LEI GERAL DE PROTEÇÃO DE DADOS | LGPD

ENUNCIADOS PARA AUXILIAR NA GARANTIA DA SEGURANÇA JURÍDICA

O aprimoramento da segurança jurídica na interpretação e na aplicação da Lei Geral de Proteção de Dados (LGPD – 13.709/2018) é a proposta central desta publicação. A fim de auxiliar a sociedade na busca por um ambiente digital mais sustentável, reunimos situações-problema vivenciadas por operadores do Direito conhecedores dos vários aspectos envolvidos no debate sobre a privacidade e proteção de dados. Os enunciados estão divididos em eixos temáticos que compõem a legislação: princípios; aplicação das bases legais para dados pessoais e dados pessoais sensíveis; bases legais para transferência internacional de dados; direitos dos titulares; sujeitos da LGPD; segurança da informação; governança; responsabilidade civil dos agentes de tratamento; sanções administrativas e atribuições da ANPD; Inteligência Artificial (IA) e tratamento automatizado de dados; e regulamentação complementar de proteção de dados pessoais.

LEI GERAL DE PROTEÇÃO DE DADOS | LGPD

ENUNCIADOS PARA AUXILIAR NA GARANTIA DA SEGURANÇA JURÍDICA

UM AMBIENTE DIGITAL ÉTICO E SEGURO

A rotina do mundo contemporâneo é, cada vez mais, permeada por dados que podem ser classificados, armazenados e usados por cidadãos, empresas e Poder Público. Ainda que a Lei Geral de Proteção de Dados (LGPD – 13.709/2018) tenha como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade das pessoas, eventuais incidentes ou tratamento de dados ilícitos podem sujeitar às organizações responsabilidade civil e sanções administrativas.

Por esta razão – e com o propósito de auxiliar a sociedade em relação aos diversos aspectos compreendidos pela LGPD –, esta publicação reúne enunciados que versam sobre os princípios e a aplicação da lei. Em outras palavras, são situações-problema vivenciadas e analisadas por magistrados, advogados, acadêmicos e especialistas interessados em um ambiente digital mais sustentável.

A formulação deste material foi possível graças à atuação de uma Comissão Científica formada especificamente para este trabalho, além da coordenação da Federação do

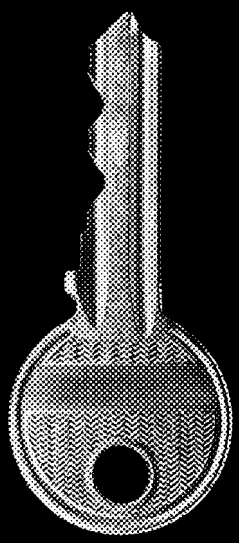
Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FecomercioSP).

Nas páginas a seguir, os enunciados estão divididos em eixos temáticos que compõem a Lei 13.709/2018: princípios; aplicação das bases legais para dados pessoais e dados pessoais sensíveis; bases legais para transferência internacional de dados; direitos dos titulares; sujeitos da LGPD; segurança da informação; governança; responsabilidade civil dos agentes de tratamento; sanções administrativas e atribuições da ANPD; Inteligência Artificial (IA) e tratamento automatizado de dados; e regulamentação complementar de proteção de dados pessoais.

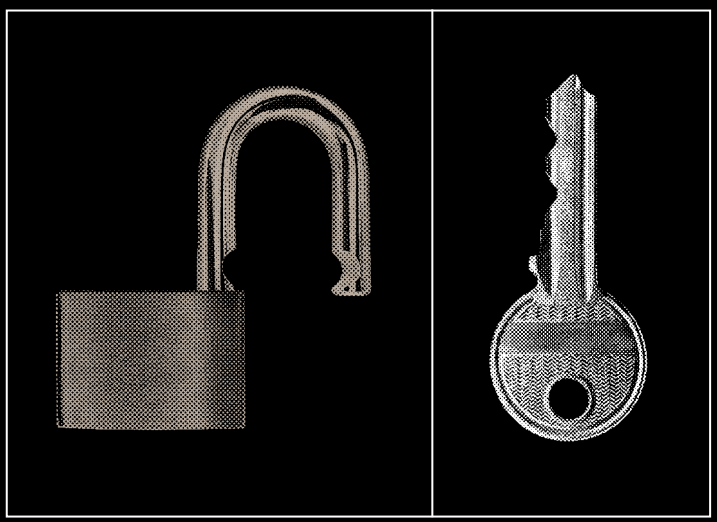
A LGPD deve ser internalizada por organizações de todos os portes para um uso ético, responsável e seguro das informações. Garantir a sua plena aplicação é uma questão de competitividade. Não à toa, a atuação da FecomercioSP em prol da cultura de proteção de dados e de um ambiente digital confiável a todas as partes vem de longa data. A Entidade participou da discussão da Lei de Crimes Informáticos, em 2012, e do Marco Civil da Internet, dois anos mais tarde, além de ter tido papel relevante no processo de elaboração e regulamentação da LGPD.

Almejamos garantir a devida segurança jurídica na interpretação da lei por meio de entendimentos sobre

temas controversos. Afinal, conciliar o uso das novas tecnologias com privacidade digital é agir em benefício do desenvolvimento sustentável do País.



SUMÁRIO DOS ENUNCIADOS



APLICAÇÃO DE BASES LEGAIS PARA DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

ENUNCIADO

Não há hierarquia entre as bases legais previstas nos incisos dos artigos 7º e 11 da LGPD, ou seja, não há base legal prioritária e uma não sobrepõe à outra.

Beatriz Puertas P. Rossi, Thamara Consul S. Chaves e Tiago Neves Furtado

JUSTIFICATIVA

A LGPD não prevê hierarquia entre as bases legais. Isso, porque cada uma das bases legais previstas nos artigos 7º e 11 da LGPD trazem consigo requisitos próprios para sua aplicação.

Assim, apesar de a base legal do consentimento aparecer no inciso I do referido artigo, isso não significa que esta seja hierarquicamente superior, nem que as demais sejam inferiores, tampouco que haja ordem de grandeza ou de preferência a partir da disposição de cada uma dentro dos artigos 7º e 11. Todas as bases possuem a mesma hierarquia, sua diferença está nos requisitos próprios para a sua aplicação, de acordo com a finalidade do tratamento dos dados.

BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BLUM, Renato Opice, *et al.* LGPD: Lei Geral de Proteção de Dados Comentada. 4ª edição. São Paulo: *Revista dos Tribunais*, 2022.

ENUNCIADO

É preciso cautela na valoração do consentimento para atividades de tratamento de dados pessoais no contexto das relações trabalhistas, considerando que o consentimento deve ser coletado de forma livre, inequívoca e informada.

Beatriz Puertas P. Rossi e Thamara Consul S. Chaves

JUSTIFICATIVA

Segundo o inciso XII, do artigo 5º, da LGPD, consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, ou seja, é a concordância do titular com o tratamento dos dados pessoais ou dados pessoais sensíveis.

Segundo o *Guidelines 05/2020 on consent under Regulation 2016/679*, consentimento livre significa que o titular não pode se sentir compelido a consentir, ou seja, ele deve ter a livre e efetiva escolha em concordar (ou não) com o tratamento de seus dados.

Por sua vez, o referido *guideline* indica que consentimento precisa ser específico, ou seja, deve ser dado em relação a uma ou mais finalidades específicas, bem como que o titular deve ter escolha em relação a cada uma dessas finalidades, de forma a garantir controle e transparência ao titular.

Ainda, cabe ao controlador fornecer algumas informações fundamentais ao titular, antes de obter seu consentimento, para que o titular entenda com o que está anuindo. Para que o consentimento seja informado, é necessário informar o titular dos dados de determinados elementos, como: a identidade do controlador; o objetivo de cada uma das operações de processamento para as quais é solicitado o consentimento; quais (tipos de) dados serão coletados e usados; o direito de retirar o consentimento; e as informações sobre o uso dos dados para tomada de decisão automatizada.

Por fim, o consentimento deve ser inequívoco, de maneira a não causar nem dúvidas ao titular, nem dúvidas quanto à demonstração livre de aceitação do titular. Por isso, não é recomendável a utilização de opções pré-assinaladas para o titular fornecer o seu consentimento.

Portanto, caso o consentimento não seja colhido de forma livre, específica, inequívoca e informada, este pode ser considerado nulo e, por esta razão, o consentimento obtido do empregador com seus colaboradores é controverso.

Isso, porque, conforme o *Guidelines 05/2020 on consent under Regulation 2016/679*, é pouco provável que o titular dos dados possa negar ao seu empregador o consentimento para o tratamento de dados sem sentir o medo ou o risco real de efeitos prejudiciais como resultado de uma recusa, por isso, dado o desequilíbrio de poder entre um empregador e seus funcionários, estes só podem dar consentimento livre em circunstâncias excepcionais, quando não haverá consequências adversas. Assim, não recomenda-se a utilização desta base legal para relações trabalhistas.

Igualmente, o Considerando 43 do General Data Protection Regulation (GDPR) aponta expressamente que "a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento".

No caso da relação entre o empregado (titular) e o empregador (agente de tratamento), há um inequívoco desequilíbrio entre as partes, razão pela qual,

inclusive, vigora o Princípio da Proteção ao Trabalhador (ou princípio da proteção ao hipossuficiente), ou seja, o funcionário é tratado como parte hipossuficiente em relação ao empregador, pois, juridicamente, está na parte mais frágil e delicada no contrato, por não haver equilíbrio contratual entre as partes.

Desta forma, verifica-se que o empregado não conseguiria, na maioria das situações, dar seu consentimento de forma livre, sendo, portanto, nulo, nos termos do §1º, do artigo 9º, da LGPD.

Por esta razão, é recomendável cautela e que esta base legal não seja utilizada, majoritariamente, para o tratamento de dados pessoais nas relações empregatícias. Contudo, isso não significa que a base legal do consentimento não seria aplicável em nenhuma situação envolvendo relações trabalhistas, ou seja, há situações em que é possível utilizar a referida base legal, desde que sejam observados os requisitos legais:

a. garantia de coleta de consentimento livre, inequívoco, específico e informado;

b. se fornecido por escrito, deverá conter cláusula destacada das demais cláusulas contratuais;

c. deverá referir-se a finalidades determinadas;

d. deve-se observar a granularidade do consentimento, ou seja, os titulares dos dados devem ser livres para escolher qual finalidade aceitam, em vez de terem que consentir com um conjunto de finalidades de tratamento;

e. o consentimento não poderá ser genérico; e

f. deve ser dado ao titular a opção de revogar seu consentimento, de maneira facilitada e sem nenhuma sanção patronal.

Para melhor elucidar uma hipótese de tratamento de dados dos colaboradores baseado no consentimento, indica-se o exemplo dado pelo *Guidelines 05/2020*: "Uma equipe de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nesta zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutro local de trabalho equivalente, numa outra zona do edifício, enquanto durar a filmagem".

No caso acima exposto, a coleta do consentimento ocorreu seguindo todas as diretrizes legais, sendo, portanto, válida.

Por fim, ressalta-se que, nos termos no artigo 14 da LGPD, haverá a coleta de consentimento para o tratamento de dados de crianças e adolescentes, como para os casos dos empregadores (agentes de tratamento) que contam com empregados menores de idade (ex.: Jovem Aprendiz) ou quando há a necessidade de tratamento de dados dos dependentes dos funcionários (ex.: inclusão em benefício, plano de saúde etc.).

Além disso, esse tratamento será realizado sempre visando ao melhor interesse da criança e por meio do consentimento específico e em destaque dado por, pelo menos, um dos pais ou representante legal, nos termos do §1º, do artigo 14, da LGPD.

BIBLIOGRAFIA

BRASIL. Decreto-Lei 5.452/1943 – Consolidação das Leis do Trabalho (CLT). Rio de Janeiro/RJ, Senado. 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BLUM, Renato Opice, *et al.* LGPD: Lei Geral de Proteção de Dados Comentada. 4ª edição. São Paulo: *Revista dos Tribunais*, 2019.

Guidelines 05/2020 on consent under Regulation 2016/679. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, Andre. *Reflexos da LGPD no direito e no processo do trabalho.* São Paulo: Thomson Reuters Brasil, 2020.

Opinion 15/2011 on the definition of consent. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). Disponível em: https://gdprinfo.eu/pt-pt

ENUNCIADO

O consentimento pode ser utilizado como base legal para o tratamento de dados pessoais na relação de emprego, desde que observadas as especificidades da desigualdade existente entre os contratantes, em especial a hipossuficiência do empregado. Portanto, para que o consentimento seja considerado válido, a manifestação de vontade do empregado deve ser informada, inequívoca e livre.

Tatiana Bhering Roxo

JUSTIFICATIVA

O consentimento é uma base legal que somente pode ser utilizado caso a manifestação de vontade do titular dos dados seja fornecida de forma inequívoca, informada e livre. Há uma discussão em relação à possibilidade de o empregado fornecer o consentimento de forma livre, considerando que, na relação de emprego, há um desbalanceamento entre as partes, tendo em vista que o empregado está em situação de desigualdade em relação ao empregador e é considerado hipossuficiente. Diante dessa desigualdade existente entre os contratantes, o ordenamento trabalhista traz princípios que protegem o trabalhador e pretendem reduzir a desigualdade que existe no plano fático, no plano jurídico. Propõe-se que o consentimento possa ser utilizado, em situações exceptivas, desde que observada a manifestação livre, informada e inequívoca do empregado. Neste sentido, a inexistência de prejuízo ou "consequência negativa" na hipótese de o empregado negar o consentimento deve ser considerada elemento definidor da análise da validade do consentimento dado pelo empregado.

BIBLIOGRAFIA

BRASIL. Decreto-Lei 5.452, de 1° de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Artigo: https://www.dataguidance.com/opinion/brazil-analysis-adequacy-lgpd-and-labour-laws-work

ENUNCIADO

Desde que integralmente atendido o Princípio do Melhor Interesse da criança e dos adolescentes, é possível a adoção de outras bases legais, além da base legal do consentimento dado por um dos pais ou do representante legal para crianças, levando em conta a interpretação extensiva do referido princípio.

Beatriz Puertas P. Rossi, Thamara Consul S. Chaves e Tiago Neves Furtado

JUSTIFICATIVA

Conforme o artigo 1º do Estatuto da Criança e do Adolescente – Lei 8.069/1990 (ECA), criança é a pessoa com até 12 (doze) anos incompletos; e adolescente é aquele entre 12 (doze) e 18 (dezoito) anos incompletos, sendo que, para o viés da LGPD, parecer existir apenas uma base legal apropriada para o seu tratamento, qual seja, o consentimento.

