzido para o português pelo Instituto Alana e o ITS Rio.

Para aprofundar...

- ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA E INSTITUTO ALANA. A proteção de dados de crianças e adolescentes: uma radiografia institucional do Boletim da Infância e Privacidade. 2021.
- FERNANDES, Elora; MEDON, Filipe. Proteção de crianças e adolescentes na LGPD: desafios interpretativos. **REVISTA ELETRÔNICA DA PGE-RJ**, *[S. l.]*, v. 4, n. 2, 2021. DOI: 10.46818/pge.v4i2.232.
- FERNANDES, Elora. Direitos de Crianças e Adolescentes por Design: Uma agenda regulatória para a ANPD. *In*: Priscilla Laterça; Elora Fernandes; Chiara de Teffé; Sérgio Branco. (Org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. 1ed. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio; Obliq, 2021, v. 1, p. 200-254.
- TEFFÉ, Chiara A. Spadaccini de. Proteção de dados de crianças e adolescentes. **Revista do Advogado**, v. 39, p. 1-225, 2019.
- TEFFÉ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. In: Priscilla Laterça; Elora Fernandes; Chiara de Teffé; Sérgio Branco. (Org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. 1ed. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio; Obliq, 2021, v. 1. E-book disponível em: <https://itsrio.org/pt/publicacoes/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes/>
- HENRIQUES, Isabella; PITA, Marina; e HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; e RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, pp. 199-225.

SÉRIE LGPD EM MOVIMENTO

LGPD E A BASE LEGAL DA EXECUÇÃO DO CONTRATO

Webinar realizado no dia 12 de novembro de 2020

POR *Bruno Bioni e Mariana Rielli*

Dando continuidade à tarefa de endereçar temas sensíveis, ou mesmo polêmicos, da Lei Geral de Proteção de Dados, a Associação Data Privacy Brasil de Pesquisa organizou, no dia 12 de novembro, o terceiro Webinar da série "LGPD em movimento: temas chave de implementação", que abordou a base legal da execução do contrato.

As bases legais para o tratamento de dados pessoais despertam questionamentos que vão além da escolha da hipótese mais adequada em um caso concreto. No segundo Webinar da série, por exemplo, o tema foi a proteção de dados de crianças e adolescentes, e boa parte da discussão concentrou-se nas diferentes possibilidades de interpretação da lei quanto às bases legais aplicáveis para o tratamento de dados de menores.

Diante da multiplicidade de pontos em aberto sobre uma base legal específica, a de execução do contrato (art. 7º, V), Camila Nagano (Ifood), Luciana Xavier (UFPR), Marcel Leonardi (Leonardi Advogados) e Renato Santa Rita (PROTESTE Brasil) juntaram-se à equipe da Associação para um debate multissetorial, que buscou avançar o entendimento sobre uma questão que, embora muito relevante, é pouco discutida na área.

A base legal da execução do contrato vale para todos os contratos?

No caso da base legal do execução do contrato, as ponderações iniciam-se pela própria redação ambígua do art. 7º, segundo a qual o tratamento de dados pessoais poderá ser realizado "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados".

Resultado de um provável descuido na técnica legislativa, o dispositivo abre espaço para duas interpretações: a primeira, alinhada com o Regulamento Geral de Proteção de Dados europeu e com o entendimento firmado pelo European Data Protection Board (EDPB), de que o titular dos dados pessoais tratados com base nessa hipótese deve sempre ser parte na relação jurídica, seja contratual ou pré-contratual. Uma segunda opção, entretanto, é que essa exigência de vinculação valeria apenas para os "procedimentos preliminares relacionados a contrato do qual seja parte o titular". Segundo tal entendimento, a base legal em questão poderia ser mobilizada para o tratamento de dados necessários à execução de *qualquer* contrato, independente de o titular ser parte nele ou não. Tal dúvida é acentuada pela escolha da palavra "ou", partícula que denota uma alternativa.

Para Marcel Leonardi, sócio do Leonardi Advogados, a segunda via interpretativa é a mais condizente com a realidade das empresas e dos negócios no país, sendo a terceirização um bom exemplo de situação que poderia se beneficiar dessa base legal sem a necessidade de o agente de tratamento e o titular serem ambos partes do contrato. Nesse caso, um tomador de serviço poderia tratar, amparado nessa base legal, os dados pessoais de empregados terceirizados, com os quais ele não guarda relação direta, já que o contrato se dá com a intermediação da prestadora.

No entanto, o advogado observou que não é essa a abordagem que vem sendo adotada pelas grandes empresas, que preferem uma posição mais conservadora, seguindo o entendimento europeu. Camila Nagano, DPO do Ifood, concorda com tal enfoque cauteloso, privilegiando a aplicação de outras bases legais nos casos de dados de terceiros que não são parte do contrato.

O que significa ser necessário para a execução de um contrato?

Ainda sobre os requisitos decorrentes da própria redação do art. 7º, V, parte da discussão do Webinar voltou-se para a exigência do caráter "necessário" para a execução de um contrato. O primeiro ponto levantado, por Renato Santa Rita, DPO da Proteste Brasil, foi a relação entre o dispositivo e os princípios da LGPD, como finalidade e a própria necessidade, além da boa-fé. O foco, segundo ele, deve estar no titular e na expectativa razoável que ele tem sobre um determinado tratamento dos seus dados ser necessário, ou não. Quanto às empresas, Marcel Leonardi aponta que o requisito "necessário" deve se conectar à realidade dos fatos, e não necessariamente à letra do contrato, uma vez que pode haver distorções ou mesmo a inclusão de tratamentos de dados que sejam interessantes, úteis e proveitosos a um modelo de negócio, mas não necessários para a entrega do produto ou serviço em questão.

Onde, entretanto, traçar a linha do que pode ser considerado, de fato, uma necessidade contratual? Uma primeira pista levantada por Leonardi é o princípio da finalidade (art. 6º, I), que fala em propósitos "legítimos, específicos, explícitos e informados ao titular", mas não menciona uma *necessidade estrita*. Outra

seria o art. 10, §1º, que, ao contrário, afirma que quando a base legal for o legítimo interesse, somente os dados estritamente necessários poderão ser tratados. Tal qualificadora não foi imposta à necessidade da execução do contrato, o que poderia sinalizar para uma interpretação mais flexível dessa exigência.

Em resposta, Camila Nagano fez referência a um teste prático, do dia-a-dia, utilizado para averiguar a necessidade de um determinado tratamento: ele inclui as perguntas "para quê" (finalidade), "por quê" (necessidade) e "como" (segurança). Ao se referir ao teste da necessidade, a advogada sublinhou se tratar de uma "necessidade real", e não de um tratamento que seja meramente conveniente para o negócio.

A prof. Luciana Xavier, da Universidade Federal do Paraná, trouxe duas abordagens sobre esse ponto: uma acadêmica, que considera "necessário" sinônimo de "indispensável", "imprescindível", "vital" e outra mais prática, que parte da existência de "nuances" para questionar uma interpretação excessivamente restritiva do dispositivo, ao mesmo tempo em que reconhece que necessário não pode ser sinônimo de "útil". O cerne da fala, entretanto, foi a dificuldade imposta pela própria lei para o desenho dessa linha e a sugestão da professora, a exemplo do que fora mencionado pelo representante da Proteste, foi o recurso à boa-fé como "fiel da balança". A esse respeito, é importante observar que, em termos topográficos e de técnica legislativa, boa-fé é o "princípios dos princípios", em razão de estar no caput do artigo 6º da LGPD.

Execução do contrato e consentimento: qual a diferença?

Partindo para outras questões interpretativas bastante complexas, os participantes do Webinar discutiram as diferenças primordiais entre a base legal de execução do contrato e a base legal do consentimento. Possíveis confusões entre as duas hipóteses autorizativas decorrem do fato de que a assinatura (ou um aceite não-verbal) de um contrato que envolva algum tratamento de dados pessoais pode ser lida como a oferta de consentimento por parte do titular. Nesse sentido, nas palavras de Marcel Leonardi, haveria uma confusão entre a "manifestação de vontade de adesão a um contrato e o fundamento jurídico que autoriza o tratamento de dados derivado deste contrato".

A respeito da diferença entre as bases legais, todos os painelistas concordaram que, a partir da celebração de um contrato, o tratamento dos dados pessoais nele envolvidos pode ter como hipótese autorizativa qualquer uma das listadas na LGPD, inclusive a execução do contrato, quando cabível, ou o consentimento, desde que respeitadas as suas qualificadoras. Trata-se, portanto, de momentos diferentes, com consequências jurídicas distintas. Camila, do Ifood, lembrou, inclusive, que, em negócios digitais, as empresas devem seguir os requisitos do Marco Civil da Internet/MCI, que exige o consentimento destacado das demais cláusulas contratuais. A esse respeito, inclusive, é importante lembrar que o MCI utilizar ''expresso" como parte da ampla adjetivação empregada ao consentimento.

Base legal de execução do contrato no contexto de coleta de dados para publicidade direcionada: pode?

Uma das questões mais relevantes sobre a base legal de execução do contrato é sua aplicação no contexto da publicidade direcionada, especificamente por plataformas e redes sociais. O principal ponto que gera discussões, nesse caso, é o fato de que as plataformas não são remuneradas com o dinheiro dos usuários, mas sim com os seus dados pessoais, que são tratados para uma variedade de finalidades, inclusive para a criação de anúncios personalizados.

