Rony Vainzof: LGPD e relatÃ³rio de impacto Ã proteÃ§Ã£o de dados

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) é baseada na avaliação de riscos, postura dos regulados e responsabilização e prestação de contas, visando inserir o indivíduo na sua legítima posição de titular/proprietário dos seus dados e, portanto, com direito de administrá-los, o que foi certeiramente positivado na Lei como fundamento da autodeterminação informativa, já reconhecida em 2020 pelo Supremo Tribunal Federal como consignada dentro de outros direitos e garantias fundamentais da Constituição Federal, no julgamento que anulou a Medida Provisória 954/20 [1].

Aliás, esse *leading* case brasileiro, que se equipara ao paradigmático julgamento do Censo da Alemanha de 1983 [2], abordou também justamente o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), vez que a MP anulada pelo STF previa a elaboração deste importante instrumento, mas posteriormente a transferência dos milhões de dados de clientes das operadoras de telecomunicações ao IBGE. Na ocasião, o STF ressaltou que *"a confecção de RIPD dos consumidores não pode ser feito a destempo, depois de já compartilhados e ocorridos eventuais abusos, pois assim, seria tarde demais para que fosse* *slação e como foi impactado o regime de proteção de dados".*

O RIPD, como todas as avaliações de riscos que pautam a

LGPD, são focadas, corretamente, nos direitos dos indivíduos. Tanto é assim que: 1) o conceito do RIPD prevê a elaboração deste instrumento quando as atividades puderem gerar *"riscos às liberdades civis e aos direitos fundamentais"* (artigo 5º, XVII); e 2) dentre as competências da ANPD, está a de regulamentar o RIPD para os casos em que o tratamento represente *"alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na lei"* (artigo 55-J, XIII).

Portanto, estamos aqui diante de uma abordagem normativa também baseada em direitos e não somente em riscos regulatórios.

E como dado é a moeda da economia digital e a LGPD é um *"mapa"* a ser seguido pelas organizações para o uso ético, responsável e seguro dos dados, cumprir a lei vai muito além de mitigar sanções e responsabilidades. É uma questão de competividade, reputação e cumprimento de direitos fundamentais. Afinal, como indivíduos, cada vez mais somente confiaremos nossos dados a quem respeita nossos direitos.

Dito isso, uma vez que os regulamentos da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) devem ser precedidos também de análises de impacto regulatório (artigo 55-J. § 2º), importante medir e avaliar em quais circunstâncias os esforços para a realização do RIPD, como tempo e custo, são proporcionais a proteção contra violações a direitos e garantias individuais, identificação e gerenciamento de riscos e segurança a serem descobertos na condução do instrumento em discussão.

Em 2012, a Comissão Europeia publicou sua análise de Impacto Regulatório do *General Data Protection Regulation* (GDPR) [3]. Acerca do *Data Protection Impact Assessment* (DPIA), identificou o seguinte:

1) A necessidade de critérios para aplicabilidade precisamente definidos para garantir que a sua obrigatoriedade não seja desproporcionalmente ampla;

2) Que os custos dependem de critérios variáveis, como tamanho da organização e quão significativos são os impactos de proteção de dados de uma nova tecnologia, serviço ou produto;

3) A estimativa de custo de um DPIA

3.1) Baixa complexidade: €14,000;

3.2) Média complexidade: €34,500;

3.3) Alta complexidade: €149,000.

4) Preocupação do setor privado com os custos associados aos DPIAs obrigatórios;

5) Preferência por muito dos entrevistados de um DPIA voluntário ou flexível, que fornecesse incentivos e que fossem encorajados pelas autoridades nacionais.

O que se consolidou nas normas da UE foi o seguinte:

1) GDPR (artigo 35, 3º): rol exemplificativo de circunstâncias que levam o tratamento ao alto risco, que é o gatilho para a elaboração do DPIA [4];

2) Article 29 Working Party (WP29)/European Data Protection Board (EDPB) [5]: estabelece nove critérios e ao menos dois deles necessários para que o DPIA seja realizado [6]. Quanto mais critérios forem satisfeitos, maior será a probabilidade de o tratamento implicar em elevado risco e, portando, necessitar de um DPIA.

3) Autoridades: obrigação de elaborar e publicar lista dos tipos de operações de tratamento sujeitos ao DPIA (artigo 35,4º). Podem também elaborar e tornar pública lista de tratamento em que o DPIA não é obrigatório (artigo 35,5º);

4) Pareceres do EDPB acerca das referidas listas [7].