Isso, porque, de acordo com o artigo 14, §1º, da LGPD, a base legal para o tratamento de dados de crianças será o consentimento coletado de forma específica, destacada, e dado pelo representante legal.

Desta forma, cabe ao controlador aplicar medidas para verificar se o consentimento está sendo fornecido por pessoa apta ao fazê-lo, por meio da solicitação de documentos pessoais, certidão de nascimento, carta de tutela/curatela (se aplicável), entre outros, conforme disposto no §4º, do artigo 14, da LGPD.

Além disso, a LGPD também indica que poderão ser coletados dados pessoais de crianças sem o consentimento dos pais ou representantes legais, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o referido consentimento.

Contudo, a possibilidade e o cabimento de apenas uma base legal para o seu tratamento são amplamente questionáveis, uma vez que a Lei dispõe que o tratamento de dados de crianças e adolescentes deverão ser realizados conforme o melhor interesse, o que abre um leque de discussão sobre as hipóteses de cabimento de demais bases legais, quando o consentimento não for possível, para atender ao melhor interesse da criança e do adolescente.

O "melhor interesse" de crianças e adolescentes possui sua definição em doutrinas nacionais e internacionais, além de documentos legais, como é o caso do Comunicado Geral 14 à Convenção Internacional sobre Direitos da Criança das Nações Unidas, de 20 de novembro de 1989, recepcionada pelo Brasil logo após, em 1990.

A Convenção Internacional sobre Direitos da Criança das Nações Unidas trata o tema como acepção tripla, pois, para garantir a fruição plena e efetiva de todos os direitos e promover os desenvolvimentos físico, mental, moral, espiritual e social da criança, é necessário analisar o melhor interesse como:

a. direito fundamental: deve-se ponderar como primordial o melhor interesse da criança quando diversos interesses estiverem em conflito, devendo este direito ser garantido sempre que for envolvida uma criança (ou um grupo de crianças);

b. princípio jurídico interpretativo: quando em um dispositivo jurídico couber mais de uma interpretação, a norma deverá ser interpretada da forma que o melhor interesse da criança seja priorizado;

c. regra de procedimento: as decisões relacionadas a uma criança, a um grupo de crianças ou às crianças em geral, deverão ser realizadas avaliando os impactos da decisão, prezando sempre pelo interesse do menor.

Segunda a *Análise Jurídica* de BIBÁ; FEIJÓ; FIGUEIREDO (2022), toda e qualquer decisão, resolução de conflitos ou interpretação jurídica que envolva este grupo prioritário deverá considerar, primordialmente, o melhor interesse das crianças, a fim de que haja a efetivação dos seus direitos fundamentais e que seja prezado o seu desenvolvimento global.

Nesta esfera, considerando que o princípio do melhor interesse deve nortear todas as relações nas quais as crianças estão inseridas, diferente não seria no tratamento de dados pessoais desta categoria de titular pelos controladores.

Isso, porque há situações em que o tratamento de dados pessoais de criança deve ser realizado visando ao seu melhor interesse, independentemente da coleta do consentimento, como nos casos em que se tornar oneroso ou de difícil operacionalização a coleta do consentimento; ou, ainda, para os casos de inércia ou mesmo da recusa de um dos pais ou do representante legal em fornecer o consentimento específico.

Para tais situações, é possível aplicar outras bases legais, como nos casos em que há violação ao melhor interesse e ao direito à saúde; violação ao melhor interesse e ao direito à educação; violação ao melhor interesse e ao direito ao lazer; e violação ao melhor interesse e à dignidade humana.

Ainda nos termos da *Análise Jurídica* de BIBÁ; FEIJÓ; FIGUEIREDO (2022), sob o ponto de vista dos agentes de tratamento – considerando o dever que lhes é imposto de observar o melhor interesse da criança no tratamento de dados desses titulares, previsto não apenas na LGPD (artigo 14, *caput*), como no ECA, na CF e na Convenção Internacional sobre Direitos da Criança das Nações Unidas –, verificam-se diversos cenários em que, ao tratar dos dados de crianças apenas quando fornecido o consentimento dos pais e/ou responsáveis legais, o agente estaria violando o melhor interesse e, até mesmo, outros direitos fundamentais da criança. Por exemplo:

a. o agente de tratamento tem **obrigação legal** de cadastrar os dados pessoais dos dependentes dos seus colaboradores no Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial), conforme previsto na Lei 8.213/91 e no Decreto 8.373/2014; e

b. quando hospitais e/ou profissionais de saúde necessitam tratar os dados de criança em procedimentos de saúde (**tutela da saúde**).

Assim, ainda que no Brasil não existam diretrizes específicas para tratamento de dados de crianças e adolescentes emitidas pela ANPD, buscam, nas legislações e nos pareceres internacionais, diretrizes sobre o tratamento de dados de criança, como o Information Comissioner's Office (ICO), do Reino Unido[1]:

– "As crianças precisam de proteção especial quando você coleta e processa seus dados pessoais, porque podem estar menos cientes dos riscos envolvidos.

- Se você processa dados pessoais de crianças, deve pensar sobre a necessidade de protegê-las desde o início e projetar seus sistemas e processos com isso em mente.

- A conformidade com os princípios de proteção de dados e, em particular, a Justiça deve ser fundamental para todo o processamento de dados pessoais de crianças.

- Você precisa ter uma base legal para processar os dados pessoais de uma criança. O consentimento é uma possível base legal para o processamento, mas não a única opção. Às vezes, usar uma base alternativa é mais apropriado e fornece melhor proteção para a criança.

- Se você está contando com o consentimento como base legal para o processamento, ao oferecer um serviço online diretamente a uma criança, no Reino Unido, apenas indivíduos de 13 anos ou mais podem fornecer o próprio consentimento.

- Para crianças menores de idade, você precisa obter o consentimento de quem detém a responsabilidade dos pais pela criança – a menos que o serviço online que oferece seja preventivo ou de aconselhamento.

- Ao confiar em 'interesses legítimos', assumimos a responsabilidade de identificar os riscos e as consequências do processamento e implementamos salvaguardas adequadas à idade.

- As crianças merecem proteção específica quando você usa seus dados pessoais para fins de marketing ou para criar perfis de personalidade ou de usuário.

- Normalmente, você não deve tomar decisões com base unicamente no processamento automatizado de crianças se isso tiver um efeito legal ou significativo sobre elas.

- Você deve escrever avisos de privacidade claros para as crianças, de modo que elas possam entender o que acontecerá com os dados pessoais delas e quais direitos têm.

- As crianças têm os mesmos direitos que os adultos sobre os dados pessoais. Isso inclui o direito de acessar esses dados, solicitar retificação, opor ao tratamento e ter os os dados pessoais apagados.

- O direito de um indivíduo de apagar é particularmente relevante se ele deu seu consentimento para o processamento quando era criança.

- O que precisamos considerar ao escolher uma base para o processamento de dados pessoais de crianças? Assim como acontece com os adultos, você precisa ter uma base legal para processar os dados pessoais dessa

criança e precisa decidir qual é essa base antes de iniciar o processamento. Você pode usar qualquer uma das bases legais para processamento estabelecidas no GDPR ao processar dados pessoais de crianças".

Portanto, apenas com base na leitura fria do texto da LGPD, o consentimento deverá ser considerado para o tratamento de dados. No entanto, após uma leitura ampla e por meio de uma interpretação extensiva, há possibilidades de aplicações de demais bases legais, em especial visando ao "melhor interesse" da criança.

NOTAS

1 ICO/UK. *Diretriz de tratamento de dados de crianças.* Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/

BIBLIOGRAFIA

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília/DF, Senado. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Lei 8.069/1990 – Estatuto da Criança e do Adolescente. Brasília/DF, Senado. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm

BRASIL. Decreto 99.710/1990 – Convenção sobre Direitos das Crianças. Brasília/DF, Senado. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto/1990-1994/D99710.htm

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BIBÁ, Ana Rita; FEIJÓ, Renata; FIGUEIREDO, Ana Carolina. *Análise Jurídica – Base ou bases legais atribuíveis ao tratamento de dados de crianças*. São Paulo/SP. 2022. Opice Blum, Bruno Vainzof Advogados Associados.

ICO/UK. *Diretriz de tratamento de dados de crianças.* Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/

ENUNCIADO

A LGPD, em seu artigo 14, não exclui a possibilidade de aplicação de outras hipóteses de tratamento de dados pessoais de crianças, além do consentimento, observado o melhor interesse da criança.

Annette Pereira

JUSTIFICATIVA

O artigo 14 da LGPD, muito embora trate do consentimento, não exclui a possibilidade de aplicação das demais hipóteses, ou bases legais, previstas na LGPD, no caso de tratamento de dados pessoais de crianças. Referido artigo traz requisitos específicos a serem observados no caso de a base legal aplicável ao caso concreto ser o consentimento, não sendo excludente da aplicação das demais bases legais.

De qualquer forma, o melhor interesse da criança deve ser observado, independentemente da base legal aplicável ao caso concreto, especialmente em razão do disposto no *caput* do artigo 14 da LGPD.

Importante ressaltar que há diversas atividades de tratamento de dados de crianças em que não é recomendável, ou mesmo possível, utilizar o consentimento como base legal, como é o caso, por exemplo, do cumprimento de obrigações legais e regulatórias. Restringir ao consentimento as diversas atividades de tratamento de dados pessoais de crianças, além de inviável, também iria ao encontro do disposto na própria LGPD, que traz a possibilidade de aplicação de diferentes bases legais, independentemente do tipo de titular de dados.

ENUNCIADO

O consentimento não é a única base legal para o tratamento de dados pessoais de crianças e adolescentes, desde que haja, pelo agente de tratamento de dados, observância expressa a princípios, direitos e garantias, em especial o melhor interesse da criança e do adolescente.

Juliano Maranhão e Maria Gabriela Grings

JUSTIFICATIVA

O artigo 14 da Lei Geral de Proteção de Dados Pessoais faz referência apenas ao consentimento como base legal para o tratamento de dados de crianças, o que faz com que haja o questionamento sobre ser esta uma regra de autorização de tratamento específica para crianças e adolescentes, em oposição à regra geral prevista nos artigos 7º e 11 da LGPD. Isto é, a questão é se a única base legal para tratamento de dados pessoais de crianças e adolescentes seria o consentimento. Esta não parece ser a melhor interpretação, pois levaria a algumas situações absurdas, como a de um cartório de registro civil de pessoais naturais ficar impedido de cumprir suas obrigações legais, caso haja falta de consentimento pelos pais da criança, ou, ainda, em caso de tratamento para proteção da vida, incolumidade física ou saúde da criança, em contexto de urgência, no qual seja inviável obter o consentimento dos pais. Para superar esta dúvida, a presente proposta sugere esclarecer que o consentimento específico dos pais ou responsáveis aplica-se às hipóteses de tratamento cuja base legal seja o consentimento individual do titular. Deste modo, reconhece-se que o artigo 14, na verdade, complementa os artigos 7º e 11, e com ele não rivaliza, esclarecendo a questão.

BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

ENUNCIADO

Não é possível presumir que toda imagem da pessoa natural revele dados pessoais sensíveis, motivo pelo qual deverá ser confirmada a finalidade do seu uso, a fim de atribuir a base legal. Assim, o § 1º do artigo 11 não deve ser aplicado de forma automática, mas somente quando a atividade de tratamento efetivamente revelar dado sensível.

Tiago Neves Furtado

JUSTIFICATIVA

A fotografia, por si só, é o registro da imagem de uma pessoa. De forma isolada, não é suficiente para revelar um dado pessoal sensível. Isso, porque esse dado sensível precisa ser inferido da fotografia e associado ao indivíduo cuja foto está relacionada.

O que vai determinar a revelação de um dado sensível é o tratamento subsequente daquela imagem, associado à sua respectiva finalidade. Se não, vejamos os seguintes exemplos:

a. a foto do rosto de alguém só será dado biométrico se for realizado um procedimento técnico, que normalmente envolve o uso dos dados da imagem para criar um modelo ou perfil digital individual, com a finalidade de ser utilizado para identificação automatizada de imagens em processo de validação de identidade;

b. a foto de uma pessoa negra, por si só, não é suficiente para que se conclua qualquer dado pessoal ou de etnia. É preciso a associação do dado sensível com a imagem, por exemplo, uma autodeclaração de raça em um processo de cadastramento para contratação de empregados que contenha a foto da pessoa.

No Direito comparado, o item 3 do Considerando 51 do General Data Protection Regulation (GDPR) aponta nesta direção, ao indicar que "o tratamento de fotografias não deve ser sistematicamente considerado como tratamento de categorias especiais de dados pessoais, uma vez que são abrangidos pela definição de dados biométricos apenas quando tratados por um meio técnico específico que permita a identificação ou autenticação única de uma pessoa singular".

BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). Disponível em: https://gdprinfo.eu/pt-pt

ENUNCIADO

O artigo 10 da LGPD também se aplica ao Legítimo Interesse de Terceiros.

Tiago Neves Furtado

JUSTIFICATIVA

O inciso IX, do artigo 7º, da LGPD traz, de forma expressa, que o interesse legítimo pode ser do controlador e de terceiros. Contudo, o artigo 10 da LGPD, que traz as nuances desta base legal, não faz qualquer referência ao interesse legítimo de terceiros, apenas do controlador.

Neste contexto, pode haver opiniões no sentido de que o silêncio do artigo 10 da LGPD restringe a sua aplicação somente ao legítimo interesse do controlador. Entendemos, contudo, que este não é o melhor entendimento, uma vez que:

a. há menção expressa ao legítimo interesse de terceiro no inciso IX, do artigo 7; e

b. o fato de o artigo 10 só trazer regras e parâmetros para legítimo interesse do controlador não tem poder para revogar o artigo anterior.

O Direito comparado, especialmente o General Data Protection Regulation (GDPR), também prevê o legítimo interesse de terceiro no seu artigo 6º, e mesmo antes, no artigo 7º da Diretiva 95/46/EC (que precedeu o GDPR). Neste sentido, é o posicionamento do Information Commisioner's Office (ICO), autoridade do Reino Unido, sobre a possibilidade da utilização do interesse legítimo de terceiros, inclusive sob uma perspectiva mais ampla de benefícios para a sociedade. Se não, vejamos:

> "Os interesses legítimos do público em geral também podem desempenhar um papel importante ao decidir se os interesses legítimos no processamento prevalecem sobre os interesses e direitos do indivíduo. Se o processamento tiver um interesse público mais amplo para a sociedade em geral, isso pode agregar peso aos seus interesses ao compará-los com os do indivíduo".