Para Marcel Leonardi e Renato Santa Rita, uma vez considerado que a contraprestação ao serviço fornecido pela plataforma é a coleta e utilização dos dados pessoais do usuário, seria razoável o tratamento para finalidades diversas, desde que respeitados os princípios de proteção de dados, especialmente a transparência junto ao titular.

Para além desse ponto inicial, o debate suscitado por tais modelos de negócio é o seguinte: o tratamento de dados para fins de publicidade direcionada pode ser considerado *necessário* à execução do contrato entre a plataforma e o usuário (titular) e, portanto, basear-se na hipótese autorizativa do art. 7º, V? Sobre isso, foram expostas visões antagônicas: de um lado, aquela defendida, por exemplo, pelo European Data Protection Board, de que o uso dos dados para a realização de anúncios personalizados não seria inerente ao contrato celebrado com o titular para a utilização do serviço, de forma que o recurso a outra base legal seria necessário nesse caso. De outro, a visão defendida pelas próprias empresas, de que esse é o núcleo que sustenta o seu modelo de negócio, sem o qual elas não poderiam funcionar.

Extinção do contrato e ciclo de vida de dados: qual a relação?

Outra questão levantada e debatida no Webinar diz respeito ao fim do contrato, seja qual for o motivo ou modalidade. Sobre esse ponto, questionou-se se imediatamente a base legal da execução do contrato deixa de ser adequada e, em segundo lugar, se é possível "trocar" de base legal para eventualmente continuar o tratamento dos dados em questão.

Nesse caso, Camila Nagano considerou que sim, tal "troca" seria possível, desde que tomados os devidos cuidados (se a troca for para o legítimo interesse, por exemplo, seria necessária a documentação e realização de um LIA). Os outros painelistas, na sequência, elaboraram que, nesse caso, não necessariamente se trata de uma troca de base legal, mas sim de uma troca de finalidade, seguida da eleição de uma nova hipótese autorizativa para o tratamento de dados pessoais.

Assim, findo o contrato, criaria-se uma nova atividade de tratamento, com uma nova finalidade específica, que pode ser, por exemplo, resguardar-se na eventualidade de ações judiciais futuras (no âmbito trabalhista e consumerista, por exemplo) – art. 7º, inciso VI – ou responder a uma obrigação legal ou regulatória (art. 7º, inciso I).

A esse respeito, a experiência cotidiana dos painelistas foi útil para ilustrar, na prática, a operacionalização de um ciclo de vida de dados pessoais: Camila Nagano e Marcel Leonardi mencionaram não apenas a eliminação dos dados pessoais após o cumprimento da finalidade, mas, no caso de haver um novo tratamento, a segmentação de bases de dados para garantir a limitação do uso e a segurança de tais informações.

Para além da LGPD

Em diversos momentos do evento, os painelistas ressaltaram a importância de se aliar a interpretação dos dispositivos da LGPD ao ordenamento jurídico em que ela está inserida, que conta com leis setoriais sobre proteção de dados, além de normas como o Código Civil e o Código de Defesa do Consumidor, que regem as relações contratuais.

Assim, diante de questionamentos sobre a possibilidade de existência de cláusulas contratuais que descrevam finalidades diversas, inicialmente Luciana Xavier levantou a possibilidade de se recorrer a dispositivos como o CDC para verificação de eventual abusividade no caso concreto. Camila Nagano, por outro lado, lembrou que, a depender da situação, é aceitável a inclusão de cláusulas com finalidade distinta daquela que é o objeto principal do contrato, e, nesses casos, a baliza deve ser o risco que tal tratamento imporá ao titular, o que também deve ser analisado casuisticamente.

Por fim, Marcel Leonardi lembrou que, no caso de haver cláusulas abusivas ou ilegais em um contrato, "não há base legal na LGPD que justifique". Por outro lado, em casos em que isso não ocorra, o advogado considera que tanto é possível como é extremamente comum que haja uma série de tratamentos e finalidades díspares no mesmo contrato, desde que cada uma conte com uma base legal justificada.

Em resumo, a LGPD apresenta um rol extremamente amplo de bases legais. Tão desafiador quanto entender em quais hipóteses a base legal de execução do contrato será aplicável, é compreender como combiná-la com outras ao longo de todo o ciclo de vida de um dado pessoal.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

Para aprofundar...

- TEFFÉ, Chiara Spadaccini de; VIOLA, Mário. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: BIONI, Bruno Ricardo; DONEDA, Danilo; MENDES, Laura Schertel; JUNIOR, Otávio Luiz Rodrigues; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. São Paulo: Editora Forense, 2021. p. 117-149.
- EUROPEAN DATA PROTECTION BOARD. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. 2019.
- INFORMATION COMMISSIONER'S OFFICE. Guide to the General Data Protection Regulation (GDPR). Lawful basis for processing. Contract.

SÉRIE LGPD EM MOVIMENTO

LGPD E DECISÕES AUTOMATIZADAS

Webinar realizado no dia 03 de dezembro de 2020

POR *Bruno Bioni e Pedro Martins*

Dando continuidade à tarefa de endereçar temas sensíveis, ou mesmo polêmicos, da Lei Geral de Proteção de Dados, a Associação Data Privacy Brasil de Pesquisa organizou, no dia 3 de dezembro, o quarto Webinar da série "LGPD em movimento: temas chave de implementação", que abordou a regulamentação de decisões automatizadas na LGPD.

O que são decisões automatizadas?

Antes de entrar em um debate sobre como a LGPD regulamenta decisões automatizadas, é preciso entender esse conceito. Como Enrico Roberto, pesquisador do Internetlab e doutorando na USP, pontuou, esse conceito ainda está em formação e não há, na LGPD, uma definição clara para ele, como existem para outros termos relevantes para a proteção de dados. Contudo, a lei trouxe em seu artigo 20 alguns direitos que incidem no caso de atividades de tratamento automatizadas.

Ainda, Enrico pontua que a regulamentação de decisões automatizadas é uma forma que tanto a LGPD, quanto o GDPR, encontraram para fazer referência sobre uma forma de tratamento de dados, que é a inteligência artificial. Podemos então, entender, decisões automatizadas como processamento de dados feitos por técnicas de inteligência artificial que visam encontrar correlações em um banco de dados e fazer previsões com base nessas correlações.

Contudo, há um elemento adicional trazido pela LGPD, que é a noção de decisão tomada **unicamente** com base em tratamento automatizado, visto que o artigo 20 impõe essa condicionante ao direito de revisão.

A confusa ideia de decisão tomada unicamente com base em tratamento automatizado

Como pontuou Enrico Roberto, há sempre uma interação entre os algoritmos e sistemas de inteligência artificial de tomada de decisão automatizada e pessoas humanas. Sendo assim, uma questão que precisa ser melhor analisada é em que momento se pode dizer que uma decisão foi de fato tomada com base unicamente em tratamento automatizado, ou se houve **participação humana significativa** nesse processo. Em poucas palavras, será adotada uma interpretação: a) literal do termo "unicamente" e que praticamente esvaziará o direito de revisão ou; b) uma outra que desengatilhará tal direito levando em consideração o *grau* de automatização desses processos decisórios, ainda que este não sejam totalmente automatizados?

Juliana Sakai, diretora de operações do Transparência Brasil, contou que o projeto Transparência Algorítmica está realizando um mapeamento no Governo Federal para entender como o Poder Público faz uso de algoritmos de tomada de decisão automatizada. Dentro desse mapeamento, nenhum órgão afirmou que essas ferramentas tomam ações, e todas seriam usadas apenas para dar suporte à tomada de decisão humana.

Fica então evidente a tensão entre o conceito de decisão **unicamente** automatizada e a prática corrente de uso dessas ferramentas. Enrico propõe, nesse sentido, a compreensão de uma decisão totalmente automatizada como aquela em que todas as fontes de informação necessárias para se chegar à decisão vieram do algoritmo, e não daquela pessoa apontada como responsável para tomar a decisão.

Assim, a inserção de um humano no processo de tomada de decisão (*human-in-the-loop*) só descaracterizaria a noção de "unicamente automatizado" caso ela de fato tenha competência e uma atuação significativa no processo de tomada de decisão. A mera validação da decisão por um humano, um papel meramente formal, não descaracterizaria a decisão totalmente automatizada.

Os direitos previstos pelo art. 20 e o direito de revisão

O direito de revisão de decisões automatizadas, previsto pelo art. 20 da LGPD, já existia dentro do microssistema do setor de crédito na Lei do Cadastro Positivo (Lei 12.414/11). Segundo Vanessa Butala, do Serasa Experian, no momento da elaboração da Lei do Cadastro Positivo a preocupação desse direito de revisão se concentrava sobre a decisão final, de concessão ou não de crédito. A LGPD, segundo Vanessa, deu um passo adiante nesse tema, não se atendo somente à decisão final, mas também incidindo nos processos de formação de perfis e garantindo um maior dever de transparência no caminho que leva à decisão final.

Contudo, no processo de aprovação da LGPD houve o veto parcial ao trecho do artigo 20 que determinava o direito de revisão como um direito de revisão humana, ou seja, feito por uma pessoa natural. Segundo Enrico Roberto, esse veto trouxe uma insegurança jurídica ainda maior, removendo a clareza de qual tipo de revisão deve ser feito, além de remover a "unha" do artigo, ou seja, deixá-lo mais fraco.

Quanto à operacionalização do direito de revisão dentro do escopo de score de crédito, Vanessa Butala entende que o titular tem direito de acesso às informações que foram consideradas para se chegar à pontuação de crédito. Isso daria um controle, para o titular, de corrigir ou atualizar alguma informação e, a partir dessa correção, uma nova pontuação pode ser alcançada. Por outro lado, em relação à fórmula e aos pesos atribuídos a cada elemento para a chegada no score final, haveria nesse caso a proteção dessas informações com base no segredo de negócio.