Nos EUA, diferentemente, o denominado *Privacy Impact Assessment* não é previsto em leis federais para o setor privado, sendo somente obrigatório em algumas circunstâncias para órgãos da administração pública.

Superado os fundamentos acima, passamos às perguntas formuladas pela ANPD em reunião técnica realizada também com a minha participação no dia 23/06/21, sobre *"situações/circunstâncias que ensejam a necessidade ou dispensa de elaboração de relatório de impacto"* [8]:

De quem a ANPD deverá solicitar a elaboração do RIPD? Quais são as exceções?
Somente junto aos controladores, quando o tratamento apresentar alto risco, de acordo com parâmetros previamente estabelecidos pela ANPD para realização do cálculo do risco, como explicarei posteriormente.

Se houver utilização parcial ou total de um operador, este deve prestar assistência ao controlador para execução do RIPD, devendo prover todas as informações necessárias sem as quais o objetivo do procedimento poderia ser prejudicado. No GDPR há expressa previsão legal da obrigação acima. Já a LGPD é omissa.

Sobre o Encarregado (Data Protection Officer), idealmente suas funções no RIPD serão as seguintes:

1) Avaliar quando a organização deve ou não realizar o RIPD;

2) Opinar sobre a metodologia a ser utilizada no RIPD e se deve ser realizado interna ou externamente;

3) Esclarecer quais as salvaguardas (incluindo medidas técnicas e administrativas) a serem aplicadas para atenuar os eventuais riscos para os direitos e interesses dos titulares de dados;

4) Dar parecer acerca do RIPD, se a avaliação de impacto foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com a legislação.

Quais são as circunstâncias que devem estar presentes para que um RIPD seja recomendável?
Recomendo que o RIPD seja voluntário ou quando a atividade de tratamento apresentar alto risco, de acordo com parâmetros previamente estabelecidos pela ANPD para realização do cálculo do risco, como:

1) Envolver dados sensíveis;

2) Envolver dados pessoais relacionados a condenações criminais;

3) Envolver dados financeiros, incluindo status social;

4) Envolver dados de vulneráveis;

5) Envolver geolozalicação;

6) For capaz de afetar sensivelmente a segurança pessoal do indivíduo ou sua integridade física/psíquica;

7) De acordo com o volume de dados: a) número de titulares envolvidos, seja por meio de um número específico, ou por meio de percentual da população pertinente; b) do volume de dados e/ou a diversidade de dados diferentes tratados; c) da duração da atividade de tratamento de dados ou a sua pertinência; d) da dimensão geográfica da atividade de tratamento;

8) Avaliação ou classificação dos titulares, incluindo definição de perfis e análise preditiva;

9) Decisões automatizadas que produzam efeitos jurídicos ao titular ou o afetem significativamente, como o tratamento que possa implicar a exclusão ou a discriminação de indivíduos;

10) Tratamento dos dados empeça os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato;

11) Controle sistemático, utilizado para observar, monitorar ou controlar os titulares dos dados;

12) Estabelecer correspondências ou combinar conjuntos de dados com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes controladores;

13) Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais.

Ou seja, os parâmetros acima serviriam para que as respectivas organizações conduzam seu cálculo de risco, por meio de metodologias próprias, seguindo boas práticas e de acordo com as especificidades de cada setor. Caso o cálculo resulte em alto risco, a organização realizaria o RIPD. Se for baixo ou médio, não.

O cálculo de risco não seria elaborado para qualquer atividade de tratamento, mas somente para aquelas que contemplarem algum dos parâmetros previstos pela ANPD.

As metodologias de cálculo de risco, individualmente ou por meio de associações, poderiam ser levadas à ANPD para reconhecimento (autorregulação regulada).

A ANPD avaliaria, quando solicitado por ela o RIPD, cada caso concreto, gerando precedentes acerca da coerência ou não dos critérios utilizados pela respectiva organização.

Há alguma hipótese em que o relatório de impacto de proteção de dados deveria ser obrigatório? Se sim, qual(is)?
Visando gerar maior segurança jurídica, a ANPD poderia elencar um rol enxuto exemplificativo de atividades de tratamento que representam, diretamente, alto risco, como:

1) Dados biométricos ou genéticos de titulares vulneráveis ou utilizados para decisões automatizadas;

2) Alto volume de dados sensíveis;

3) Alto volume de dados em espaços públicos;

4) Uso de inteligência artificial para processar dados pessoais para controlar a interação com o titular dos dados ou para avaliar aspectos pessoais do titular.