Neste contexto, isto é, seja pela previsão expressa na LGPD, seja pelo que temos como exemplo na GDPR – e somando-se os benefícios para sociedades decorrentes do legítimo interesse de terceiros –, entendemos que esta é, sim, uma base legal possível de ser utilizada.

Sendo uma base legal válida, e por excesso de cautela e zelo, é recomendável a observância dos requisitos do artigo 10 da LGPD, mesmo que, naquele dispositivo, a referência seja unicamente para fins de legitimo interesse do controlador.

Isso, porque o artigo 10 traz os parâmetros para utilização do legítimo interesse controlador e, portanto, faria sentido obedecer aos mesmos limites quando da aplicação do legitimo interesse de terceiros.

BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). Disponível em: https://gdprinfo.eu/pt-pt

Diretiva 95/46/EC (que precedeu o GDPR)

Information Commisioner's Office (ICO)

ENUNCIADO

O benefício previsto no inciso II, do artigo 10, do Legítimo Interesse deve ser entendido de maneira ampla e, portanto, não se limita àqueles auferidos pelo titular por meio de serviços. É possível que esse benefício englobe, dentre outros: condição vantajosa; desconto; prêmio financeiro; ou produto.

Tiago Neves Furtado

JUSTIFICATIVA

Ao justificar uma atividade no legítimo interesse, o controlador deve demonstrar que a atividade de tratamento inclui: (i) a proteção, em relação ao titular, do exercício regular de seus direitos; ou (ii) prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e as liberdades fundamentais, nos termos desta Lei.

Na prática, é possível que este benefício ao titular não seja tecnicamente um serviço. Por sua vez, o termo "serviço" tem definições e nuances jurídicas, que pode restringir a aplicação da base legal do legítimo interesse, caso prevaleça a interpretação literal. Por exemplo:

a. no CDC: o artigo 3°, § 2º, define "serviço" como qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista; e

b. a Lei Complementar 116, de 31 de julho de 2003, traz uma lista de serviços anexa, com uma série de atividades.

Neste sentido, o serviço está sempre associado a uma atividade que alguém faz/exerce para outra pessoa. Logo, pela interpretação literal, o benefício decorrente do tratamento fundamentado no Legítimo Interesse seria sempre uma atividade.

Contudo, é comum que outros benefícios sejam concedidos aos titulares de dados, por exemplo, uma condição comercial vantajosa, um desconto, um prêmio financeiro, a participação em um evento, a inclusão como beneficiário de um seguro ou mesmo uma mercadoria (entre vários outros que se possa imaginar).

Esses benefícios não estariam em hierarquia inferior a um benefício decorrente de um serviço. Muito pelo contrário. Por isso, é preciso que se interprete o termo "serviço" de maneira bastante ampla, de modo a abarcar todo e qualquer benefício ao titular, garantido, assim, a amplitude necessária à aplicação da base legal do legítimo interesse.

BIBLIOGRAFIA

BRASIL. Lei 8.078/1990 – Código de Defesa do Consumidor (CDC). Brasília/DF, Senado. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

ENUNCIADO

A biometria, dado sensível dos empregados, poderá ser objeto de tratamento pelos empregadores com a utilização das bases legais do cumprimento de obrigação legal ou prevenção à fraude (artigo 10, inciso II, alíneas *a* e *g*, da LGPD), desde que seja justificável a utilização no contexto do empregador, em especial verificados o porte da empresa e a quantidade de empregados, ou a natureza da atividade econômica explorada, que pode envolver uma necessidade especial de preservação da saúde e segurança.

Tatiana Bhering Roxo

JUSTIFICATIVA

O tratamento de dados de biometria dos empregados é prática usual nas relações de emprego, em especial para o controle de jornada e o acesso a setores das empresas. O artigo 74, §2º, da CLT obriga os empregadores com mais de 20 empregados a registrar os horários de entrada e saída dos empregados, e a Portaria 1.510/2009 dispõe sobre o controle de jornada pela biometria – Sistema de Registro Eletrônico de Ponto, o que fez com que diversas empresas adotassem o controle de ponto por meio da biometria. Além disso, com o objetivo de garantir a segurança no acesso a setores que envolvam situações de risco à saúde, ou com o objetivo de proteção de dados sigilosos ou produtos valiosos, utiliza-se a biometria. No entanto, diante das disposições de proteção de dados pessoais, propõe-se que a utilização da biometria para controle de jornada e acesso a setores seja justificável no contexto da empresa – seja porque há uma quantidade relevante de empregados que justifique o uso da biometria e a prevenção à fraude, seja porque a atividade econômica explorada faz com que existam setores com condições especiais que justifiquem a limitação e o controle rígido de acesso.

BIBLIOGRAFIA

BRASIL. Decreto-Lei 5.442 – Consolidação das Leis do Trabalho (CLT). Disponível em: www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452compilado.htm

BRASIL. Portaria Ministro de Estado do Trabalho e Emprego 1.510, de 21 de agosto de 2009. Disponível em: https://www3.semesp.org.br/portal/pdfs/juridico2009/Portarias/26.08.09/Portaria_MTE_1510_21.08.09.pdf

ENUNCIADO

A política pública referida na LGPD deve ser interpretada de forma ampla, podendo também estar calcada no interesse público ou na materialização de garantias e disposições constitucionais, legais, regulamentares ou contratuais.

Annette Pereira

JUSTIFICATIVA

A política pública é programática de uma atuação da Administração Pública e, muito embora possa estar expressa em uma legislação, regulamentação ou contratação, pode também decorrer da concretização de uma leitura mais ampla – constitucional, legal e regulamentar –, a partir do interesse público, o que não prejudica em nada a consecução de princípios e direitos fundamentais do nosso Estado de Direito, dentre os quais, passa a fazer parte a própria proteção e o tratamento de dados pessoais.

Ademais, na LGPD, a política pública, referida no contexto do tratamento de dados pessoais pelo Poder Público e também por entidades privadas, é prevista de forma ampla e deve ser interpretada como tal, não restrita a uma legislação, regulamentação ou contratação pontual e específica, mas aberta a outras ações, políticas, programas, contratos, convênios e legislações que possam levar, inclusive, à concretização de matérias constitucionais, legais, regulamentares, contratuais ou de interesse público.

Assim, é essencial que a interpretação do conceito de política pública não se limite a hipóteses em que o conteúdo dessas políticas inclua, necessariamente, objetivos, metas ou prazos prescritos em lei. Isso, porque é possível que uma política pública tenha uma concepção mais genérica, sem a definição de sua forma específica de implementação detalhada em leis, regulamentos, contratos ou convênios.

ENUNCIADO

Por não haver hierarquia das bases legais, o tratamento de dados pessoais sensíveis, inclusive de dados biométricos, para garantia da prevenção a fraudes e segurança do titular dos dados, nos processos de identificação e autenticação de cadastro, não depende do consentimento do titular e pode ser realizado pelo agente de tratamento, de acordo com o disposto no artigo 11, II, *g*, da Lei 13.709, de 14 de agosto de 2018.

Annette Pereira

JUSTIFICATIVA

Ao tratar dados pessoais para prevenção a fraudes, especialmente dados pessoais biométricos, inclusive a coleta, a validação e o compartilhamento desses dados para estes fins, os agentes de tratamento procuram proteger os titulares de dados e as operações nos quais se envolvem, trazendo mais segurança para toda a sociedade. Para fins de prevenção a fraudes e segurança, os tratamentos não dependem do consentimento do titular, e o agente pode realizar o tratamento, no caso de dados pessoais sensíveis, com fundamento no artigo 11, II, "g", da Lei 13.709, de 14 de agosto de 2018 (LGPD).

Importante destacar que os titulares dos dados são beneficiados por tal tratamento, posto que proporcionada a segurança de seus dados, mitigando que fraudadores tentem se passar pelo titular para realizar fraudes em prejuízo do titular dos dados pessoais.

Ainda referido tratamento estando embasado em prevenção à fraude, não há necessidade de um segundo embasamento, mesmo sendo este o consentimento ou qualquer outro previsto na LGPD para o tratamento de dados sensíveis.

ENUNCIADO

1. Na ausência de regulação vinculante expressa sobre bases legais específicas para o tratamento de dados pessoais decorrentes de *cookies* não essenciais e tecnologias assemelhadas, o legítimo interesse se torna uma base legal apta a respaldar tal tratamento.

2. O legítimo interesse é tão capaz quanto o consentimento de promover a autodeterminação informativa do titular de dados, ao mesmo tempo que pode melhorar a experiência de navegação do titular, dadas as exigências de transparência e minimização de dados reforçadas pelo legislador (LGPD, artigo 10).

Maria Beatriz Previtali

JUSTIFICATIVA

Em suma, o objetivo do presente enunciado é propor uma alternativa à questão do uso dos *cookies* não essenciais e sua dificuldade de implementação pelos controladores e de entendimento por parte dos titulares de dados pessoais.

No dia 7 de junho de 2022, a Autoridade Nacional de Proteção de Dados (ANPD) publicou o Ofício 6/2022/CGTP/ANPD/PR, contendo recomendações de adequação ao portal *gov.br* e seus métodos de coleta de *cookies*. Dentre estas recomendações, destaca-se a da base legal apropriada para o tratamento de dados decorrentes de *cookies*: para os *cookies* necessários, caberia o legítimo interesse, ao passo que para os *cookies* não necessários (como os analíticos, de performance e de marketing), seria necessário utilizar a base legal do consentimento.

Este posicionamento logo chamou a atenção do mercado, por se tratar de uma prévia de possível determinação legal a ser emitida por relevante órgão regulador. A própria ANPD, inclusive, indicou, no Ofício, que, em breve, iria publicar um guia orientativo para solidificar estas recomendações. Contudo, é importante reforçar que as recomendações da ANPD são específicas para o portal *gov.br* – que hospeda páginas pertencentes ao governo federal e que, por sua própria natureza, tem obrigações reforçadas de demonstrar a transparência e legitimidade de suas práticas, inclusive em termos de proteção de dados. Já no que tange aos entes privados, por outro lado, este dever, embora existente, não é tão pronunciado quanto para as pessoas jurídicas de direito público.

Neste sentido, é perfeitamente possível e razoável argumentar que, quando realizado por entes privados, o tratamento de dados pessoais decorrentes do uso de *cookies* não essenciais e tecnologias assemelhadas pode ser respaldado tanto pelo consentimento (como referendado pela ANPD) quando pelo legítimo interesse. Isso se dá por dois motivos principais: primeiro, porque no Direito brasileiro não há qualquer previsão vinculante de uma base legal específica para o uso de *cookies* e tecnologias assemelhadas; segundo, porque, quando bem utilizado, o legítimo interesse é tão capaz quanto o consentimento de garantir a autonomia informativa do titular, permitindo uma escolha sobre o uso de *cookies* e com a vantagem de melhorar a experiência do usuário.

Em relação ao primeiro argumento, a respeito da inexistência de normas sobre uma base legal específica para o tratamento de dados pessoais decorrentes de *cookies*: nota-se que a ANPD novamente se inspirou no Direito europeu, mais especificamente na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações electrônicas, também conhecida como Diretiva ePrivacy. Em 2009, esta Diretiva foi modificada e passou a incluir previsões específicas para o tratamento de dados de *cookies*, inclusive a obrigatoriedade do uso da base legal do consentimento. A partir de 2016, inclusive, com a entrada em vigor do Regulamento Geral de Proteção de Dados (Regulamento UE 2016/679), aumentou-se a pressão para a conformidade com estas normas

sobre *cookies*, tendo em vista que as penalidades aplicáveis são significativas. Portanto, é natural que não somente o mercado como também as demais autoridades de proteção de dados ao redor do mundo observem, com atenção, estas repercussões. Contudo, também é importante que eventuais incorporações dessas diretivas nos respectivos ordenamentos domésticos sejam feitas de maneira coerente com as circunstâncias locais.

Especificamente no caso brasileiro, observa-se que ainda não houve uma movimentação no sentido de realizar tal inclusão. Mesmo que se argumente que esta obrigação encontraria respaldo no Marco Civil da Internet (Lei 12.965/2014), usando, por exemplo, seus dispositivos relacionados ao consentimento e ao sigilo para armazenamento e tratamento de informações referentes aos registros de conexão (artigo 7º, VII-IX), também seria necessário examinar até que ponto estes dispositivos ainda podem ser aplicados ao tratamento de dados pessoais, visto que a LGPD é uma lei especial e posterior em relação ao Marco Civil, tendo o condão de revogar tacitamente os dispositivos conflitantes.

Em relação ao segundo argumento, sobre o legítimo interesse ser capaz de observar a autodeterminação informativa do titular de dados: preliminarmente, vale lembrar que a própria LGPD estabelece critérios específicos para o uso do legítimo interesse, reforçando a necessidade de práticas de transparência para com o titular de dados (artigo 10, § 2º) e o uso dos dados estritamente necessários para a finalidade pretendida (artigo 10, § 1º) – reiterando a aplicação dos princípios da necessidade (artigo 6º, III) e da transparência (artigo 6º, VI). Além disso, não se pode ignorar que o próprio modelo originado no Direito europeu, com *cookie banners* ou *cookie walls* e diversas estratégias para obtenção do consentimento do titular, também está em discussão, em virtude das dificuldades que apresenta na prática, como reconheceu a própria Comissão Europeia na exposição de motivos da proposta do Regulamento relativo à privacidade e às comunicações eletrônicas (item 3.1), e como têm alertado especialistas em privacidade (NYOB, 2022).

No Brasil, a situação não é muito diferente, considerando que 50% dos usuários de internet "aceitam" *cookies* sem nem saber o que estes, de fato, representam (MANCUZO, 2022). Mesmo com explicações mais elaboradas e opção de escolher especificamente quais *cookies* aceitar, a tendência do titular é clicar nos *prompts* que lhe parecem mais atraentes para que possam prosseguir com a navegação, sem se preocupar efetivamente com o conteúdo do seu consentimento, o que evidencia o risco de os *cookie banners* adotarem *dark patterns*, isto é, práticas que podem enganar o titular a aceitar termos com os quais ele realmente não concorde ou não tenha ciência (NOCERA, 2022). Por isso, é relevante pensar em mecanismos que contemplem esta liberdade de escolha e facilidade de entendimento e navegação.