Enrico pontuou, ainda, que o art 20 §1º traz um direito às informações relevantes para a decisão automatizada, e propôs uma interpretação de que devem ser fornecidas as informações necessárias para o exercício dos demais direitos dos titulares, já que ele está previsto no capítulo dos direitos dos titulares.

Transparência

A transparência é um dos temas mais debatidos quando se fala em tomada de decisões automatizadas e uso de algoritmos. Visto que, muitas vezes, são empregadas técnicas de processamento de dados complexas, como machine learning, a compreensão de como se deu esse processamento e por que determinado resultado foi alcançado se torna um obstáculo. Contudo, existem outros pontos relativos a esse dever geral de transparência que podem ser melhor explorados e com uma barreira técnica menor.

Juliana Sakai pontuou, inicialmente, que uma maior transparência do poder público em relação ao uso de algoritmos e tomada de decisão automatizada é importante até mesmo para se avaliar a eficiência dessas ferramentas. Mesmo que não exista ameaças a direitos fundamentais, deve-se avaliar como essas ferramentas estão sendo usadas e se há um ganho, de fato, na sua utilização. Além disso, o controle social deve também incidir de forma mais acentuada para decisões mais sensíveis, que podem levar a discriminações, especialmente quando se fala em Poder Público, em que o dever de transparência é ainda mais forte que para o setor privado, não havendo também a incidência do segredo de negócio.

Enrico Roberto pontuou que existem diversos mecanismos para averiguar se decisões automatizadas estão sendo justas e respeitando os princípios da lei sem a quebra do segredo de negócio. Dentre eles, informações como os tipos de dados que são usados para alimentar a base de dados, quais decisões de fato são tomadas por algoritmos, como elas podem afetar direitos fundamentais, quais populações são afetadas pela decisão automatizada, bem como informações sobre quais testes foram feitos

com determinado algoritmo a fim de se evitar discriminações.

Bruno Bioni, um dos indutores do debate, trouxe também a discussão sobre a elaboração de relatórios de impacto à proteção de dados como um instrumento de intermédio entre o controle social de decisões automatizadas e as medidas de mitigação que eventualmente são (ou não) adotadas pelos controladores. Além disso, há um importante debate sobre a publicação desses relatórios, como forma de ampliar a transparência. No mesmo sentido, Enrico reforçou a importância dessa publicação destes relatórios, ainda que adaptados para não serem divulgados segredos de negócio.

Vanessa afirmou, ainda, que esse aumento na transparência e na comunicação é um movimento que já se iniciou no mercado de birôs de crédito, aumentando o acesso, aos titulares, às informações que compõem os modelos e se elas impactam positiva ou negativamente o score. Esse movimento teve como pontapé inicial a Lei do Cadastro Positivo. Em seguida, outro marco importante foi o Recurso Especial 1.419.697/RS, em que houve a primeira audiência pública da história do STJ para tratar justamente sobre a elaboração de scores de crédito.

Em 2014, o Superior Tribunal de Justiça acabou por reforçar o direito à revisão, indiretamente, ao aplicar direitos básicos do Código de Defesa do Consumidor, dentre eles o dever de informação e transparência. O STJ considerou também os princípios da necessidade e da não-discriminação para limitar os dados que poderiam ser usados para essa finalidade: "*Não podem ser valoradas pelo fornecedor do serviço de "credit scoring" informações sensíveis, como as relativas à cor, à opção sexual ou à orientação religiosa do consumidor avaliado, ou excessivas, como as referentes a gostos pessoais, clube de futebol de que é torcedor etc.*"

Esse movimento ganha agora um novo capítulo com a LGPD, que vem como marco importante para ampliar ainda mais o dever de transparência para além da decisão final.

Pode-se perceber, a partir do debate, como a LGPD trouxe importantes avanços no tema, ampliando o dever de transparência e de fornecimento de informações quanto a decisões automatizadas. Contudo, dois principais pontos ainda aguardam uma melhor definição: i) o que, de fato, são decisões tomadas unicamente com base em tratamento automatizado, e ii) quais os parâmetros do direito de revisão, já que não há mais a previsão expressa da revisão humana na LGPD.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- A ANPD ainda não se debruçou especificamente sobre o tema.
- Tem havido movimentações relevantes para o tema no Judiciário, especialmente na esfera da Justiça do Trabalho.
- Por exemplo, em maio e junho de 2021 foi discutido um caso de reconhecimento de vínculo empregatício com a Uber no qual a primeira instância determinou a perícia técnica do aplicativo como prova, já que uma série de informações, e inclusive decisões, são operadas por meio do sistema automatizado: o caso busca esclarecer, por exemplo, como chamadas são distribuídas, definição de valores, restrições com base em avaliações, etc. O TRT1 manteve essa decisão, mas o TST decidiu suspender a perícia pois considerou que, sem maiores elementos para determinar a sua necessidade, essa diligência tem potencial de revelar informações sigilosas e essenciais para o negócio da Uber.
- Um documento recente e interessante sobre o tema, que trata especificamente de transparência algorítmica, é o Algorithmic Transparency Standard, do governo do Reino Unido.

Para aprofundar...

- MARTINS, P. B. L.; HOSNI, D. Tomada de Decisão Automatizada e a Regulamentação da Proteção de Dados: Alternativas Coletivas Oferecidas pela Lei Geral de Proteção de Dados. **Internet & Sociedade**, v. 1, p. 77-101, 2020.
- KAMINSKI, Margot E. URBAN, Jennifer M. The Right to Contest AI. **Columbia Law Review**, Vol. 121, No. 7, U of Colorado Law Legal Studies Research Paper No. 21-30. 2021.
- MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados no Brasil? Instituto Igarapé. Artigo Estratégico 39. 2018.

SÉRIE LGPD EM MOVIMENTO

O LEGÍTIMO INTERESSE NA LGPD

Webinar realizado no dia 29 de janeiro de 2021

POR *Bruno Bioni e Mariana Rielli*

No quinto Webinar da série "LGPD em movimento: temas chave de implementação", realizado no dia 29 de janeiro como parte do 2º Summit Data Privacy Brasil, a Associação Data Privacy Brasil de Pesquisa promoveu um debate sobre a base legal do legítimo interesse.

Na esteira de discussões anteriores sobre as hipóteses autorizativas do tratamento de dados pessoais, como execução de contrato e consentimento, Paula Pedigoni (Universidade de São Paulo), Mario Viola (Centre for Media Pluralism and Media Freedom do Instituto Universitário Europeu), Giovanna Carloni (Centre for Information Policy Leadership) e Mariana Rielli (Associação Data Privacy Brasil de Pesquisa) foram recebidas por Bruno Bioni e trocaram perspectivas sobre algum dos pontos mais sensíveis desse tema tão complexo.

Na mesma ocasião, a Associação lançou o policy paper "O Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação", documento que reúne achados, recomendações normativas e casos concretos que buscam elucidar e propor interpretações para os aspectos da base legal do legítimo interesse que têm gerado maiores dúvidas e discussões.

Questões introdutórias: a história do legítimo interesse, hierarquia entre bases legais e *accountability*

Não há hierarquia entre as bases legais elencadas no art. 7º da LGPD, e a escolha por uma determinada hipótese para lastrear o tratamento de dados pessoais depende, exclusivamente, das circunstâncias concretas e da sua finalidade. No mesmo sentido, para Paula Pedigoni, doutoranda na Universidade de São Paulo e Mário Viola, pesquisador afiliado ao Centre for Media Pluralism and Media Freedom do Instituto Universitário Europeu, não há que se falar em uma base legal mais ou menos intrusiva, a priori,

mas apenas em bases legais mais ou menos adequadas a uma determinada situação concreta de tratamento de dados.

Esse entendimento, hoje consolidado, é produto de um longo processo de construção jurídica e integração do legítimo interesse à normativa brasileira. Mariana Rielli, coordenadora de projetos da Associação Data Privacy Brasil de pesquisa, compartilhou com os colegas e o público um pouco dessa história, ao descrever como a hipótese do legítimo interesse apenas foi incluída nos textos que deram origem à LGPD em 2015, depois de pelo menos 5 anos de discussão.

Antes disso, as propostas que tramitavam, tanto no Congresso, quanto no âmbito do Ministério da Justiça, não previam o legítimo interesse e tinham o consentimento como base legal "principal". Foi na 2º Consulta Pública do Anteprojeto de Lei de Proteção de Dados, a partir da contribuições de distintos setores, que se discutiu com mais profundidade tanto a inclusão dessa nova base legal (com parâmetros específicos para a sua aplicação) quanto a equalização de todas as hipóteses autorizativas, sem a prevalência de nenhuma sobre as outras.

Ainda como tópico introdutório à discussão, Giovanna Carloni, do Centre for Information Policy Leadership, abordou a relação da base legal do legítimo interesse com os princípios da lei e, especificamente, com o princípio da responsabilização e prestação de contas, ou *accountability*, também presente no Regulamento Europeu: a advogada afirmou que embora o legítimo interesse seja uma base flexível – ou seja, uma hipótese não atrelada a uma finalidade específica e que serve a um grande número de tratamentos em diferentes setores – isso não significa que ela seja uma "carta em branco".