E quando o RPID pode ser dispensado?
1) Sempre que o cálculo de risco for baixo ou médio;

2) No caso de cumprimento de obrigação legal ou regulatória;

3) Quando a natureza, o escopo, o contexto e os objetivos do processamento são muito semelhantes ao processamento para o qual um RIPD já foi realizado;

4) Tratamento de dados por startups (Marco Legal das Startups) e pequenas empresas (LC 123/2006) para fins de RH e desde que não seja utilizada a definição de perfis;

5) Realizado por associação, fundação ou qualquer outra instituição sem fins lucrativos para a gestão dos seus membros e doadores no âmbito das suas atividades normais, desde que os dados não envolvam dados sensíveis;

6) Tratamento por pessoa física no exercício das suas funções profissionais, especialmente médicos, profissionais de saúde ou advogados;

7) Para gestão de controle de acesso e horários para jornada laboral, com exceção de dados biométricos e desde que o tratamento não revele dados sensíveis.

Essas circunstâncias devem ser as mesmas consideradas para fins de cumprimento da obrigação do artigo 4º, §3º, da LGPD? Se não, quais aspectos devem ser considerados?
Os parâmetros para o critério de risco podem ser distintos.

Seria possível a criação de um rol taxativo de obrigatoriedade de elaboração do RIPD? E a criação de um rol taxativo de dispensa?Não indico, pelos motivos já expostos.

Por fim, visando a avaliação de impacto regulatório, sugiro a realização pela ANPD de pesquisa junto aos órgãos públicos e ao setor privado visando entender:

1) Qual o custo e esforço para realização do RIPD de baixa, média e alta complexidade?

2) Em termos de segurança jurídica, é mais adequado um rol de atividades que exigem RIPD ou parâmetros para cálculo de risco das atividades de tratamento?

Assim, o modelo ora defendido proporcionaria uma regulação dinâmica, com constante atualização, bem como possibilitando a criação de parâmetros setoriais, em conjunto com outras entidades reguladoras e os próprios regulados.

[1] Supremo Tribunal Federal. Disponível em http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&tip=UN. Acessado em 23/06/21.

[2] Sobre o assunto, recomendo a leitura do artigo de minha autoria *"Um novo marco histórico de Proteção de Dados Pessoais no Brasil – Julgamento da MP 954/20 no STF"*. Disponível em https://www.linkedin.com/pulse/um-novo-marco-hist%C3%B3rico-de-prote%C3%A7%C3%A3o-dados-pessoais-brasil-vainzof/. Acessado em 23/06/21.

[3] Comissão Europeia. Avaliação de Impacto do GDPR. 2012. Disponível em <https ://www europarl europa eu/cmsdata/ 59702 / 20130508 ATT 65856 1873079025799224642 pdf>. Acesso 23/6/21.

[4] O artigo 35º, nº 3, do GDPR, prevê alguns exemplos de quando é que uma operação de tratamento é «suscetível de implicar elevados riscos»:

– a) Avaliação sistemática, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

– b) Operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações; ou

c) Controlo sistemático de zonas acessíveis ao público em grande escala».

[5] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Disponível em https://ec.europa.eu/newsroom/article29/items/611236. Acessado em 23/06/21.

[6] As operações de tratamento «suscetível de implicar um elevado risco»14, devem ser considerados os seguintes nove critérios:

Avaliação ou classificação, incluindo definição de perfis e previsão;

Decisões automatizadas que produzam efeitos jurídicos ao titular ou o afetem significativamente;

Controle sistemático, utilizado para observar, monitorar ou controlar os titulares dos dados;

Dados sensíveis ou dados de natureza altamente pessoal, bem como dados pessoais relacionados a condenações penais e infrações.

Dados tratados em grande escala, por meio da avaliação: 1) do número de titulares de dados envolvidos, quer por meio de um número específico, quer por meio de percentual da população pertinente; 2) do volume de dados e/ou a diversidade de dados diferentes tratados; 3) da duração da atividade de tratamento de dados ou a sua pertinência; 4) da dimensão geográfica da atividade de tratamento;

Estabelecer correspondências ou combinar conjuntos de dados: com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes controladores de tal forma que excedam as expectativas razoáveis do titular;

Dados relativos a titulares vulneráveis;

Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais;

Quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato.

[7] EDPB. Disponível em: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en?f%5B0%5D=opinions_topics%3A138. Acessado em 23/6/21.

[8] O inteiro teor dos debates pode ser acessado em https://www.youtube.com/watch?v=ClB-gXhhoE4. Acessado em 23/6/21.