Para tanto, o uso dos *cookies* com o legítimo interesse é uma solução de fácil implementação e mais amigável ao usuário do que o consentimento. O critério da escolha não seria feito via *opt-in*, como é atualmente, mas via *opt-out*. A exemplo do que se tem sugerido na União Europeia, os *cookie banners* podem adotar a recomendação de incluir o botão "rejeitar todos os *cookies* não essenciais", o que permite uma ação direta e de compreensão mais rápida do que solicitar ao titular que escolha exatamente quais *cookies* deseja ou, ainda, impor

um consentimento generalizado para todos os *cookies* – o que claramente viola os requisitos de validade do consentimento previstos na LGPD. Ao permitir esta solução, a ANPD valida um método de conformidade de fácil implementação e com uma série de benefícios agregados.

BIBLIOGRAFIA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. "ANPD emite recomendações para adequação da prática de coleta de cookies do portal gov.br", 26 de maio de 2022. Disponível em:: https://web.archive.org/web/20220624055320/https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-emite-recomendacoes-para-adequacao-da-pratica-de-coleta-de-cookies-do-portal-gov.br (acesso em 21 de julho de 2022).

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. Versão 2.0, abril 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf (acesso em 12 de agosto de 2022).

CASTRO. J. "'Fomentar cultura de proteção de dados no país ainda é desafio', diz diretor da ANPD". *JOTA*, 28 de janeiro de 2022. Disponível em: https://www.jota.info/jotinhas/fomentar-cultura-de-protecao-de-dados-no-pais-ainda-e-desafio-diz-diretor-da-anpd-28012022 (acesso em 25 de julho de 2022).

COOKIE INFORMATION. "The evolution of the cookie banner". Disponível em: https://cookieinformation.com/resources/blog/the-evolution-of-the-cookie-banner/ (acesso em 29 de julho de 2022).

FERREIRA, R. "LGPD e cookies: fundamentos técnicos e regulatórios para uma abordagem coerente no Brasil". *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 27, nº 6.926, 18 junho de 2022. Disponível em: https://jus.com.br/artigos/98459 (acesso em 1º de agosto de 2022).

FITTON, D. “The rise of dark web design: how sites manipulate you into clicking”. *The conversation*, 29 de setembro de 2021. Disponível em: https://theconversation.com/the-rise-of-dark-web-design-how-sites-manipulate-you-into-clicking-168347 (acesso em 29 de julho de 2022).

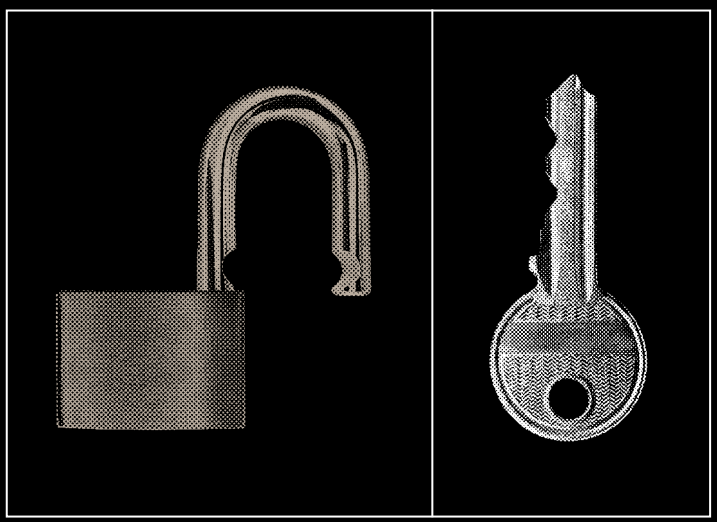
IETF. “HTTP State Management Mechanism. RFC2109”. Disponível em: https://datatracker.ietf.org/doc/html/rfc2109 (acesso em 22 de julho de 2022).

KUKU KA, M. “What are browser cookies? The history of cookies in digital advertising”. 23 de julho de 2021. Disponível em: https://newprogrammatic.com/blog/what-are-browser-cookies-in-digital-advertising/ (acesso em 28 de julho de 2022).

MANCUZO, R. “Metade dos brasileiros aceita cookies online mesmo não sabendo o que são esses códigos”. *Olhar Digital*, 13 de julho de 2022. Disponível em: https://olhardigital.com.br/2022/07/13/seguranca/metade-dos-brasileiros-aceita-cookies-online-mesmo-nao-sabendo-o-que-sao-esses-codigos/ (acesso em 14 de julho de 2022).

NOCERA, J. “How Cookie Banners Backfired”. *Dealbook Newsletter*, 29 de janeiro de 2022. Disponível em: https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html (acesso em 29 de junho de 2022).

NYOB. “More Cookie Banners to go: second wave of complaints underway”. 4 de março de 2022. Disponível em: https://noyb.eu/en/more-cookie-banners-go-second-wave-complaints-underway (acesso em 29 de julho de 2022).



DIREITO DOS TITULARES

ENUNCIADO

O titular de dados tem direito de acesso à informação de entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados (artigo 18, VII, LGPD), salvo se a divulgação de tais informações prejudicar eventuais segredos comerciais e industriais dos agentes de tratamento de direito privado. Nesta hipótese, é possível que o titular seja informado do segmento de mercado de eventuais fornecedores e parceiros, sem que seja exigível a exposição da razão social ou o nome fantasia destas empresas.

Dayane Oliveira Martins e Jéssica Cabrera Reis

JUSTIFICATIVA

A Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), traz, em seu artigo 18, uma série de direitos do titular de dados, que poderão ser exercidos em face do controlador, em relação aos dados do titular tratados pelo controlador, a qualquer momento e mediante requisição.

Destaca-se, oportunamente, o inciso VII, o qual confere ao titular o direito de acesso à informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados.

Conforme definição trazida pela própria LGPD, em seu artigo 5º, inciso XVI, o uso compartilhado de dados refere-se a:

> "Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados" (BRASIL, 2018).

Neste sentido, este direito confere ao titular de dados o conhecimento acerca das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de suas informações pessoais, a fim de "manter o titular no pleno controle de seus dados pessoais" (MALDONADO, 2020, pág. 233). Destarte, o exercício desse direito corrobora para que o titular venha a atingir a autodeterminação informativa, fundamento da legislação em comento (artigo 2º, inciso II).

Não se olvida, contudo, que o Supremo Tribunal Federal (STF) já preconizou que nenhum direito ou garantia individual tem caráter absoluto no ordenamento jurídico brasileiro, posto que devem ser considerados o interesse público e as exigências de convivência equilibrada das liberdades (BRASIL, 2000). Assim, é inequívoco que devem coexistir tanto o direito fundamental à proteção de dados como a livre-iniciativa e a livre concorrência, todos constitucionalmente consagrados.

Neste contexto, é possível afirmar que constatado pela organização que a divulgação de informações eventualmente venha a prejudicar segredos comerciais e industriais, os agentes de tratamento de direito privado poderão apresentar, ao titular de dados, apenas os segmentos de mercado aos quais seus fornecedores e parceiros pertencem, não sendo exigível, porém, o fornecimento da razão social ou do nome fantasia destas empresas.

O estabelecimento comercial diz respeito ao conjunto de bens corpóreos e incorpóreos reunidos pelo empresário ou pela sociedade empresária para a exploração de sua atividade econômica. Os bens corpóreos referem-se a mercadorias, mobiliários, utensílios e todos os bens materiais necessários para a exploração da atividade econômica. Os bens incorpóreos, por sua vez, são os bens industriais,

como patentes, modelo de utilidade, marca registrada, nome empresarial, entre outros, e o ponto comercial, isto é, local onde ocorre a exploração da atividade econômica (COELHO, 2015).

Dentre os bens incorpóreos de um estabelecimento comercial, estão os relacionados à propriedade industrial e, consequentemente, o chamado "segredo de empresa", uma vez que esta categoria propicia a proteção dos direitos relativos à propriedade industrial. Elizabeth Fekete (2003) apresenta interessante reflexão acerca do conceito de segredo de empresa, segundo a qual se trata de:

> "Conhecimento utilizável na atividade empresarial, de caráter industrial ou comercial, de acesso restrito, provido de certa originalidade, lícito, transmissível, não protegido por patente, cuja reserva representa valor econômico para o seu possuidor, o qual exterioriza o seu interesse na preservação do sigilo através de providências razoáveis" (FEKETE, Elisabeth Kasznar, 2003, pág. 420).

Fekete (2018), ainda no estudo do tema, propõe que o "segredo de empresa" seja dividido em duas categorias, quais sejam, os segredos comerciais e industriais:

> "O 'segredo de empresa', sinônimo, portanto, de 'segredo de negócio' ou 'informação confidencial', representa o gênero agrupante de duas espécies: os **segredos industriais**, que abrangem, dentre muitos outros exemplos possíveis, os processos de fabricação, as fórmulas de produtos, os dados técnicos de P&D e os **segredos comerciais**, como os projetos de lançamento de novos produtos ou serviços, os estudos de marketing, os resultados de pesquisas de mercado, **as listas de clientes ou fornecedores**, os métodos internos de trabalho e os estudos financeiros, tais como previsões de lucros, precificação etc." (FEKETE, Elisabeth Kasznar, 2018, s/pág.) [*grifo nosso*].

No ponto, destacamos que a mera lista de fornecedores, ainda segundo Fekete (2018), pode constituir segredo de empresa, razão pela qual terá tutela jurídica resguardada pelo ordenamento jurídico brasileiro, que visa a garantir a livre-iniciativa e a livre concorrência, nos preceitos da Constituição Federal (FEKETE, 2018).

Cumpre-nos salientar, por exemplo, que o Acordo sobre aspectos dos direitos de propriedade intelectual relacionado ao comércio (TRIPS)[1], em seu artigo 39, garante às empresas a proteção da chamada "informação confidencial" (FEKETE, 2018). A propósito, o dispositivo em estudo prescreve que:

> "**2.** Pessoas físicas e jurídicas terão a possibilidade de evitar que informação legalmente sob seu controle seja divulgada, adquirida ou usada por terceiros, sem seu

> consentimento, de maneira contrária a práticas comerciais honestas, desde que tal informação:
>
> **a)** seja secreta, no sentido de que não seja conhecida em geral nem facilmente acessível a pessoas de círculos que normalmente lidam com o tipo de informação em questão, seja como um todo, seja na configuração e montagem específicas de seus componentes; **b)** tenha valor comercial por ser secreta; e **c)** tenha sido objeto de precauções razoáveis, nas circunstâncias, pela pessoa legalmente em controle da informação, para mantê-la secreta" (BRASIL, 1994).

Ademais, a Lei 9.279, de 14 de maio de 1996, ou Lei da Propriedade Industrial (LPI), no artigo 195, incisos XI e XII, entende como crime de concorrência desleal aquele que divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais. A bem dizer, mesmo em âmbito trabalhista que, em regra, vige o princípio *in dubio pro operario*, o segredo de empresa também é prestigiado ao alçar como justa causa, para rescisão do contrato de trabalho pelo empregador, a violação de segredo da empresa pelo empregado, conforme observado na Consolidação das Leis do Trabalho (CLT), em seu artigo 482, alínea "g" (FEKETE, 2018).

A LGPD não se esquivou de abordar o tema, conferindo exaustiva positivação ao segredo de empresa. Nesta toada, nota-se que em diversos dispositivos da LGPD são resguardados pelo legislador os segredos comerciais e industriais.

Com efeito, a supracitada legislação aborda, por exemplo, que na apresentação do relatório de impacto à proteção de dados pessoais, solicitado pela autoridade nacional, deverão ser observados os segredos comercial e industrial (artigo 10, § 3º, e artigo 38, da LGPD), bem como na portabilidade dos dados a outro fornecedor de serviço ou produto (artigo 18, inciso V); na declaração completa de acesso a dados pessoais (artigo 19, inciso II); na solicitação de cópia eletrônica integral de dados pessoais, que tiver origem no consentimento do titular ou em contrato (artigo 19, § 3º); nas informações fornecidas a respeito dos critérios e procedimentos utilizados para a tomada decisão automatizada (artigo 20, § 1º); e na indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados (artigo 47, inciso III).

A legislação em comento preocupou-se tanto com o tema que instituiu como papel da Autoridade Nacional de Proteção de Dados (ANPD) zelar pela observância dos segredos comercial e industrial (artigo 55-J, inciso II, da LGPD), bem como dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial (artigo 55-J, inciso X).

Nesta medida, o princípio da transparência, expresso no artigo 6º, inciso VI, da LGPD, que representa garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, também deve expressamente observar os segredos comercial e industrial. Assim, é forçoso concluir que obstar o acesso a determinadas informações que estejam diretamente relacionadas a segredos de empresa não compromete o princípio da transparência, consagrado na legislação.

NOTAS

1 Sigla que identifica o Agreement on Trade-Related Aspects of Intellectual Property Rights, ou, em protuguês, "Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio". O tratado entrou em vigor no Brasil pelo Decreto 1.355, de 30 de dezembro de 1994.

BIBLIOGRAFIA

BRASIL. Congresso Nacional. *Constituição da República Federativa do Brasil*, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (acesso em 7 de agosto de 2022).

BRASIL. Congresso Nacional. Decreto-Lei 5.452/1943 – Consolidação das Leis do Trabalho (CLT). Rio de Janeiro/RJ. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm (acesso em 7 de agosto de 2022).

BRASIL. Congresso Nacional. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (acesso em 7 de agosto de 2022).

BRASIL. Congresso Nacional. Lei 9.279/1996. Brasília/DF. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9279.htm (acesso em 7 de agosto de 2022).

BRASIL. Presidência da República. Decreto 1.355/1994. Brasília/DF. Disponível em: https://www.gov.br/inpi/pt-br/backup/legislacao-1/27-trips-portugues1.pdf (acesso em 7 de agosto de 2022).

BRASIL. Supremo Tribunal Federal (STF). Recurso Ordinário em Mandado de Segurança.

23.452/RJ. Relator ministro Celso de Mello, publicado em 12 de maio de 2000, pág. 20.

COELHO, Fábio Ulhoa. *Curso de direito comercial: direito de empresa*. 19ª ed. Vol. 1. Saraiva: São Paulo, 2015.

FEKETE, Elisabeth Kasznar. *O regime jurídico do segredo de indústria e comércio no direito brasileiro*. Rio de Janeiro: Forense, 2003.

FEKETE, Elisabeth Kasznar. Segredo de empresa. *Enciclopédia jurídica da PUC-SP.* Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Comercial. Fábio Ulhoa Coelho, Marcus Elidius Michelli de Almeida (coord. de tomo). 1ª ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/248/edicao-1/segredo-de-empresa (acesso em 8 de agosto de 2022).

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice (coord.). LGPD: *Lei Geral de Proteção de Dados – comentada*. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

UNCTAD-ICTSD. "Resource book on TRIPS and development". Cambridge: Cambridge University Press, 2005. Disponível em:: http://www.iprsonline.org/unctadictsd/docs/RB_2.28_updae.pdf (acesso em 8 agosto de 2022).