Isso por alguns motivos: em primeiro lugar, a própria lei estabelece uma série de parâmetros de aplicação do legítimo interesse, prezando pelo equilíbrio entre os interesses do controlador e os interesses e direitos do titular. Em segundo, se é verdade que cabe ao próprio controlador decidir pelo emprego dessa hipótese, também é verdade que ela carrega deveres específicos, como o dever de transparência "qualificada". Nesse sentido, Giovanna afirmou que o legítimo interesse pode ser, inclusive, mais protetivo do que outras bases legais.

Decifrando o legítimo interesse: alcance, pressupostos de aplicação e obrigações

As condições descritas no art. 10 aplicam-se apenas ao controlador ou também a terceiros?

Um ponto considerado "em aberto" sobre a base legal do legítimo interesse é se o art. 10 da lei, que descreve os seus pressupostos de aplicação, aplica-se à figura do terceiro ou apenas ao controlador, uma vez que o art. 7º menciona explicitamente o legítimo interesse de terceiro, mas o art. 10 não.

Erro legislativo ou não, trata-se de um assunto que merece atenção, pois, a depender da interpretação adotada, pode-se chegar a um regime assimétrico para os diferentes atores que fazem uso dessa base legal nas suas operações de tratamento de dados pessoais.

O pesquisador Mário Viola, ao tratar do assunto, afirmou interpretar que o comando do art. 10 dirige-se apenas ao controlador propositalmente porque, ainda que uma situação concreta possibilite a aplicação da base legal para um terceiro, ainda caberá ao controlador avaliar se esse interesse se sustenta frente aos parâmetros estabelecidos pela lei, bem como fornecer acesso aos dados, no caso em que estiverem sob seu domínio. Rielli, complementando a discussão sobre o tema, defendeu que, independente de quem venha a realizar a análise sobre o cabimento da base legal, a melhor interpretação do art. 10, em conjunto com o art. 7º, é que, no caso de ser um terceiro o detentor do interesse analisado, também se apliquem as condições do dispositivo, sob pena de se criar uma assimetria que não encontra justificativa finalística ou sistemática na lei.

O famoso "teste do legítimo interesse" está na própria lei? Como operacionalizá-lo?

Partindo para o próprio conteúdo do art. 10, a doutoranda em direito Paula Pedigoni afirmou, assertivamente, que "o art. 10 coloca uma série de elementos que devem ser, necessariamente, considerados para a decisão sobre a utilização do legítimo interesse" e que "o teste do legítimo interesse deve ser um referencial metodológico para a aplicação desses elementos, é como se fosse uma organização para quem quer fazer isso na prática". Com base em um artigo escrito com Marcela Mattiuzzo, ela sugere o recurso ao teste de proporcionalidade, da tradição constitucional, como uma das formas de operacionalizar essa avaliação.

Alguns motivos para esse "empréstimo" seriam a familiaridade dos Tribunais com o teste e a possibilidade de se ponderar direitos fundamentais. A proposta difere sutilmente do teste organizado por Bioni e descrito no policy paper da Associação, bem como de versões sugeridas por autoridades europeias, como o ICO ou o antigo Working Party 29: ele propõe uma etapa de avaliação da legitimidade do interesse, seguida de uma análise de adequação e uma avaliação da necessidade e, por fim, um balanceamento dos interesses do controlador ou terceiros com a legítima expectativa e os direitos e liberdades do titular. A última etapa, nesse caso, absorveria a análise sobre as salvaguardas do tratamento.

Para Giovanna Carloni, existem modelos já consolidados, como o do ICO, mas não há uma "receita" pronta de teste de legítimo interesse para todos os casos, o que importa é que os elementos do art. 10 sejam contemplados na análise prévia à adoção da base legal. Assim, cada empresa ou órgão público deverá realizar essa avaliação seguindo uma metodologia que se adeque às suas capacidades, recursos e às particularidades do negócio ou atividade e do próprio tratamento de dados pessoais alme-

jado. Algumas possibilidades citadas pela advogada são o emprego de perguntas e respostas ou de sistemas automatizados.

A legítima expectativa do titular é parte estruturante da análise de cabimento do legítimo interesse e deve ser considerada em todos os casos?

Viola, ao tratar da legítima expectativa do titular de dados pessoais, recorreu a uma diferenciação entre tratamentos que integram uma relação de consumo, em que a consideração da expectativa do titular deve ser reforçada, e outros tipos de tratamentos (por exemplo, em situações humanitárias ou de inovação por meio da inteligência artificial), em que pode não ser possível, ou mesmo desejável, dimensionar a legítima expectativa, pela própria natureza de um tratamento em que a relação com o titular seja mais abstrata.

Carloni complementou essa abordagem ao afirmar que, principalmente no segundo caso, é importante lembrar do aspecto da análise de risco que permeia toda aplicação do legítimo interesse: deve-se considerar, sempre, os riscos que um tratamento de dados pessoais pode implicar para um indivíduo ou para a sociedade e diante deles, avaliar quais medidas podem ser tomadas para mitigar esses riscos (ex: anonimização, transparência e opt-out, este último mencionado por Viola). Ainda que não haja uma obrigação legal específica, é comum que empresas empreguem essas salvaguardas como uma medida de *accountability*.

Para Rielli, ainda que, de fato, a relação consumerista seja mais próxima e direta, o que permite uma mensuração mais concreta de legítimas expectativas, esse elemento não deve ser desconsiderado em nenhuma análise de aplicação do legítimo interesse. O que pode ocorrer, na prática, é que o somatório de fatores levados em conta nessa avaliação resulte em uma certa flexibilização da expectativa do titular em favor do interesse em jogo (como a inovação ou a ação humanitária), desde que, evidentemente, não haja prejuízo desproporcional aos direitos e liberdades do indivíduo afetado. Nesse sentido, a pesquisadora ressaltou a necessidade de interpretar os dois incisos do art. 10 da LGPD como, justamente, os dois lados dessa balança.

O teste do legítimo interesse deve ser documentado?

A análise dos elementos do art. 10, que embasa uma decisão sobre o cabimento do legítimo interesse no caso concreto, é obrigatória, embora a sua forma possa variar, conforme concordaram os participantes do debate. Mas, uma dúvida recorrente é se essa análise, ou esse teste, deve ser documentada, e como. Para Paula, a documentação é "altamente recomendada", especialmente em razão do art. 37 da

lei. Ela ressalta que embora a documentação exigida neste dispositivo seja primordialmente descritiva e a documentação do teste do legítimo interesse envolva um importante aspecto valorativo, analítico, ela seria uma das diferentes formas de cumprir com a exigência do artigo, além de uma boa prática.

Quanto ao relatório de impacto à proteção de dados, a pesquisadora opinou que sua realização não é obrigatória, e que isso é coerente com a própria natureza do relatório, deflagrado por situações que envolvam riscos mais elevados aos direitos e titulares de dados pessoais e que "não devem ser banalizadas".

Giovanna Carloni apontou a importância de, mais do que necessariamente documentar o teste em alguns casos, estar pronto para justificar, diante de uma eventual requisição de autoridade, o processo de análise que culminou na decisão de aplicar o legítimo interesse. Em casos "mais complexos", afirmou que é recomendável que o teste seja documentado e, ainda, em casos que envolvam riscos (ou potenciais riscos) maiores, é recomendável a realização de um relatório de impacto. Alertou, por outro lado, para a necessidade de cautela com uma possível "burocratização excessiva" que poderia, inclusive, gerar efeitos contrários aos desejados, como foco excessivo na demonstração formal de conformidade em detrimento de aspectos que exigem, de fato, maior atenção no manuseio da base legal.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- A ANPD ainda não se debruçou especificamente sobre o tema das bases legais, que estão na terceira fase da sua Agenda Regulatória para 2021 e 2022.
- Depois do webinar, que marcou o lançamento do policy paper Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação, a Associação lançou o Jogo do Legítimo Interesse, que gamifica a parte prática do documento, facilitando o consumo.
- Além disso, o paper foi traduzido para o inglês em uma parceria com o Future of Privacy Forum, e lançado em um novo webinar, dessa vez com a participação de Gabriela Zanfir-Fortuna (FPF), Bruno Bioni, Lara Kehoe Hoffman (Netflix), Miriam Wimmer (Autoridade Nacional de Proteção de Dados - ANPD) e Hielke Hijmans (Autoridade Belga de Proteção de Dados). O webinar também gerou um ensaio, que pode ser conferido no blog do Observatório.

Para aprofundar...

- BIONI, Bruno Ricardo; KITAYAMA, Marina; RIELLI, Mariana. Legítimo Interesse na LGPD: quadro geral e exemplos de aplicação. Associação Data Privacy Brasil de Pesquisa. 2021.
- BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma perspectiva informacional. *In*: BIONI, Bruno Ricardo; DONEDA, Danilo; MENDES, Laura Schertel; JUNIOR, Otávio Luiz Rodrigues; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. São Paulo: Editora Forense, 2021. p. 163-177.
- BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Editora Forense. 3.a ed. 2021. p. 238-265.
- MATTIUZZO, Marcela; PONCE, Paula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. **Internet & Sociedade**. v.1 n.2. 2020.
- TROESTER-FALK, Teresa; ZANFIR-FORTUNA, Gabriela. Processing personal data on the basis of legitimate interests under the GDPR: practical cases. Future of Privacy Forum and Nymity. 2018.

SÉRIE LGPD EM MOVIMENTO

OS DIREITOS DOS TITULARES NA LGPD

Webinar realizado no dia 11 de fevereiro de 2021

POR *Júlia Mendonça, Mariana Rielli e Thaís Aguiar*

O sexto webinar da série "LGPD em movimento: temas chave de implementação" teve como tema os direitos dos titulares. Para discuti-lo a partir de perspectivas múltiplas, foram convidadas profissionais de diferentes áreas, formando uma mesa multissetorial. Participaram do debate Bárbara Simão (IDEC), Juliana Domingues (SENACON), Daniela Copetti Cravo (ESDM) e Raíssa Moura (Head Legal Incognia).