ENUNCIADO

A Lei Geral de Proteção de Dados (LGPD) e o direito à obtenção de cópia de processo administrativo, assegurado no artigo 5º, XXXIII e XXXIV, *b*, da Constituição Federal. Situação com previsão e enquadramento em uma das hipóteses do artigo 7º da LGPD (inc. VI), nas quais o compartilhamento de informações pode ser feito, dando cumprimento ao comando constitucional. Existência de base legal para a Administração Pública compartilhar com o cidadão-requerente as informações contidas em processo administrativo quando, na qualidade de terceiro interessado, alegar a necessidade de conhecimento dessas informações para o exercício de direito próprio em processo judicial ou administrativo. Compatibilidade da

LGPD com a Lei de Processo Administrativo, Lei 9.784, de 1999, artigo 3º, inciso II, que assegura ao administrado o direito de ter vista aos autos e de obter cópias dos documentos nele contidos. Compatibilidade da LGPD com a Lei de Acesso a Informações, Lei 12.527, de 2011, que institui, como uma de suas diretrizes, a observância da publicidade como preceito geral e do sigilo como exceção. Resolução CNJ 363, de 2021, que trata da adequação do Poder Judiciário à LGPD, não afasta a proteção dada aos cidadãos pelo artigo 5º, XXXIII, XXXIV, *b* e LXXIX, da Lei Maior Federal, não afronta a Lei de Processo Administrativo Federal, tampouco desrespeita a Lei de Acesso à Informação (LAI).

Débora Maria Lima Machado e Edite Hupsel

BIBLIOGRAFIA

HUPSEL, Edite; AGUIAR, Risane; LAGO FILHO, José Ângelo. Lei Geral de Proteção de Dados Pessoais e o direito à obtenção de cópia de processo administrativo. Revista Brasileira de Direito Público – RBDP, Belo Horizonte, ano 20, n. 76, p.149-158, jan./mar. 2022

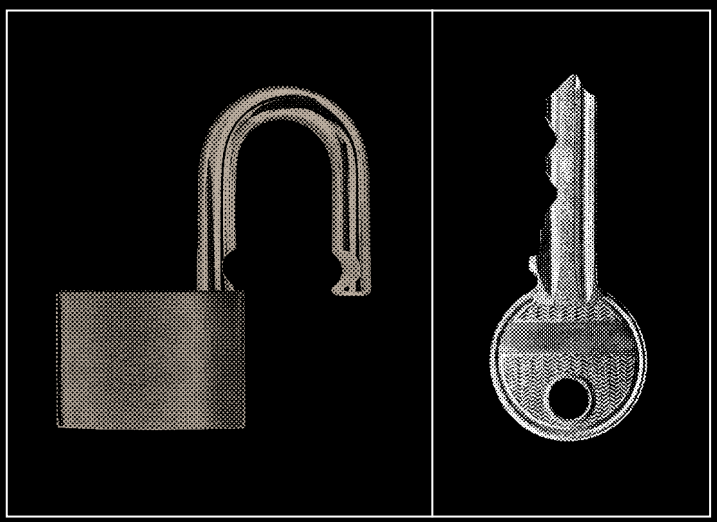
MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação. In: TEPEDINO, Gustavo et al. (coord.). Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2019.

PROCESSO. ADMINISTRATIVO. DIREITO À EXTRAÇÃO DE CÓPIA DOS AUTOS. DEVER DE PUBLICIDADE DA ADMINISTRAÇÃO. INEXISTÊNCIA DE SIGILO. 1. Com efeito, na ordem jurídica vigente, tanto o jurisdicionado quanto o administrado devem ter amplo acesso aos procedimentos que lhe digam respeito, que possam influir na sua esfera de direitos, ressalvados aqueles cujo sigilo seja imprescindível à segurança da sociedade e do Estado. 2. A Constituição Federal, em seu artigo 5º, inciso LX prevê que "a lei só poderá restringir a publicidade dos atos processuais quando a defesa da intimidade ou o interesse social o exigirem". No inciso XXXIII, prevê que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas

cujo sigilo seja imprescindível à segurança da sociedade e do Estado". 3. A Lei 9.784/99, que regula o processo administrativo no âmbito da Administração Pública Federal, estabelece no inciso II, do artigo 3º, que o administrado possui direito a obter cópias de documentos contidos nos processos administrativos. 4. Remessa oficial improvida. (TRF-2. AMS 67.377 RJ 2006.51.01.012479-2. Relator: des. federal Luiz Antonio Soares. Julgamento em 8 de maio de 2007. Quarta Turma Especializada. DJU, 11 de junho de 2007, pág. 242).

ADMINISTRATIVO. EXTRAÇÃO DE CÓPIA DE PROCESSO ADMINISTRATIVO. PRINCÍPIO DA PUBLICIDADE. ART. 3º DA LEI 9.784/99. 1. A teor do princípio da publicidade constitucionalmente consagrado, deve a Administração Pública garantir aos administrados o acesso aos documentos e decisões contidas em processos administrativos, mormente se interferirem na esfera do indivíduo. 2. O art. 3º da Lei 9.784/99 confere ao administrado o direito de obter cópias dos documentos contidos nos processos administrativos, razão pela qual configura cerceamento ao direito de defesa e ao exercício do contraditório a denegação injustificada de cópias. 3. Remessa necessária desprovida. (TRF-2. REOMS 73.372 RJ 2006.51.10.000589-5. Relator: des. federal Marcelo Pereira/no afast. Relator. Julgamento em 16 de setembro de 2008. Oitava Turma Especializada. DJU, 24 de setembro de 2008, pág. 122).

CERTIDÃO ADMINISTRATIVA – Direito de obtenção (art. 5º, XXXIV, "b", da CF). Omissão administrativa. Autoridade que não fornece certidão no prazo constitucional. Lesão a direito líquido e certo configurada. MS concedido. Inteligência do art. 114 da Constituição do Estado. (TJSP – Ap. 119.889-1 – (reexame) – Rel. des. Ernani de Paiva – J. 8 de março de 1990) (RT 653/106, apud Juris Síntese nº 16, ementa sob nº 100145 – CD-ROM); MANDADO DE SEGURANÇA – CERTIDÃO ADMINISTRATIVA, DOCUMENTOS E INFORMAÇÕES – DIREITO DE OBTENÇÃO (ART. 5º, INCS. XXXIII E XXXIV, "B", DA CF) – RECURSO E REMESSA DESPROVIDOS – Qualquer cidadão é parte legítima para propor ação popular que vise a anular ato lesivo ao patrimônio público de modo que a negativa no fornecimento de certidões, documentos e informações solicitados não se afeiçoa ao princípio de transparência dos atos da administração pública. Assim, a autoridade que se esquiva de apresentar certidões ou de prestar informações de interesse particular ou de interesse coletivo ou geral (CF, art. 5º, XXXIII), age contra disposição prevista no art. 5º, inc. XXXIV, "b", da Carta Magna e a omissão enseja a interposição de mandado de segurança. (TJSC. AC no Mandado de Segurança nº 97.003746-5 – 2ª C. C. Esp. Relator: des. Nelson Schaefer Martins. Julgamento em 14 de agosto de 1997).



SUJEITOS DA LGPD

ENUNCIADO

Redes computacionais formadas por nós distribuídos, como a rede bitcoin, não possuem personalidade jurídica e a elas não se aplica a LGPD. São controladores as pessoas físicas ou jurídicas que se utilizam da rede computacional distribuída, desde que tomem decisões quanto ao tratamento dos dados.

Renata Souto Baião

JUSTIFICATIVA

Nas redes distribuídas, não há centralização na tomada de decisões quanto ao seu funcionamento. As decisões em redes distribuídas são tomadas por meio da formação de consenso entre os nós. Serão controladores pessoas físicas e jurídicas que utilizarem as redes computacionais distribuídas, desde que tomem decisões referentes ao tratamento de dados pessoais, a eles incumbindo as medidas de adequação à LGPD.

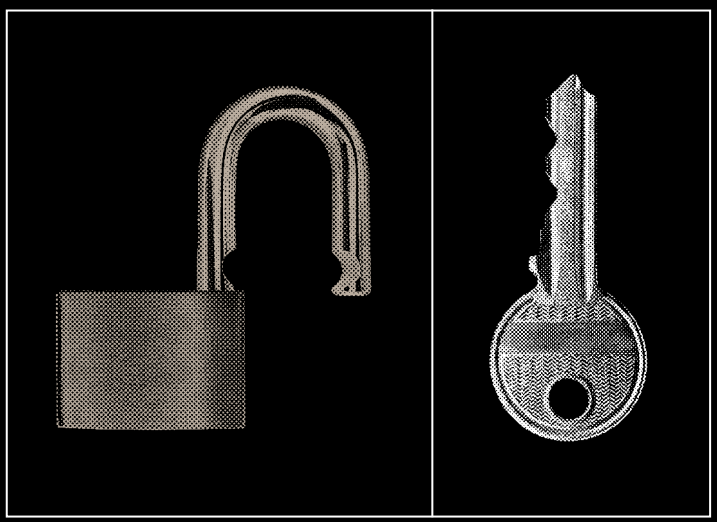
BIBLIOGRAFIA

ANTONOPOULOS, Andreas. *Mastering bitcoin. Programming the open blockchain*. 2nd. Edition. O´Reilly. United States of America: 2017.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (acesso em 9 de setembro de 2022).

BARAN, Paul. On Distributed Communications. I. Introduction to distributed communications networks. Research Memorandum. Relatório publicado em janeiro de 1964. Disponivel em: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf (acesso em 9 de setembro de 2022).

NAKAMOTO, Satoshi. "A peer-to-peer electronic cash system". Disponível em: https://bitcoin.org/bitcoin.pdf (acesso em 9 de setembro de 2022).



SEGURANÇA DA INFORMAÇÃO (SI)

ENUNCIADO

O agente de tratamento de dados pode valorar o risco de incidentes envolvendo dados pessoais para justificar a decisão por notificar ou não a Autoridade Nacional de Proteção de Dados (ANPD), considerando que empregue metodologia em consonância com boas práticas de mercado, enquanto não houver paradigma de cálculo estabelecido pela ANPD.

Fábio Dacêncio Pereira e Pedro Luís Ventroni Pereira

JUSTIFICATIVA

Quando especificamente notificar a Autoridade Nacional de Proteção de Dados (ANPD) sobre um incidente? Para os controladores, a falta de critérios objetivos torna este ato previsto no artigo 48 da LGPD (BRASIL, 2018) algo envolto em incertezas e questionamentos. De acordo com a atual orientação da ANPD, a inexistência de delimitadores faz com que a recomendação seja a de cautela: na dúvida, notifique a autoridade nacional (BRASIL, 2021).

E para a ANPD, quão viável é analisar estes casos? A tendência é de que haja um volume excessivo de notificações, com triagens complexas, por conterem análises subjetivas. Demasiados tempo e esforço podem acabar sendo empregados em situações não tão críticas, em detrimento de outras que necessitariam de maiores atenção e urgência da autoridade nacional.

Para que os controladores tenham clareza e estejam seguros de que estão cumprindo a lei, e para que a autoridade nacional consiga exercer sua função com mais excelência, deve-se admitir que critérios de notificação de incidentes sejam definidos de modo objetivo, simples, e que possam ser evoluídos conforme a necessidade.

Em um cenário análogo, o Departamento de Saúde e Serviços Humanos dos Estados Unidos (HHS) emitiu o HIPAA (Health Insurance Portability and Accountability Act), que define um padrão federal para a proteção das informações confidenciais de saúde dos pacientes. Dentre as regras, estabeleceu-se o critério de notificação de incidentes à autoridade, sendo estipulado que, caso haja mais de 500 titulares afetados, deve-se realizar a notificação; caso seja um contingente inferior a 500 titulares, o incidente deverá ser reportado em um relatório anual.

Assim, para justificar a viabilidade de adoção de critérios objetivos, será traçada uma proposta exemplificativa com base em critérios objetivos, para direcionar a notificação ou a não notificação à ANPD.

Neste exemplo, o valor do HIPAA para notificação, de 500 titulares afetados, será utilizado como base orientativa para nossos cálculos objetivos de notificação. **Isto é, que a referência para notificar a ANPD seja com base no número de titulares afetados, em que esta quantidade mínima possa variar de acordo com o nível de criticidade do incidente.**

Assim, nesta metodologia exemplificativa, para se obter o nível de criticidade do incidente – e, por consequência, a quantidade mínima de titulares para notificar a ANPD –, serão considerados quatro critérios: o tipo dos dados; a ocorrência de danos relevantes; o envolvimento em transferências internacionais; e a possibilidade de conter dados de titulares menores:

- tipo dos dados: o primeiro critério que o controlador deverá analisar é o tipo de dado envolvido no incidente. A classificação será feita em quatro nichos: dados pessoal, comportamental, financeiro e sensível;

- ocorrência de danos relevantes: deverá informar se, até o momento, danos

relevantes já ocorreram em decorrência do incidente. Isto é, se os dados envolvidos já causaram algum prejuízo relevante aos titulares de dados (sim) ou se, por enquanto, permanece apenas o risco de que ocorra (não);

- transferência internacional: o terceiro critério é informar se são feitas transferências internacionais na atividade de tratamento de dados que sofreu o incidente. Caso ocorra, isso aumentará o nível de criticidade do incidente;

- titular menor (criança ou adolescente): deverá indicar se o incidente afetou uma atividade de tratamento que contenha dados de titulares menores (crianças ou adolescentes).

A fórmula a seguir estipulará a quantidade mínima de titulares para que a ANPD seja notificada. Observe que ela é simples e objetiva, permitindo uma fácil automação da análise (com questões de múltipla escolha), bem como é evolutiva, pois permite que novos critérios sejam incluídos conforme a necessidade, e que seus pesos sejam recalibrados:

Qtd. de Titulares =
500 * [Tipo de Dado] * [Transferência Internacional] * [Titular Menor] * [Dano]

A tabela a seguir contém os valores dos **fatores críticos** sugeridos para cada critério:

TIPO DE DADO (TD)	FATOR CRÍTICO
Sensível	1
Financeiro	1,25
Comportamental	1,5
Pessoal	2

TRANSFERÊNCIA INTERNACIONAL (TI)	FATOR CRÍTICO
Sim	0,5
Não	1

TITULAR MENOR (TM)	FATOR CRÍTICO
Sim	0,5
Não	1

HOUVE DANO? (D)	FATOR CRÍTICO
Sim, material	0,5
Sim, moral	0,5
Não houve	1

Como uma primeira observação, vale ressaltar que **o fator crítico é inversamente proporcional, ou seja, quanto menor o peso, maior o impacto.** Exem-

plificando: em dada circunstância, o referencial é de 1.000 titulares e será acrescentado um parâmetro crítico, com peso de 0,5. Ao multiplicar 1.000 por 0,5, a quantidade mínima de titulares para notificar a ANPD será reduzida para 500, ou seja, um referencial mais rigoroso.