Como consideração inicial, Juliana Domingues, Secretária Nacional do Consumidor, afirmou que a análise do tema dos direitos dos titulares deve ser feita com base em diferentes aspectos e sua aplicação deve ser casada entre os órgãos setoriais. Nesse sentido, muitas vezes a implementação desses direitos se dará a partir da atuação conjunta entre, por exemplo, a Autoridade Nacional de Proteção de Dados (ANPD) e a Secretaria Nacional de Direito do Consumidor (SENACON). Outras vezes se dará, por exemplo, entre a ANPD e o Conselho Administrativo de Defesa Econômica (CADE), quando for relacionada a problemáticas que de alguma forma interfiram na concorrência, ou envolvam falhas de mercado, como a assimetria de informações.

Qual o impacto do recente megavazamento de dados de 223 milhões de pessoas para os titulares dos dados pessoais? Quais são os direitos dos titulares frente a um cenário como este?

Raíssa Moura, ao compartilhar sua experiência e visão sobre o tema, observa que, recorrentemente, os titulares dos dados têm receio com relação ao tratamento de dados pessoais, especialmente após os recentes megavazamentos, pois temem que não haja um processo de investigação adequado e nem a devida responsabilização. Diante da situação, aponta Raíssa, observa-se que o titular pode, a partir de meios próprios, requerer a proteção dos seus dados pessoais via judiciário ou via autoridade competente, seja ela a ANPD ou entidades da seara consumerista. No entanto, ela destaca também que,

ainda que haja mecanismos legais para o exercício dos direitos dos titulares, existem poucas instruções sobre como o titular deve realizar os procedimentos na prática.

Ainda tratando sobre os direitos dos titulares, Raíssa apontou que nem sempre a base legal vai ser o único norte para se inferir se há um processamento de dados excessivo. Olhando para os princípios previstos na LGPD, seria possível ter uma ideia do que poderia ser considerado desnecessário ou excessivo, como, por exemplo, pelos princípios da finalidade e necessidade. Se não há uma justificação baseada nos princípios, possivelmente há um tratamento desnecessário e excessivo.

Para Bárbara Simão, o megavazamento mencionado reflete um cenário em que a proteção de dados pessoais não está sendo levada a sério no Brasil, afirmação corroborada com o fato de que, até a data do webinar, nenhuma empresa se manifestou quanto ao vazamento de dados, nem se responsabilizando, tampouco informando quais dados e de que forma foram vazados. Para ela, é importante que haja transparência quanto aos erros cometidos pelas empresas que possivelmente estão envolvidas no caso para que novos episódios sejam prevenidos. Nesse sentido, as autoridades competentes - já que o dever de segurança do titular não advém apenas da Lei Geral de Proteção de Dados, mas também do Código de Defesa do Consumidor - devem agir para a responsabilização e identificação de quais problemas específicos deram força à violação dos direitos dos titulares.

O ônus de um incidente de segurança não pode recair inteiramente sobre o titular, que precisará adotar várias medidas para reduzir eventuais danos, como monitorar o uso dos seus dados ou buscar uma indenização no JEC (o que é custoso e gera um desvio produtivo do consumidor). Retomando o comentário de Moura, Daniela Copetti Cravo afirma, nesse sentido, que a boa-fé objetiva cria o dever de cuidado, ou seja, as empresas teriam um dever adicional de repensar - proativamente - quais cuidados deveriam ser tomados de antemão, previamente a um incidente de segurança. Nesse sentido, o megavazamento pode servir como exemplo para outras empresas que não necessariamente estão envolvidas no caso mas, diante do dever anexo da boa-fé, deverão repensar seus sistemas de segurança, autenticação, etc.

Para Daniela, os ‘‘direitos dos titulares’’ previstos no art. 18 da LGPD não excluem outros direitos, como aqueles decorrentes dos princípios dispostos no artigo 6º da LGPD, do CDC ou outros diplomas. Ainda, há debates na doutrina sobre a natureza das disposições previstas no artigo 18, no sentido de que seriam verdadeiros “remédios” para a promoção da proteção de dados.

Quais são as expectativas para regulação por parte da ANPD e quais as formas de se efetivar os direitos dos titulares, como por exemplo, a portabilidade dos dados?

Juliana Domingues apontou que uma das formas mais efetivas de combate à atividade lesiva ao titular é, de fato, a atuação das autoridades competentes, em especial a ANPD. Essa atuação, no entanto, não deve se restringir à atividade fiscalizadora apenas, mas à uma tríade com monitoramento e educação e empoderamento do consumidor, de modo a combinar um maior controle e poder decisório dos consumidores sobre o tratamento de seus dados, combinado ao estímulo à inovação e à concorrência entre as empresas de tecnologia.

Sobre o aspecto da regulamentação, no entanto, é possível inferir que, no caso da portabilidade dos dados, por exemplo, não há meios efetivos para o exercício desse direito e, portanto, o titular não poderia exigir do controlador dos dados a portabilidade. Para Daniela, a portabilidade dos dados seria um direito muito "à frente" do seu tempo, embora a sociedade e os titulares ainda não tenham percebido os benefícios que podem ser gerados pelo exercício desse direito. A partir do momento que o titular também conceber a portabilidade como uma possibilidade de ter benefício econômico, o seu uso será expandido, mas há um problema relevante quanto à segurança necessária para o exercício dessa prática. Se, por exemplo, não existir um sistema qualificado de autenticação, os incidentes decorrentes de fluxos de portabilidade poderão ser sem precedentes.

Na mesma toada, Daniela afirma que a portabilidade não deve ser restrita apenas ao direito do consumidor, especialmente tendo em vista que o próprio exercício do direito demanda a interligação de diferentes áreas, como por exemplo, dados bancários, dados de saúde, etc. E, nesse sentido, muitas vezes os dados vêm de uma relação de consumo e vão para uma outra relação, não sendo mais possível separar as duas coisas. Diante disso, a finalidade da portabilidade não seria atingida se fosse restrita a uma questão apenas de concorrência ou apenas do consumidor. É por isso que a regulamentação, na visão da pesquisadora, é extremamente necessária para o exercício adequado da portabilidade, a fim de permitir que os titulares atinjam a finalidade almejada e que as empresas cumpram com seus deveres de responsabilidade e segurança.

Do ponto de vista do setor privado, Raíssa Moura apontou que há uma dificuldade de cumprimento dos direitos dos titulares sem a regulamentação adequada. Serão quase dois anos, previstos pela agenda regulatória, em que o setor privado será solicitado pelos titulares para o cumprimento de determinados direitos sem, no entanto, existir uma regulamentação ou diretrizes e boas práticas sobre os temas previstos na Lei. Essa é uma situação que, para Raíssa, traz insegurança jurídica não apenas para os titulares dos dados mas também para as empresas.

O art. 20 da LGPD fala sobre decisões automatizadas e abre a possibilidade de que elas não tenham revisão humana. Qual o impacto disso para os titulares?

Já ao final do webinar, houve espaço para uma reflexão curta sobre essa questão polêmica.

A transparência é um elemento essencial para as decisões automatizadas. A checagem humana, para Juliana Domingues, é determinante para o aditamento, desmistificação dos mecanismos de inteligência artificial e a prevenção de vieses e resultados discriminatórios. Por conseguinte, a decisão automatizada sem revisão humana apresenta um risco maior aos titulares dos dados e não deveria ser possível, especialmente sem a devida transparência.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- A ANPD ainda não se debruçou especificamente sobre o tema dos direitos dos titulares, também previsto para a terceira fase da sua agenda regulatória. Apesar disso, destaca-se que a minuta de regulação sobre a aplicação da LGPD para pequenas e médias empresas, submetida a consulta pública entre setembro e outubro de 2021, incluiu uma previsão de prazo em dobro para estes agentes na resposta a requisições de direitos dos titulares.
- A ANPD avançou nas investigações sobre os megavazamentos de dados, com a colaboração de uma série de outros órgãos federais. Também publicou, em fevereiro de 2021, um texto intitulado "Meus dados vazaram, e agora?", em que apresenta algumas orientações gerais voltadas a cidadãos.
- Na linha de colaboração entre órgãos para a orientação aos cidadãos, muito abordada no webinar, a ANPD e a Senacon lançaram, em setembro de 2021, o guia "Como proteger seus dados pessoais". A publicação ocorreu após a celebração de Acordo de Cooperação Técnica entre os órgãos, em março do mesmo ano.
- Por fim, em outubro de 2021 a ANPD também publicou um Guia de Segurança da Informação para Agentes de Pequeno Porte.

Para aprofundar...

- CUEVA, Ricardo Villas Boas. Proteção de dados pessoais e direito ao esquecimento. *In*: BIONI, Bruno Ricardo; DONEDA, Danilo; MENDES, Laura Schertel; JUNIOR, Otávio Luiz Rodrigues; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. São Paulo: Editora Forense, 2021. p. 627-641.
- CRAVO, Daniela Copetti. Direitos do titular dos dados no Poder Público: análise da portabilidade de dados. **Revista da EDSM**. v.6. n. 11. 2020.
- PONCE, Paula Pedigoni. Direito à portabilidade de dados: entre a proteção de dados e a concorrência. **Revista de Defesa da Concorrência**. v.8 n.1. 2020.
- GOMES, Maria Cecília Oliveira. Novos direitos. **GV EXECUTIVO**, v. 18, n. 4, p. 34-37, 2019.