Também é necessária a observação no sentido de que se deve entender que o HIPAA aplica-se para o cenário de dados sensíveis, o que, no contexto da LGPD, compreende-se como a classe de dados mais crítica. Por ser nossa base, recebe o peso 1, e, como os demais tipos de dados são menos impactantes que os sensíveis, o peso destes é maior do que 1, pois isso fará com que a quantidade mínima de titulares requeridos aumente. Nas situações em que a quantidade mínima de titulares afetados pelo incidente não for atingida, a notificação à ANPD não será necessária naquele momento.

Uma possibilidade de regulação à ANPD, assim como estipulado no HIPAA, seria exigir das organizações o envio de um relatório semestral ou anual à própria ANPD, para que estes incidentes de menor gravidade também sejam registrados, ou seja, incidentes que eventualmente restassem fora do escopo que determina a notificação.

Para arrematar este exemplo, a seguir, realizam-se três simulações de incidentes.

- **CENÁRIO 1:** incidente com dados pessoais, sem transferência internacional, não envolve menores e sem danos ocorridos até o momento.

  Qtd. de Titulares = 500 * 2 * 1 * 1 * 1
  Critério de notificação = Ao menos 1.000 titulares afetados

- **CENÁRIO 2:** incidente com dados sensíveis, sem transferência internacional, não envolve menores e sem danos ocorridos até o momento.

  Qtd. de Titulares = 500 * 1 * 1 * 1 * 1
  Critério de notificação = Ao menos 500 titulares afetados

- **CENÁRIO 3:** incidente com dados sensíveis e envolvendo menores, mas sem transferência internacional e sem danos ocorridos até o momento.

  Qtd. de Titulares = 500 * 1 * 1 * 0,5 * 1
  Critério de notificação = Ao menos 250 titulares afetados

Por fim, na tabela a seguir é possível verificar que a quantidade média de titulares afetados nos incidentes notificados à autoridade norte-americana, nos meses de maio, junho e julho de 2022, é de 1.447 (HHS). Isto é, são números próximos dos obtidos com a aplicação da fórmula proposta. Vale ressaltar que essa média foi feita com base nos incidentes que atingiram o critério mínimo de 500 titulares para serem notificados, e que os cenários com valores de titulares muito altos foram desconsiderados, no momento do cálculo.

PERÍODO	MAIO/22	JUNHO/22	JULHO/22
Média	62.313	83.710	62.313
Média desconsiderando incidentes com mais de 10 mil titulares	1.389	1.565	1.389
Incidente com o maior número de titulares afetados	2.000.000	1.290.104	1.918.941

Logo, verifica-se ser possível estipular critérios objetivos para se notificar a ANPD em casos de incidentes com dados pessoais. Na metodologia utilizada como exemplo, o valor de referência para essa notificação será o número de titulares afetados, em que a quantidade mínima irá variar de acordo com o nível de criticidade dos incidentes. Os critérios que compõem este cálculo de criticidade são: o tipo dos dados; a ocorrência de danos relevantes; o envolvimento em transferências internacionais; e a possibilidade de conter dados de titulares menores (crianças ou adolescentes).

Desta forma, desde que o controlador, ao tomar a decisão pela notificação ou não à ANPD, realize exercício com critérios objetivos, que considerem critérios atinentes às características do incidente, tal decisão deve ser considerada admissível, por ser admissível tal metodologia objetiva de decisão.

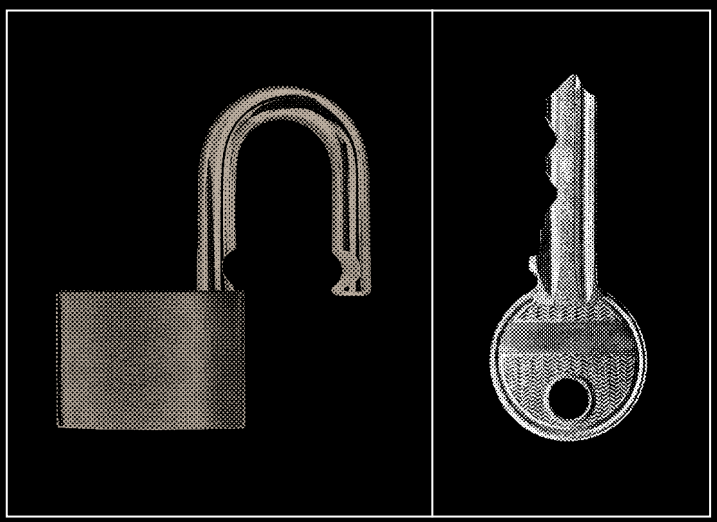
BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm

BRASIL. *Comunicação de incidentes de segurança*. Brasília: Autoridade Nacional de Proteção de Dados, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

HHS – Health Human Services (EUA). *HIPAA: Breach Notification Rule*. Disponível em: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

HHS – Health Human Services (EUA). *Office for Civil Rights: Breach Portal*. Disponível em: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf



GOVERNANÇA

ENUNCIADO

O “risco” às liberdades civis e aos direitos fundamentais, previsto no inciso XVII, do artigo 5º, da Lei Geral de Proteção de Dados Pessoais (LGPD), deve ser entendido como “alto risco” às liberdades civis e aos direitos fundamentais. O alto risco deve adotar como base critérios que evidenciem a proteção centralizada no titular de dados.

Jéssica Cabrera Reis e Dayane Oliveira Martins

JUSTIFICATIVA

Ao definir o conceito do relatório de impacto à proteção de dados, o legislador foi objetivo em seus dizeres ao apontar que tal relatório deve ser composto pelos processos de tratamento de dados pessoais que podem gerar "risco" às liberdades civis e aos direitos fundamentais.

Veja-se, assim, a literalidade da LGPD:

> "**XVII** – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que **podem gerar riscos** às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018) [*grifo nosso*].

Entendemos que o legislador foi objetivo, porque todo e qualquer processo de tratamento de dados pessoais tem intrínseco um risco aos titulares de dados, por menor que seja esse risco.

A melhor interpretação deste dispositivo, que aqui se justifica, é entender que os processos de tratamento de dados pessoais que podem gerar "riscos" são, em termos práticos, "altos riscos".

É dizer: todo processo de tratamento de dados pessoais pode gerar riscos aos titulares de dados. Quando se traz o relatório de impacto como mais um mecanismo de governança para a proteção de dados pessoais, deve-se entender que tal mecanismo recai sobre os processos de tratamento de dados que contêm alto risco às liberdades civis e aos direitos fundamentais.

Pensemos em um exemplo cotidiano. A entrada de uma visitante em um condomínio residencial em que é necessário o fornecimento do seu nome e número de Registro Geral (RG) se caracteriza como um processo simplório, com poucos dados e a envolver dados não sensíveis. Entretanto, como qualquer outra atividade, tem um nível de risco em si atrelado, ainda que seja um baixo risco.

Vainzof (2021), em uma verdadeira e esclarecedora sistematização sobre o tema do relatório de impacto, no modelo de perguntas e respostas, ensina que documento deve ser elaborado quando se estiver diante de uma operação de tratamento de alto risco:

> **"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" (2021) [*segundo grifo nosso*].

O jurista deixa explícito este entendimento, inclusive, ao mencionar que esse alto risco deve ser analisado de acordo com parâmetros estabelecidos de maneira prévia. E de forma a confirmar esta compreensão, Maria Cecília Gomes ensina que:

> "Na análise de Gellert, o risco possui dois elementos distintivos: prever eventos futuros (negativos e positivos) e tomar decisões com base nisso, em outras palavras, **isso significa que o risco não possui um significado dualista, não se trata de ter ou não ter risco.** O risco existe e é inerente, se trata, portanto, de quanto risco um agente de tratamento é capaz de assumir e o quanto de risco ele consegue mitigar" (GOMES, 2020).

Mais adiante, a autora ainda é mais explícita especificamente sobre a expressão "podem gerar riscos", ao esclarecer que não se pode depreender uma concepção dualista de risco (há riscos *versus* não há risco), de modo a ser a melhor interpretação no sentido de que toda e qualquer operação de tratamento de dados pessoais tem riscos:

> "Nesse sentido, interessante notar que **o verbo 'podem' gerar riscos, na definição de RIDPD do artigo 5º parece considerar o risco numa perspectiva dualista (pode ter risco ou não ter risco).** Conforme vimos na análise da noção de risco feita no tópico anterior, consideramos que **essa não é a melhor interpretação.**
>
> **Fato é que operações de tratamento de dados pessoais possuem riscos:** o ponto é como identificar esses riscos, compreender e avaliar o seu impacto e, assim, mitigá-los, preservando e protegendo os direitos dos titulares. Quando se discute gerenciamento de risco, é exatamente isso que está sendo levado em consideração: **se o risco é inerente**, como posso fazer para torná-lo ao menos gerenciável?" (GOMES, 2020) [*grifos nossos*].

Denota-se, então, que conforme a autora pondera acima, os processos de tratamento de dados têm riscos, quer dizer: não é sobre ter ou não ter risco, mas adotar a premissa do risco intrínseco e, a partir disso, desenvolver ações para torná-lo gerenciável.

Exatamente no mesmo sentido, ao abordar a necessidade de elaboração de um relatório de impacto à proteção de dados, Isabely Pimentel Ceolin corrobora este mesmo entendimento aqui apresentado, segundo o qual todo e qualquer processo de tratamento de dados pessoais é uma operação de risco:

> **"É inegável que as atividades de tratamento de dados pessoais, por si, só são atividades de risco** e que sujeitam os titulares de dados pessoais a riscos. Se a regra para elaboração de relatórios de impacto fosse pura e simplesmente apresenta-

ção de riscos em uma atividade, todas, portanto, demandariam sua elaboração" (CEOLIN, 2021).

É possível depreender, então, que a elaboração do relatório de impacto deve ser precedida da análise dos níveis de risco, porque toda e qualquer operação de tratamento de dados gera riscos aos titulares de dados, por menor que sejam esses riscos.

Nesse sentido, justifica-se a primeira parte do enunciado proposto: "O 'risco' às liberdades civis e aos direitos fundamentais, previsto no inciso XVII, do artigo 5º, da Lei Geral de Proteção de Dados Pessoais, deve ser entendido como 'alto risco' às liberdades civis e aos direitos fundamentais".

Assentado o entendimento sobre o risco intrínseco aos processos de tratamento de dados pessoais, é indispensável entender quais são os critérios que se justificam para avaliar cada nível de risco.

Neste contexto, é fundamental abordar dois conceitos: risco e nível de risco. É imprescindível adentrar o conceito de risco para que seja possível o estudo de como se devem dar os critérios para avaliação dos níveis de risco de operações de tratamento de dados.

Risco é "efeito da incerteza nos objetivos" (ABNT, 2018), de acordo com a norma ISO/IEC 27000:2018. Ora: um processo de tratamento de dados pessoais tem seu objetivo, ou melhor, a sua finalidade. Mas esses "objetivos" são incertos, tendo em vista que o processo de tratamento tanto pode se desenvolver regularmente (efeito positivo), quanto pode acontecer um incidente de segurança (efeito negativo) envolvendo esse processo de tratamento de dados pessoais.

O efeito desta incerteza nos objetivos, portanto, quando se está a explorar um processo de tratamento de dados pessoais, é ou o tratamento de dados acontecer normalmente ou a ocorrência de um incidente de segurança a envolver tais dados pessoais.

O sistema de proteção de dados pessoais surge para proteger o titular de dados e, assim, assegurar que boas práticas sejam adotadas para minimizar este efeito negativo dos processos de tratamento de dados pessoais, daí porque se monitora esse efeito negativo: a ocorrência de um incidente de dados.

Nesse contexto, o conceito de nível de risco, consoante preceitua a norma ISO/IEC 27000:2018, é: "Magnitude de um risco expresso em termos de combinação de consequências e sua probabilidade" (ABNT, 2018).

Logo, em outras palavras, o nível de risco considera as consequências e a probabilidade, combinadas, a partir de algo. E esse "algo" deve ser considerado, no contexto da proteção de dados, um incidente de dados pessoais.

Assim, aferir o nível de risco em proteção de dados pessoais deve levar em consideração a probabilidade de acontecer um incidente de dados e as consequências (ou seja, o impacto), caso esse incidente se concretize: probabilidade *versus* consequência.

O que é relevante, então, nestes aspectos? Que o titular de dados esteja no centro de qualquer metodologia de avaliação de níveis de risco.

É dizer: avaliar um risco como "baixo", "médio", "alto" e "muito alto", por exemplo, não pode, para efeitos da proteção de dados pessoais, considerar a

empresa, o órgão público, enfim, qualquer agente de tratamento como centro dessa proteção.

O centro da avaliação de risco deve ser, sempre, o titular de dados pessoais, elemento basilar do sistema de proteção de dados pessoais estabelecido pela Lei Geral de Proteção de Dados, logo em seu artigo 1º: "[...] o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

Gomes (2020), acerca da avaliação de riscos, enfatiza esse entendimento:

> "(...) é necessário estabelecer indicadores mínimos de análise. Volume de dados, espécie dos dados (pessoal e/ou sensível) e tipo de titulares de dados, são, por exemplo, indicadores na avaliação do risco em operações de tratamento. **Se uma operação de tratamento possui um grande volume de dados, provenientes de crianças e que são sensíveis (dados de saúde, por exemplo), é possível qualificar essa operação de tratamento de dados como de alto risco.** E, a partir disso, analisar qual é o impacto dela nas liberdades civis e nos direitos fundamentais desses titulares".

E prossegue, logo após, a sustentar que "(...) o que será avaliado durante a realização da avaliação de impacto ou, especificamente, a avaliação de risco, é qual é a matriz de risco envolvida que está relacionada às liberdades civis e aos direitos fundamentais, das pessoas naturais que são os titulares de dados" (GOMES, 2020).

Logo, o que se propõe não é estabelecer uma metodologia definitiva para a avaliação dos níveis de risco. A proposta paira é sobre o foco que tais metodologias devem trazer: a proteção às liberdades civis e aos direitos fundamentais das pessoas naturais que são o centro de todo o sistema de proteção de dados pessoais.

A concluir, justifica-se a segunda parte do enunciado proposto: "O alto risco deve adotar como base critérios que evidenciem a proteção centralizada no titular de dados".

BIBLIOGRAFIA

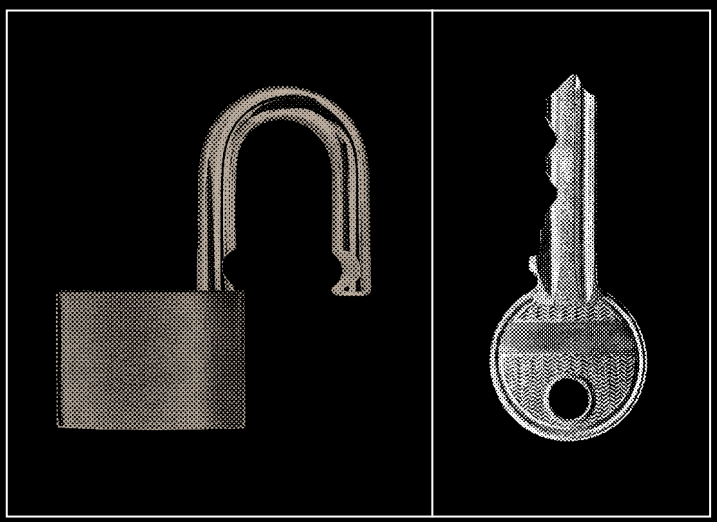
ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27000 – *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – princípios e vocabulário.* ABNT, 2018.

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/L13709.htm

CEOLIN, Isabely Pimentel. "O relatório de impacto à proteção de dados pessoais na LGPD". *Consultor Jurídico.* 2021. Disponível em: https://www.conjur.com.br/2021-set-02/ceolin-relatorio-impacto-protecao-dados-lgpd

GOMES, Maria Cecília O. "Entre o método e a complexidade: compreendendo a noção de risco na LGPD". In: *Temas atuais de proteção de dados.* PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, págs. 245-271.

VAINZOF, Rony. "A LGPD e o Relatório de Impacto à Proteção de Dados Pessoais". *Consultor Jurídico.* 2021. Disponível em: https://www.conjur.com.br/2021-jun-28/rony-vainzof-lgpd-relatorio-impacto-protecao-dados



RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO

ENUNCIADO

Como instrumento de gestão de riscos na prática negocial disforme, como nos contratos de adesão nas relações de consumo, é inválida a cláusula excludente do dever de indenizar, em caso de incidente de segurança com dados pessoais do titular, sob a responsabilidade dos agentes de tratamento, ressalvadas as hipóteses de excludentes legais.

José Emiliano Paes Landim Neto

JUSTIFICATIVA

O objetivo deste enunciado é voltado à análise da responsabilidade pelo fato do produto e do serviço em casos que haja incidente de segurança com dados pessoais do titular. O objeto do enunciado é posicionar a relação existente entre consumidor e fornecedor dentro do ordenamento jurídico, mais precisamente na inserção nos contratos de adesão de cláusulas que excluem a reparação por perdas e danos ou que fixam um teto máximo de reparação pecuniária.

Antes de adentrar especificamente na invalidade da cláusula excludente do dever de indenizar, necessário apresentar, ainda que brevemente, que o STJ tende a mitigar a teoria finalista para fins de se considerar que consumidor é todo aquele que se encontra em estado de vulnerabilidade[1], sendo este parte – hipossuficiente –, e não definidora dos direitos e das obrigações impostos pelo fornecedor.

O Código de Defesa do Consumidor (CDC), ao discorrer sobre os direitos do consumidor, exemplifica no artigo 6º, VI, que "são direitos básicos do consumidor: VI – a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos, tornando como medida eficaz de proteção ao consumidor a prevenção a fim de se evitar acidentes de consumo". Cita a prevenção e a reparação por consequência aos danos sofridos pelo consumidor, mostrando-se imprescindível, pois, a leitura do artigo 25 do CDC, que veda a estipulação contratual de cláusula que impossibilite, exonere ou atenue a obrigação de indenizar prevista na seção III, "Da responsabilidade por vício do produto e do serviço".

De acordo com artigo 51, I, são nulas de pleno direito, dentre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: I – impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos. Nas relações de consumo entre o fornecedor e o consumidor pessoa jurídica, a indenização poderá ser limitada, em situações justificáveis.

Vê-se, portanto, que a cláusula que exonera ou atenua a responsabilidade do fornecedor é nula de pleno direito em relação ao consumidor pessoa física[2], cabendo destacar que a LGPD veio a disciplinar o tratamento de dados pessoais de pessoas físicas (artigo 5º, V), o que vai ao encontro do disposto nos artigos 6º, VI, 25 e 51, I, do CDC, esclarecendo-se, ademais, que a própria LGPD estabelece, em seu artigo 45, que, em havendo violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente, o que deflui da permissiva coexistência entre as normas jurídicas do CDC e da LGPD em diálogo das fontes (artigos 7º do CDC e 64 da LGPD), tornando inválida cláusula de não indenizar em casos de incidentes de segurança com dados pessoais do titular, inclusive com a possibilidade de os agentes de tratamento responderem objetivamente pelos danos que causarem ao titular.

NOTAS

1 O STJ decidiu que "é relação de consumo a estabelecida entre o caminhoneiro que reclama de defeito de fabricação do caminhão adquirido e a empresa vendedora do veículo, quando reconhecida a vulnerabilidade do autor perante a ré" (STJ, AgRG no AREsp 426.563/PR, 4ª Turma., rel. ministro Luis Felipe Salomão, j. 3 de junho de 2014); STJ, RMS 27.512/BA, 3ª Turma., rel. min. Nancy Andrighi, j. 20 de agosto de 2009.

2 STJ, REsp 1.155.395/PR, 4ª Turma., rel. min. Raul Araújo, j. 1º de outubro de 2013.

BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm (acesso em 30 de junho de 2021).

BRASIL. Lei 8.078/1990 – Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm (acesso em 30 de junho de 2021).

BRASIL. Superior Tribunal de Justiça. AgRG no AREsp 426.563/PR, 4ª Turma., rel. ministro Luis Felipe Salomão, j. 3 de junho de 2014.

BRASIL. Superior Tribunal de Justiça. RMS 27.512/BA, 3ª Turma., rel. min. Nancy Andrighi, j. 20 de agosto de 2009.

BRASIL. Superior Tribunal de Justiça. REsp 1.155.395/PR, 4ª Turma., rel. min. Raul Araújo, j. 1º de outubro de 2013.

ENUNCIADO

A responsabilidade civil dos agentes de tratamento, na Lei Geral de Proteção de Dados Pessoais (LGPD), é subjetiva, aplicando-se o sistema da responsabilidade proativa, pelo qual o controlador, que detém melhores condições técnicas, deve comprovar o cumprimento dos requisitos legais.

Gabriela Souza e Silva, Renata Kelly Mercadante e Walter Barcellos Duque

JUSTIFICATIVA

A Lei Geral de Proteção de Dados Pessoais (LGPD) dedicou uma de suas seções para tratar, exclusivamente, das responsabilidades dos agentes de tratamento com relação ao ressarcimento dos danos ocasionados em virtude da violação à legislação. No entanto, sua redação é omissa quanto à especificação do regime de responsabilidade civil aplicado.

Ao contrário do que foi determinado pelo Código de Defesa do Consumidor (CDC), por exemplo, que deixa claro que a reparação dos danos causados aos consumidores independe da existência de culpa, a legislação referente à proteção de dados pessoais deixou uma lacuna sobre a necessidade de comprovação de culpa para haver indenização, assunto que gera debate entre os especialistas.

Contudo, antes de adentrarmos no mérito do enunciado em questão, cumpre-nos destacar alguns conceitos primordiais para embasar o conteúdo aqui exposto. Iniciaremos, portanto, com a apresentação das definições referentes à responsabilidade civil.

O Direito Civil Brasileiro contempla duas teorias relacionadas à caracterização das responsabilidades civis.

Conforme previsto no artigo 186 do Código Civil, aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Aqui, foi abordado o conceito da responsabilidade civil subjetiva, ou seja, para que haja a responsabilização pelo dano, deverá ser comprovada a culpa do agente.

Segundo Miguel Kfouri Neto (2003, pág. 61), os partidários da culpa como elemento fundamental da responsabilidade civil afirmam que a culpa possui um lastro moral, daí não se poder conceber a responsabilidade senão nela fundada. O homem se sente responsável, e obrigado, a reparar o dano causado por um ato culposo seu, o que não ocorre em relação a eventuais danos a que haja dado causa de modo absolutamente imprevisível, e pelos quais não se reconhece responsável, pois não os causou verdadeiramente.

Já no artigo 927, também do Código Civil, foi determinado que, aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.

Em seu parágrafo único, determinou que haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em Lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. Aqui, foi abordado o conceito de responsabilidade objetiva, a mesma utilizada para embasar as indenizações previstas no CDC.

Além dos conceitos supracitados, é importante salientarmos a definição de dano e culpa. Podemos caracterizar o dano como sendo o prejuízo expressamente sofrido. Nas palavras de Marcus Cláudio Acquaviva (1998, pág. 421):

> "Do latim *damnu*, prejuízo, perda. Prejuízo sofrido pelo patrimônio econômico ou moral de alguém. O dano pode ser material, também chamado real, quando

> atinge um bem economicamente apurável; ou moral, quando macula bens de ordem moral, como a honra".

Já a culpa caracteriza-se quando o agente causador do dano praticar o ato com negligência, imprudência ou imperícia. Nas palavras de Rui Stoco (2007, pág. 133):

> "Quando existe a intenção deliberada de ofender o direito, ou de ocasionar prejuízo a outrem, há o dolo, isto é, o pleno conhecimento do mal e o direito propósito de o praticar. Se não houvesse esse intento deliberado, proposital, mas o prejuízo veio a surgir, por imprudência ou negligência, existe a culpa (*stricto sensu*)".

Após a elucidação dos conceitos acima destacados, abordaremos o que a LGPD determinou acerca da responsabilidade dos agentes de tratamento e do ressarcimento de danos. Conforme previsto em seu artigo 42:

> "**Art. 42.** O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> **§ 1º** A fim de assegurar a efetiva indenização ao titular dos dados:
>
> **I** – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> **II** – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei".

Aqui, além da redação omissa quanto à especificação do regime de responsabilidade civil aplicado, também é importante destacarmos a responsabilidade solidária entre os agentes de tratamento, o que significa que o titular lesado poderá acionar qualquer uma das partes para obter a indenização. Mas e para os casos em que o agente acionado for aquele que não tiver agido com culpa, e este tiver de arcar com os prejuízos causados pela outra parte?

De acordo com a autora Maria Helena Diniz (2003, pág. 59), **não há responsabilidade sem culpa, exceto se houver disposição legal expressa, caso em que se terá a responsabilidade objetiva.**

Aqui, podemos destacar, novamente, a redação do Código Civil, em seu artigo 927, parágrafo único, o qual determinou que haverá a obrigação de reparar o dano, independentemente da culpa, nos casos especificados em Lei, por exemplo, o CDC, em seus artigos 12 e 14.

Deste modo, caso a legislação aplicável à proteção de dados pessoais entendesse que a responsabilidade dos agentes de tratamento é objetiva, teria delimitado em seu texto que o controlador ou o operador que, **independentemente da existência de culpa** e em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A ausência desta especificação abre espaço para que as partes possam decidir, conjunta ou individualmente, se a responsabilidade solidária determinada a elas ocorrerá com ou sem a constatação de culpa, o que é benéfico tanto para o titular de dados quanto para os agentes de tratamento envolvidos, pois, assim, o titular saberá que está sendo indenizado pela parte que ocasionou o seu prejuízo, enquanto a parte responsável irá arcar com os danos por ela causados.

Diante de todo o exposto, fica evidente que a LGPD pressupõe que a responsabilidade dos agentes de tratamento cursa no âmbito da subjetividade, em razão da possibilidade de comprovação da culpa das partes envolvidas no tratamento dos dados pessoais.

Portanto, é possível concluir que a subjetividade, objeto deste estudo, se sustenta pela omissão de argumentação factível para o efetivo enquadramento dos pressupostos de responsabilidade da Lei, garantindo a referida subjetividade em tela.

Em conclusão, vê-se que o legislador não optou pelo regime da responsabilidade objetiva, que seria, talvez, mais adequado à matéria dos dados pessoais, porque buscou ir além na prevenção, ao aventurar-se em um sistema que tenta, acima de tudo, evitar que danos sejam causados. Este novo sistema de responsabilização "proativa", nem subjetivo, nem objetivo, parece promissor; agora é tempo de aguardar seus resultados.

BIBLIOGRAFIA

ACQUAVIVA, Marcus Cláudio. *Dicionário jurídico brasileiro.* 9ª edição. São Paulo: Jurídica Brasileira, 1998.

BRASIL. Lei 8.078/1990. Código de Defesa do Consumidor. *Diário Oficial da União,* 1990.

BRASIL. Lei 10.406/2002. Código Civil. *Diário Oficial da União,* 2002.

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. *Diário Oficial da União,* 2018.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro.* 17ª edição. São Paulo: Saraiva, 2003.

JÚNIOR, Vital Borba de Araújo. "Responsabilidade subjetiva: a Teoria da Culpa". 2014. Disponível em:: https://www.iesp.edu.br/sistema/uploads/arquivos/publicacoes/responsabilidade-subjetiva-a-teoria-da-culpa.pdf (acesso em 2 de agosto de 2022).

KFOURI, Miguel Neto. "Responsabilidade civil do médico". 5ª edição. São Paulo: *Revistas dos Tribunais,* 2003.

Maria Celina Bodin de Moraes. "LGPD: um novo regime de responsabilização civil dito 'proativo'". Editorial à *Civilistica.com*. RJ: a. 8, nº 3, 2019.

SANTOS. Pablo de Paula Saul. "Responsabilidade Civil: origem e pressupostos gerais". 2012. Disponível em:: https://ambitojuridico.com.br/cadernos/direito-civil/responsabilidade-civil-origem-e-pressupostos-gerais/ (acesso em 2 de agosto de 2022).

STOCO, Rui. "Tratado de responsabilidade civil: doutrina e jurisprudência". 7ª edição. São Paulo: *Revista dos Tribunais,* 2007.

ENUNCIADO

As responsabilidades civil e administrativa previstas na LGPD não se aplicam ao encarregado pelo tratamento de dados, sem prejuízo de eventual responsabilidade contratual ou legal frente ao controlador.