SÉRIE LGPD EM MOVIMENTO

RESPONSABILIDADE CIVIL NA LGPD

Webinar realizado no dia 25 de março de 2021

POR *Bruno Bioni, Júlia Mendonça, Mariana Rielli e Thaís Aguiar*

Em seu sétimo episódio, a série "LGPD em movimento: temas chave de implementação", trouxe ao debate o tema da responsabilidade civil na LGPD. Novamente em um formato multissetorial e contando com profissionais de diferentes áreas, a discussão foi mediada por Rafael Zanatta (DPBR) e teve como participantes Flávia Lefèvre (Intervozes), Daniel Dias (FGV-Rio), Crisleine Yamaji (FEBRABAN) e Mauro Sobrinho (Secretaria de Governo Digital do Ministério da Economia).

Sobre a dinâmica envolvendo a responsabilidade civil na LGPD, qual é o panorama atual?

Para situar a discussão, Zanatta, diretor da Associação Data Privacy Brasil de Pesquisa, lembrou que o tema específico da responsabilidade civil traz uma série de desafios em decorrência de omissões e escolhas legislativas no texto da LGPD. Na lei, o capítulo é "*sui generis*" quanto ao regime de responsabilidade, pois além de ser curto, do art. 42 ao 45, ele cobre i) o modelo geral de tutela, com regime de responsabilidade solidária (art. 42); ii) a não responsabilização em casos específicos (art. 43); iii) as hipóteses em que o tratamento de dados se torna irregular e ilícito (art. 44) e; iv) diálogo das fontes no caso de violações dos direitos dos titulares no âmbito das relações de consumo (art. 45). Uma leitura completa desse conjunto de dispositivos costuma deflagrar um primeiro questionamento: será que o regime é de responsabilidade subjetiva, objetiva ou "um pouco dos dois"?

Como o tema da responsabilidade civil foi endereçado no debate da LGPD?

É importante relembrar que o modelo adotado pela lei apresenta tão somente a versão final de uma longa etapa de debates no legislativo. Com participação ativa no processo de discussão sobre a

LGPD, Flávia Lefèvre comentou posições em jogo sobre modelos de responsabilidade civil à época da discussão. Já de início, Flávia reconheceu a abertura do Ministério da Justiça para a construção de um espaço de debate profundo e bastante democrático, também chamando atenção para o papel do Comitê Gestor da Internet e de seus Seminários de Privacidade para que a discussão multissetorial da lei pudesse avançar.

Também atenta ao impacto de novas tecnologias, vazamentos de dados e mesmo particularidades do período pandêmico, a representante do terceiro setor apresentou algumas premissas sobre a responsabilidade civil, sustentando que a exploração da atividade econômica de dados pessoais possui riscos intrínsecos. Para ela, isso se dá, primeiramente, devido à atividade em si considerada, e também por existirem previsões no Código de Defesa do Consumidor (CDC). Em vista disso, Flávia defendeu a importância de ser adotada a responsabilidade objetiva do Estado e representantes no trato de questões públicas, considerando que a LGPD se aplica também ao setor público.

Por outro lado, explica que o período de discussão no Legislativo foi marcado por uma forte defesa do setor produtivo à tese de que a responsabilidade deveria advir de culpa. Em sua ótica, essa tensão ficou muito clara na redação dos artigos 42 e 45. Isso porque, aparentemente o legislador quis deixar clara a adoção da responsabilidade objetiva, mas, em outros momentos, parece abrir margem para interpretação diferente, como no caso da última parte do artigo 42, segundo o qual a reparação do dano ocorrerá quando houver "violação à legislação de proteção de dados pessoais". Ainda que os envolvidos no processo de elaboração da lei tenham desejado maior clareza justamente para evitar grandes incongruências, na época, "cada palavra foi disputada" entres os representantes dos setores.

Qual seria a interpretação mais adequada, com base na LGPD, sobre a adoção da responsabilidade objetiva ou subjetiva?

Em que pese certo grau de inconsistência na lei, Flávia apresentou um posicionamento firme no sentido de que existem algumas hipóteses de responsabilidade subjetiva na LGPD, mas que o que prevaleceu - e é evidenciado desde os princípios da lei até à parte específica - é a responsabilidade objetiva. Para fundamentar sua opinião, a advogada destacou que o tratamento de dados pessoais em si é uma atividade de risco e resgatou tanto a teoria do risco como uma contrapartida do princípio da livre iniciativa, quanto a superação da exclusividade da culpa no prisma da responsabilização. Além disso, lembrou que a assunção de riscos por quem explora atividade econômica é a teoria contemplada pelo Código de Defesa do Consumidor e do Código Civil, bem como chamou atenção para incidentes de segurança no Brasil que demonstrariam o risco implícito de atividades de tratamento de dados.

Acrescentou, ainda, que direitos fundamentais convergem com direitos políticos e que a explo-

ração de dados pessoais pode trazer ameaças a direitos de personalidade. Por fim, reafirmou a prevalência da responsabilidade objetiva com base na menção expressa da LGPD à interpretação sistemática com o CDC, na solidariedade entre controlador e operador previstas no art. 42 e também expressões do CDC que aparecem na lei ("serviço", "produto com vícios", art. 44), além de notar que a previsão expressa de danos coletivos também foi outro ponto de tensão no processo de elaboração da LGPD.

Por outro lado, também atenta ao processo de elaboração da LGPD, Crisleine respondeu o ponto trazido por Lefèvre quanto ao risco de atividades econômicas serem um indicativo da natureza da responsabilidade: ora, uma vez que toda atividade econômica apresenta riscos intrínsecos, esse fato, por si só, não pode induzir a uma responsabilidade objetiva. O debate acalorado na fase de projeto da lei levou à retirada da expressão "independentemente de culpa", sinalizador claro da responsabilidade objetiva.

Ao mesmo tempo, o microssistema da LGPD não permitiria falar em responsabilidade subjetiva no sentido tradicional do direito civil, mas sim em uma responsabilidade subjetiva "sui generis", com um espaço de análise de responsabilização por danos em que o critério do "dever de segurança" constitui elemento chave de interpretação. Conclui, de tal forma, que a responsabilidade objetiva prevalece nas referências ao regime consumerista, aplicável a todos os setores produtivos; entretanto, fora das relações de consumo, haveria uma responsabilização subjetiva considerando o cumprimento de deveres de segurança em relação ao tratamento legal.

Existe uma outra saída, para além de buscar a subsunção dos dispositivos da LGPD à responsabilidade subjetiva ou objetiva? Caberia uma discussão sobre um "modelo único"?

Aproveitando que as falas anteriores ilustraram as disputas de construção da lei e dificuldades de interpretação, Daniel Dias trouxe um tom ainda mais provocativo ao debate: apresentando um ponto aprofundado em artigo escrito em conjunto com Bruno Bioni, o professor da FGV Rio propôs uma mudança de perspectiva no foco dado à responsabilidade civil na LGPD, considerando que o debate transmite uma falsa ideia de dualidade, como se apenas existissem dois modelos de responsabilidade civil.

De início e para evitar confusões, Daniel deixou claro que a questão sobre os regimes de responsabilização não parte de uma separação inútil, mas sim que houve um foco extremado nessa divisão, eclipsando outros pontos importantes a serem considerados. É uma separação real, consagrada, mas que, como dito, passa uma falsa ideia de dualidade: na verdade, as responsabilidades incluem diferentes modelos que se encaixam nessas classificações. Um exemplo trazido à mesa pelo professor foi a contraposição entre responsabilidade subjetiva clássica, do art. 186 do Código Civil, e a responsabilidade civil obrigacional pela inexecução das obrigações, do art. 389 e seguintes, ambas modalidades subjetivas, porém distintas. Igualmente, o professor demonstrou que o mesmo ocorre com a responsabilidade obje-

tiva, comentando os exemplos de responsabilidade por fato de terceiro, do produto ou da coisa.

Desta forma, centralizar a discussão na pergunta se a responsabilidade é subjetiva ou objetiva diz pouco e é necessário avançar o debate, inclusive para dirimir as questões a partir do texto disputado da LGPD. Por outro lado, Dias, em referência ao artigo, também critica que o grande foco dado à dicotomia dos modelos de responsabilização levou à popularidade de argumentos *a priori*, no sentido de que não partem do texto legal, mas sim remetem ao histórico do processo legislativo ou à natureza (de risco ou não) da atividade. Por mais relevantes que sejam esses pontos, a abordagem *a priori* ainda seria incapaz de responder o que a lei diz, por tentar trazer soluções desde uma perspectiva externa ao texto legal.

A saída proposta pelo professor, portanto, é ir a campo no texto normativo, "sujar as mãos" quanto ao que a lei diz. Ocorre que ainda não se encontrou - e ao que tudo indica, na verdade, não há - uma linha condutora que dê sentido a todos os artigos referentes ao tema. Nesse ponto, a LGPD reflete de forma evidente a disputa de forças legislativas, que resultou em um texto "truncado" - às vezes ambíguo, às vezes com sobreposições. Assim, diante da provável impossibilidade de se chegar a uma linha condutora que expresse o texto em sua literalidade e exclua qualquer controvérsia ou contradição no capítulo de responsabilidade civil, "é preciso um jogo de cintura" no esforço por coerência do regime jurídico, reitera o professor.

O primeiro ponto relevante em tal construção, segundo ele, é reconhecer duas hipóteses de responsabilidades: de um lado, a responsabilidade pela violação ou inobservância da legislação de proteção de dados e, de outro, a violação da segurança dos dados. Explica, em continuidade, que o art. 42 dá a entender que a violação da legislação é o único critério; entretanto, o art. 44 e seguintes sugerem a violação de segurança como parâmetro de responsabilização, o que também aparece em outras passagens da LGPD. Novamente afastando ambiguidades, Daniel reitera que se tratam de duas hipóteses de ilicitude dentro de um modelo unitário de responsabilização, em lugar da dicotomia de responsabilidade objetiva e subjetiva.

Indo além, o professor completou que o segundo achado a partir da leitura dos dispositivos legais é que é preciso também uma análise das circunstâncias especiais, ilustradas no rol exemplificativo do art. 44. A não adoção de medidas de segurança, por exemplo, é um critério muito amplo, e o importante seria identificar o comportamento exigível - ponto que sustentou citando circunstâncias concretas e a leitura conjunta de dispositivos da lei. Ainda, concluiu que percebe na lei um juízo de responsabilidade civil subjetiva, de modo geral; no entanto, a grande preocupação da legislação é a segurança do titular e a prevenção de danos, dedicando a parte final de sua fala a questões de ônus da prova, outros agentes no tratamento de dados e relações de consumo.

Especificamente tratando sobre o setor público e suas peculiaridades, como encarar a responsabilidade civil por danos a titulares de dados?

Mauro Sobrinho, da Secretaria de Governo Digital do Ministério da Economia, apresentou sua percepção como gestor público na linha de frente da estratégia de transformação digital do Governo Federal para explicar a dinâmica da responsabilidade do poder público e a possibilidade de responsabilização pessoal de servidores.

Compartilhando sua experiência, Mauro notou que, em muitos órgãos, há uma série de medos no trabalho de conformidade com a LGPD. Primeiramente, há muitos servidores que não sabem o que fazer ou como fazer - o que leva, inevitavelmente, a receios quanto à responsabilização. De qualquer forma, o Diretor do Departamento de Governança de Dados e Informações da Secretaria de Governo Digital foi firme ao indicar que um gestor público pode, sim, ser eventualmente responsabilizado por violações à LGPD, quando enquadrado como agente na cadeia de tratamento de dados. Mauro comentou a tríplice responsabilidade que recai sobre servidores no exercício de suas funções - penal, civil e administrativa - e aprofundou comentários sobre experiências práticas e receios que percebia em reuniões.

Diante de tais inseguranças, Mauro indicou a estratégia de dar mais atenção ao artigo 43, que exime os agentes ao agirem da forma correta - um caminho que pode orientar melhor processos decisórios. Lembrou, ainda, que "o Governo Federal é o maior custodiante de dados", uma percepção que pode ser extrapolada para outros poderes e que apenas reitera a grande responsabilidade envolvida e a importância de que os processos façam o devido tratamento desses dados - por isso, a necessária atenção a cada etapa no ciclo de vida dos dados, outro tema que foi evidente em sua fala.

Por outro lado, o diretor da Secretaria de Governo Digital também chamou atenção para incidentes de segurança recém ocorridos no país e estratégias de mitigação de risco. Após ter comentado investigações nas quais teve papel ativo na recuperação de incidentes, pontuou doses de realismo necessárias para uma atuação efetiva nesse sentido: por exemplo, em que pesem as determinações da lei no art. 43, a ocorrência de um incidente de segurança é praticamente uma questão de tempo, pois mesmo o conhecimento das ameaças não tem o condão de evitar sua concretização, assim como os próprios remédios aplicáveis têm suas limitações. De tal forma, o papel central da Secretaria do Governo Digital é garantir os controles adequados de segurança e privacidade para que as melhores práticas sejam aplicadas.

Não menos importante, conjugando suas atribuições com o reconhecimento das inseguranças entre servidores públicos, a Secretaria de Governo Digital elaborou uma série de guias orientativos para apresentar aos gestores públicos um conjunto de boas práticas para o dia a dia. Direcionados a gestores no setor público, os documentos abordam, entre outras questões, como realizar o tratamento de dados de forma adequada, compreender como fazer um inventário de dados, aplicar princípios e preparar-se

para enfrentar incidentes de segurança. Ainda, a Secretaria criou metodologias práticas de avaliação de risco de segurança e privacidade, bem como criou ferramentas para aplicar esses conhecimentos e mais recursos para auxiliar servidores públicos no exercício de suas funções, em conformidade com as diretrizes da LGPD.

Por fim, os painelistas fizeram as suas respectivas considerações finais, com abertura para perguntas do público. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- Desde o webinar, muitos textos, desde artigos de opinião em veículos jurídicos até livros sobre o tema, foram publicados, tendo se mantido aberta a discussão.
- No Judiciário também não é possível, ainda, observar homogeneidade nas decisões que já aplicaram a LGPD: segundo levantamento do Jota, em agosto de 2021 era possível identificar julgados em sentidos diversos acerca do caso dos vazamentos de dados, por exemplo, e se eles geram o dever de indenizar com presunção da ocorrência de dano.

Para aprofundar...

- BIONI, B. R.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com - Revista Eletrônica de Direito Civil**, v. 14, p. 1-23, 2020.
- SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: BIONI, Bruno Ricardo; DONEDA, Danilo; MENDES, Laura Schertel; JUNIOR, Otávio Luiz Rodrigues; SARLET, Ingo Wolfgang. **Tratado de Proteção de Dados Pessoais**. São Paulo: Editora Forense, 2021. p. 319-339.
- GUEDES, Gisela Sampaio da Cruz. Regime de responsabilidade adotado pela lei de proteção de dados brasileira. **Caderno especial LGPD**, p. 167-182. São Paulo: Revista dos Tribunais, nov. 2019.
- BODIN DE MORAES, M. C. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica.com**, v. 8, n. 3, p. 1-6, 15 dez. 2019.

SÉRIE LGPD EM MOVIMENTO

LGPD E RELATÓRIOS DE IMPACTO À PROTEÇÃO DE DADOS

Webinar realizado no dia 28 de maio de 2021

POR *Júlia Mendonça e Mariana Rielli*

No dia 28 de maio, foi realizado mais um Webinar da série "LGPD em movimento: temas chave de implementação", como parte da "Semana do Relatório de Impacto", que foi composta por dois encontros. O primeiro contou com a participação do Professor Dariuzs Kloza para uma *masterclass* ao vivo sobre o tema "Data Protection Impact Assessment na Europa", moderada pela professora Maria Cecília Oliveira Gomes. O segundo encontro, objeto do presente ensaio, contou com a participação de Maria Cecília Oliveira Gomes (USP), Paula Zanona (Neoway), Victor Cravo (Procurador Federal - AGU) e Marcelo Morandini (EACH - USP), que foram recebidos por Mariana Rielli (Associação Data Privacy Brasil de Pesquisa) para debater a fundo questões envolvendo relatório de impacto (RIPD), LGPD e a atuação da ANPD.

O debate foi dividido em dois ciclos de perguntas e provocações feitas para cada convidado, incluindo questionamentos enviados pela audiência.

O que é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)? Como o Brasil está situado atualmente na discussão sobre o tema e quais serão os principais desafios regulatórios a serem enfrentados?

No primeiro ciclo de debate, Maria Cecília O. Gomes, definiu, de forma detalhada, em que consiste o relatório de impacto, identificando-o como uma documentação do controlador que é utilizada para identificar os riscos às liberdades civis e direitos fundamentais dos titulares (Art. 5º, XVII LGPD), com o objetivo de mitigá-los. Aprofundando a discussão, Cecília fez uma análise do sistema regulatório de proteção de dados brasileiro e apontou a necessidade de uma maior proatividade por parte dos controladores, tendo em vista que o relatório em si é uma ferramenta fundamental não só para mitigar os riscos, mas também para preveni-los. Conforme apontado por ela, a regulação de risco, que serviu de

inspiração para vários modelos normativos de proteção de dados em outros países, possui uma racionalidade voltada à prevenção aos riscos, que implica, inclusive, a elaboração do relatório de impacto antes de algum produto ou serviço ser disponibilizado no mercado.

Ao passar para análise dos desafios regulatórios que a ANPD virá a enfrentar quanto ao tema, citando um texto de sua autoria publicado no JOTA, ela apontou os 4 principais pontos: a conceituação do que seria efetivamente o relatório de impacto, bem como a sua função e objetivos; a compreensão de "risco" no tocante à proteção de dados pessoais junto à bagagem regulatória preexistente envolvida e quais os momentos de exigibilidade do relatório, ou seja, se ele seria obrigatório ou não com relação a determinados tipos de tratamentos.

Por sua vez, Paula Zanona trouxe sua experiência prática no setor privado, especificamente em uma empresa cujo modelo de negócio é baseado na exploração de big data. Ressaltou que os controladores no Brasil atualmente não possuem diretrizes específicas sobre o tema, o que gera a necessidade de uma postura proativa, buscando referências e metodologias sobre relatórios de impacto oriundas de outras Autoridades de Proteção de Dados no mundo. Diferente do Teste de Legítimo Interesse (LIA), que já dispõe de algumas diretrizes postas na LGPD, ainda não existem orientações padronizadas no tocante ao relatório de impacto.

Quanto à governança de dados, a advogada destacou que é insuficiente que o dado seja "apenas" coletado licitamente, sendo imprescindível que todos os outros requisitos e princípios da lei sejam cumpridos, como, por exemplo, que seja possível garantir a qualidade dos dados. Por fim, Paula ressaltou que, frente a outros documentos, ainda que cada um possua uma função diversa, o relatório de impacto tem um caráter mais "delicado", tendo em vista a sua complexidade e que, conforme já destacado, ainda não existem diretrizes claras sobre o seu conteúdo.

Como funciona a dinâmica envolvendo o Relatório de Impacto à Proteção de Dados Pessoais para o setor público?

Trazendo o debate sobre o relatório de impacto para o setor público, Victor Cravo constatou que, caso o relatório venha a não ser obrigatório, ainda assim será necessária a realização de algum tipo de documentação por entidades públicas, mesmo que apenas para controle interno. Isso porque, conforme apontado pelo procurador, a elaboração de um relatório possibilita que o ente faça o mapeamento de que tipo de dados são tratados, como são tratados e outros detalhes, ainda que não seja necessária a sua apresentação a atores externos. Ainda dentro dessa perspectiva, ele apontou que essa análise também será feita com base na gestão e organização específica de cada ente, dentro das boas práticas gerais a serem implementadas.

Em um sentido mais geral, Victor observou a necessidade urgente de uma mudança de paradigma dentro dos órgãos públicos, com a implementação e consolidação de uma cultura de proteção de dados, de forma a colocar o cidadão como o ponto central de decisão com relação aos dados pessoais. Isso porque, ele observa, a visão geral ainda é de que o Estado sempre faz o uso dos dados abarcado pelo "interesse público", o que já seria uma "finalidade" e justificativa viável para o tratamento.

Como funciona a dinâmica envolvendo o Relatório de Impacto à Proteção de Dados Pessoais para o setor público?

Iniciando o segundo ciclo de debates, Maria Cecília apontou que muitas das regulações de proteção de dados no mundo foram influenciadas pela ideia de "regulação de risco", a qual tem sua origem no direito ambiental, com a concepção de "prevenção" característica do setor. Citando Peter Bernstein, Cecília aponta que o risco seria a capacidade de "definir o que pode acontecer no futuro e escolher entre alternativas", frisando que o risco não é necessariamente algo "ruim" ou de caráter meramente dualista, que pode ser classificado como "positivo ou negativo". Nesse sentido, ela aponta que, na verdade, o risco é um fator inerente a todas as atividades de tratamento de dados, ou seja, diferente da figura do "dano", ele vai sempre existir.

De uma perspectiva autoral, a pesquisadora apontou que a forma como o risco será trabalhado em operações de tratamento depende da metodologia aplicada, e que é imprescindível ter clareza de que o referencial deve ser sempre o próprio titular dos dados, de modo que o documento final possa mensurar os riscos para as liberdades individuais, e não o risco regulatório da empresa ou órgão.

Ainda tratando sobre abordagem metodológica, Cecília menciona que todas as Autoridades de Proteção de Dados da Europa precisam seguir a lógica do risk based approach, que é uma das metodologias existentes para relatórios de impacto. O que não significa a existência de modelos prontos, ou seja, cada Autoridade precisa desenvolver o seu modelo "template" com base nessa metodologia. No entanto o risk based approach não é a única possibilidade, visto que existem metodologias baseadas em direitos, baseadas em riscos e benefícios, entre outras, o que, para ela, culmina na necessidade de se compreender qual seria a mais adequada ao contexto brasileiro.

Ao tratar sobre o Guia de Boas Práticas da LGPD publicado pelo Governo Federal, Victor Cravo, enquanto participante da equipe técnica de elaboração, apontou que um dos pontos estabelecidos foi de que o documento deveria ser abrangente, fazendo a ressalva de que eventuais preenchimentos de lacunas e interpretações diante dos casos concretos surgiriam em seguida, com atualizações recorrentes. Retomando a discussão sobre diretrizes metodológicas para o RIPD, Victor afirmou que a metodologia adotada no texto para o Guia - baseada em risco - foi a identificada como a mais recorrente no cenário

internacional, além de, em tese, ser a mais simples no momento de implementação.

Durante a elaboração de um relatório de impacto, Victor destacou a necessidade de ouvir também os interessados, ou seja, os titulares de dados, o que, dentro do setor público, poderia ser materializado por meio de mecanismos participativos Sobre o cabimento da publicização do RIPD, o procurador opinou positivamente, destacando a importância de dar publicidade ao documento inclusive para possibilitar uma maior participação dos titulares.

Sobre essa mesma discussão, Paula Zanona frisou o impacto que a publicização pode causar às empresas no tocante ao segredo de negócio, considerando que os relatórios normalmente não são só jurídicos, mas eminentemente técnicos, contendo detalhes sobre algoritmos, fontes e minúcias comerciais extremamente relevantes para o setor privado. Considerando que ainda não existe um veredicto, Paula opinou que não vê problemas na publicização, desde que respeitado o segredo do negócio, destacando que uma saída para o setor privado também é a transparência nas políticas de tratamento, com o objetivo maior de garantir sempre a proteção dos direitos dos titulares.

Como reação aos comentários de Victor e Paula, Cecília sintetizou a discussão e ressaltou que a lógica para o setor privado e para o setor público é diferente, já que para o último existe uma extensa previsão de regras de transparência, enquanto para àquele há as mencionadas previsões de segredo de negócio.

Fornecendo um exemplo de boas práticas no setor público, Cecília destacou um caso do sistema de saúde do Reino Unido, que desenvolveu um aplicativo de *contact tracing* com o objetivo de rastrear e mapear o contágio pela COVID-19. Na oportunidade, o relatório de impacto respectivo foi publicizado antes do lançamento do aplicativo, com o objetivo de receber comentários públicos, tendo uma parte deles sido posteriormente implementada antes do efetivo lançamento do aplicativo. No caso do setor privado, ela afirmou que também é preciso pensar na publicização dos relatórios, observado o segredo de negócio e tentando buscar um equilíbrio entre perspectivas setoriais diferentes.

O artigo 38 da LGPD diz que a ANPD poderá determinar ao controlador que elabore Relatório de Impacto à Proteção de Dados Pessoais sobre suas operações de tratamento, mas não o impõe como uma obrigatoriedade. Dessa forma, em quais situações a ANPD deverá exigir o RIPD?

Quanto às situações de exigibilidade do RIPD, é necessário que a análise seja feita não apenas tendo como referencial o tamanho da empresa, ou o porte econômico, mas sim identificando qual é seu respectivo modelo de negócio, conforme destacou Paula Zanona. Isso porque, segundo Paula, uma

PME ou uma *startup*, mesmo com poucos funcionários, pode ter um core que implique um tratamento massivo de dados, tornando essencial a elaboração do relatório. Ainda nesse sentido, ela apontou que várias empresas, mesmo ainda sem as diretrizes específicas da ANPD terem sido emitidas, estão tendo uma postura proativa para desenvolver os seus relatórios, e aquelas que não o fazem acabam perdendo competitividade no mercado.

Os riscos de proteção de dados pessoais também estão relacionados à experiência do titular no ambiente digital. Nesse sentido, como mitigá-los a partir do foco na experiência do usuário?

A partir de uma perspectiva da engenharia de software, o convidado Marcelo Morandini apontou para a necessidade de mitigação de riscos envolvidos na experiência do usuário (*user experience*), além de jogar luz para a cuidado que alguns desenvolvedores devem ter na escolha de quais dados serão disponibilizados em seus produtos. Nesse sentido, o professor citou o exemplo de um aplicativo que possuía como escopo o fornecimento de localizações e trajetos, o que ocasionou a publicização de informações de caráter sigiloso sobre assuntos militares, destacando o quanto isso pode ser nocivo. Retomando a discussão sobre a *user experience*, o professor concluiu pela necessidade de uma maior acessibilidade da linguagem jurídica não só para outras áreas que terão contato com o relatório de impacto, mas também para o público em geral.

Por fim, as considerações finais do painel entre os expositores focaram em olhares futuros e expectativas sobre como a figura do relatório de impacto será absorvida, analisada e implementada no contexto brasileiro. Para mais detalhes, a discussão completa pode ser acessada no canal do Youtube do Data Privacy Brasil, por meio deste link.

De lá pra cá...

- Alguns dias após o webinar, a ANPD divulgou seu cronograma de Reuniões Técnicas sobre o tema de Relatórios de Impacto à Proteção de Dados. A painelista participou dos debates, que foram transmitidos pelo Youtube.
- Um texto analítico sobre esse processo, que também resume os três dias de Reuniões Técnicas, foi publicado no Jota por membros da Associação Data Privacy Brasil de Pesquisa.

Para aprofundar...

- BIONI, Bruno. LUCIANO, Maria. O Princípio da Precaução para a Regulação da Inteligência Artificial: Seriam as Leis de Proteção de Dados seu Portal de Entrada? *In:* Frazão, A. Mulholland, C. (Coord.) **Inteligência Artificial e Direito**, Revista dos Tribunais, 2019.
- GOMES, Maria Cecília Oliveira. Relatório de Impacto a Proteção de Dados. Uma breve análise da sua definição e papel na LGPD. **Revista dos Advogados de São Paulo**. N. 144. 2019.
- GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In:* PALHARES, Felipe (Coord.). **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.
- Dariusz Kloza, Niels van Dijk, Simone Casiraghi, Sergi Vazquez Maymir, Sara Roda, Alessia Tanas and Ioulia Konstantinou (2019). Em direção a um método para avaliações de impacto sobre a proteção de dados: entendendo as exigências do RGPD. *d.pia.lab Documento de Política* n.o 1/2019. VUB: Bruxelas.
- Dariusz Kloza, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017). Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos. *d.pia.lab Documento de Política* n.o 1/2017. VUB: Bruxelas.