Henrique Fabretti Moraes

JUSTIFICATIVA

A Lei Geral de Proteção de Dados estabelece (LGPD), em seu artigo 42, que o controlador e/ou o operador devem reparar os danos causados aos titulares de dados em decorrência das atividades de tratamento de dados pessoais que realizarem.

Ainda, o artigo 52 estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar sanções administrativas em caso de infração à LGPD pelo agente de tratamento.

Por sua vez, o artigo 5º, inciso IX, define como agentes de tratamento o controlador e o operador, que, por sua vez, são definidos nos incisos VI e VII do mesmo artigo, respectivamente, da seguinte forma:

> "**VI** – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> **VII** – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Já o encarregado pelo tratamento de dados pessoais é definido no artigo 5º, inciso VIII, da LGPD como a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

Portanto, é evidente que as figuras do controlador e operador não se confundem com a do encarregado e, portanto, este não foi alcançado pela responsabilidade civil prevista no artigo 42 da LGPD, nem figura como sujeito passível de receber as sanções administrativas previstas no artigo 52 da mesma lei.

A própria ANPD, no *Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado*, dispôs que "a responsabilidade pelas atividades de tratamento de dados pessoais continua sendo do controlador ou do operador de dados, conforme estabelece o artigo 42 da LGPD".

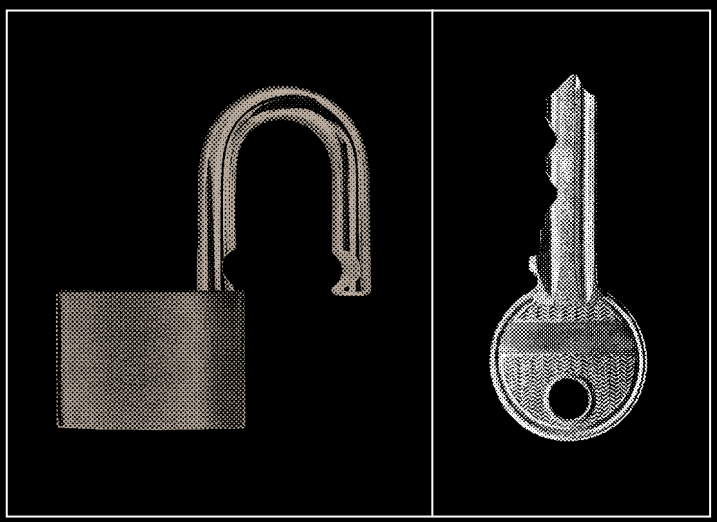
Tal entendimento também está em linha com a orientação do Grupo de Trabalho Artigo 29, que nas Guidelines on Data Protection Officers (DPOs), respondeu de forma expressa que o DPO não é pessoalmente responsável pela não conformidade com as regras de proteção de dados, uma vez que a responsabilidade pela conformidade com tais regras é do controlador e do operador de dados.

BIBLIOGRAFIA

ARTICLE 29 DATA PROTECTION WORKING PARTY. Guideline on Data Protection Officers (DPOs). Adotado em 13 de dezembro de 2016, com última revisão em 5 de abril de 2017.

BRASIL, Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. *Diário Oficial da União,* 2018.

MORAES, Henrique Fabretti. "Data Protection Officer – papéis, responsabilidades e boas práticas". In: OPICE BLUM, Renato (org.). *Proteção de dados: desafios e soluções na adequação à lei*. 2ª ed. rev. Rio de Janeiro: Forence, 2021. Págs. 49 - 64.



SANÇÕES ADMINISTRATIVAS E ATRIBUIÇÕES DA ANPD

ENUNCIADO

Nos termos do §4º, do artigo 52, da LGPD, a ANPD poderá determinar a utilização do faturamento do grupo econômico quando:

- houver pluralidade de agentes de tratamento pertencentes ao mesmo grupo econômico envolvidos na infração em apuração (artigo 52, *caput* LGPD);
- houver influência (direta ou indireta) de empresas do grupo econômico em determinada atividade de tratamento irregular, denotando participação, instrução ou colaboração na tomada de decisão do controlador de dados (artigo 5º, VI, LGPD); e
- quando a vantagem direta decorrente da infração seja percebida pelas empresas do grupo econômico (artigo 52, §1º, III, LGPD).

Tiago Neves Furtado e Helena Domingues Paes Landim

JUSTIFICATIVA

O artigo 52 da LGPD estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar multas financeiras[1] em caso de descumprimento da referida lei, e para determinar o seu valor, pode considerar até 2% (dois por cento) do **faturamento da empresa, grupo ou conglomerado no Brasil** no seu último exercício, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais).

Neste sentido, o §4º, do artigo 52, da LGPD trouxe 3 (três) hipóteses que preveem a **possibilidade** de a ANPD[2] utilizar o **faturamento do grupo econômico** como **base para cálculo da multa:**

- **HIPÓTESE 1:** quando não é possível identificar o faturamento do ramo de atividade empresarial em que ocorreu a infração;

- **HIPÓTESE 2:** quando o valor do faturamento for apresentado de forma incompleta, ou não for demonstrado de forma inequívoca e idônea; e

- **HIPÓTESE 3:** quando a ANPD determinar a utilização do faturamento do grupo econômico.

Sobre a **HIPÓTESE 3 (quando a ANPD determinar), a ANPD só deverá considerar esta possibilidade somente quando:**

- houver pluralidade de agentes de tratamento pertencentes ao mesmo grupo econômico envolvidos na infração em apuração (artigo 52, *caput* LGPD);

- houver **influência** (direta ou indireta) de empresas do grupo econômico em determinada atividade de tratamento irregular, denotando participação, instrução ou colaboração na tomada de decisão do controlador de dados (artigo 5º, VI, da LGPD); e

- a vantagem auferida pela infração for percebida pelas empresas do grupo econômico (artigo 52, §1º, III, da LGPD).

Ademais, em razão da ausência de parâmetros legais no Brasil, analisamos o cenário europeu para identificar quando os órgãos fiscalizadores consideram o faturamento do grupo econômico como base para cálculo de multas.

Não encontramos no Regulamento Europeu de Proteção de Dados Pessoais (General Data Protection Regulation – GDPR) a regulação destas hipóteses, mas, por outro lado, já há decisão que considera o critério da influência para justificar o uso do faturamento do grupo econômico para cálculo de multa, conforme comentário abaixo:

- *WhatsApp Ireland Limited e Facebook Inc. – DPC e EDPB*[3]: após a autoridade

irlandesa Data Protection Commission (DPC) estabelecer uma multa à empresa WhatsApp IE de 30 a 50 milhões de euros, o European Data Protection Board (EDPB) definiu, em decisão vinculante, que o valor da multa deveria considerar o faturamento do grupo de empresas Facebook, alcançando o valor de 225 milhões de euros. Para tanto, a decisão do EDPB levou em conta que o Facebook Inc. tinha influência decisiva e irrefutável em relação ao comportamento do WhatsApp IR no mercado[4].

Sobre o caso, um dos argumentos apresentados, com base na jurisprudência europeia[5], considerou que a composição e a participação das empresas quanto à infração cometida por uma delas corrobora com a presunção de que o faturamento do grupo determinaria a capacidade financeira da empresa em questão.

NOTAS

1 O artigo 52 da LGPD prevê a aplicação das seguintes sanções: (i) advertência; (ii) multa simples, de até 2% (dois por cento) do faturamento da empresa, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; (iii) multa diária; (iv) publicização da infração; (v) bloqueio dos dados pessoais; (vi) eliminação dos dados; (vii) suspensão parcial; (viii) suspensão máxima de 6 (seis) meses; e (ix) proibição parcial ou total das atividades.

2 Em que pese as hipóteses acima citadas servirem de orientação, o artigo 52, §4º, da LGPD é claro ao indicar que se trata de uma possibilidade facultada à ANPD, de modo que poderá determinar de forma diversa, a depender do caso prático. Tal fato decorre, especialmente, da competência investigativa e sancionatória da autoridade.

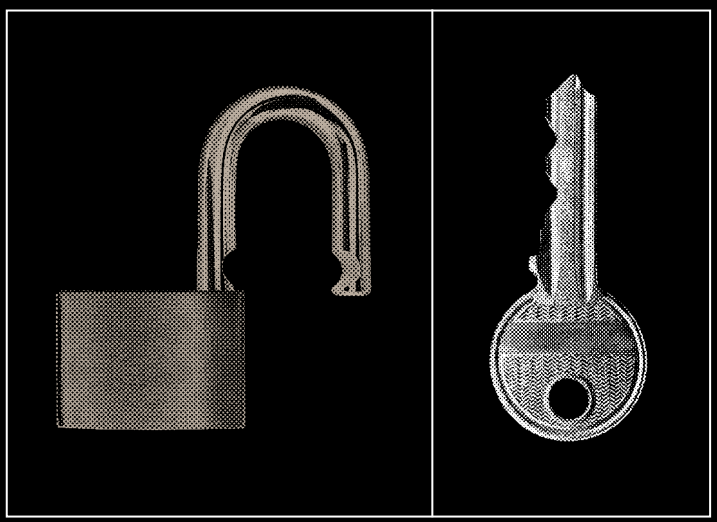
3 Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en (acesso em 24 de junho de 2022).

4 Disponível em: https://hsfnotes.com/data/2021/09/10/gdpr-fines-can-contemplate-parent-group-turnover-the-story-behind-the-whatsapp-fine/ (acesso em 24 de junho de 2022).

5 Akzo Nobel and Others v. European Commission (Case C-97/08 P, judgment delivered on 10 September 2009), ECLI:EU:C:2009:536, § 58-61. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:-62008CJ0097 (acesso em 24 de junho de 2022).

BIBLIOGRAFIA

BRASIL. Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Brasília/DF, Senado. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm



INTELIGÊNCIA ARTIFICIAL (IA) E TRATAMENTO AUTOMATIZADO DE DADOS

ENUNCIADO

Enunciado - Art. 5º, I: Dados inferidos relacionados a uma pessoa natural identificada ou identificável são considerados dados pessoais para os fins do Artigo 5º, I e II, da LGPD, mesmo se incompletos ou inexatos, permitindo o exercício dos direitos do titular previstos na LGPD.

Marco Aurélio Fernandes Garcia

JUSTIFICATIVA

O direito fundamental à privacidade, em sua faceta de proteção de dados pessoais, imputa a obrigação de estender a proteção dos dados pessoais às informações inferidas por máquinas que sejam relacionadas a uma pessoa natural identificada ou identificável. A LGPD é omissa neste ponto, muito embora essa proteção já tenha sido reconhecida em solo europeu pelo TJUE e pelo WP29, inclusive expressamente no "Caso Vyriausioji", julgado no início de agosto de 2022, que considerou que dados inferidos podem ser qualificados como dados pessoais sensíveis. Aplicando o teste da Opinião 4/2007, do WP29, verifica-se que dados inferidos são dados pessoais tanto em razão do conteúdo (fornecem informação sobre uma pessoa natural), do propósito (avaliar ou influenciar o *status* ou o comportamento de uma pessoa natural) e do resultado (potencialmente afetam os direitos e interesses de uma pessoa natural). Dados pessoais inferidos apresentam um particular potencial discriminatório e, mesmo se incompletos ou inexatos, devem permitir ao titular o exercício de seus direitos com fulcro em possibilitar, *inter alia,* o seu acesso, a sua correção e a sua exclusão.

BIBLIOGRAFIA

Brent Mittelstadt, Patrick Allo, Mariarosaria Toledo, Sandra Wachter, Luciano Floridi, "The Ethics of Algorithms: Mapping the Debate" (2016) Big Data & Society: https://journals.sagepub.com/doi/full/10.1177/2053951716679679

Felicitas Kraemer, Kees van Overveld, Martin Peterson, "Is There an Ethics of Algorithms?" [2011]13 Ethics and Information Technology 251

Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan, Cass Sunstein, "Discrimination in the Age of Algorithms" [2019] NBER Working Paper Series 25548,: https://www.nber.org/papers/w25548

Joshua Kroll, Solon Barocas, Edward Felten, Joel Reidenberg, David Robinson, Harlan Yu, "Accountable Algorithms" [2017] 165 University of Pennsylvania Law Review 633, 633-634

Lilian Edwards, Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For" [2017] 16 Duke Law & Technology Review 18

Luciano Floridi, "The Informational Nature of Personal Identity" [2011] 21 Minds & Machines 549, 557

Monique Mann, Tobias Matzner, "Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-discrimination in Responding to Emergent Discrimination" [2019] Big Data & Society 1

Sandra Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR" [2018] 34 Computer Law & Security Review 436

Sandra Wachter, Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" [2018] 2019(2) Columbia Business Law Review 22.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Casos C-465/00, 138/01 e 139/01, Rundfunk and others, 2003.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Ou, 2008.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-101/01, Bodil Lindqvist, 2003.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-70/10, Scarlet Extended SA v Societé Belge des auters, compositeurs et éditeurs SCRL (SABAM), 2011.

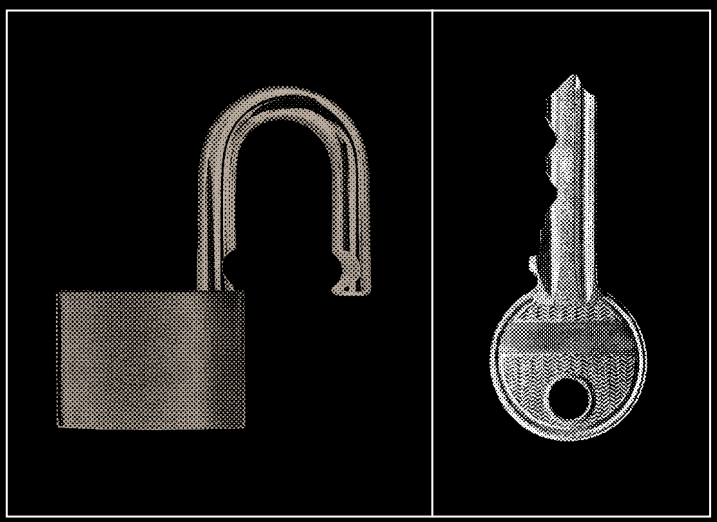
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-291/12, Michael Schwartz v Stadt Bochum, 2013.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-212/13, František Ryneš v Úrad pro ochranu osobních údaju, 2014.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Casos C-141/12 e 372/12, YS v Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel v M, S, 2014.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso 436/16, Peter Nowak v Data Protection Commissioner, 2017.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, Caso C-184/20, OT v Vyriausioji tarnybin s etikos komisija, 2022. §129.



REGULAMENTAÇÃO COMPLEMENTAR DE PROTEÇÃO DE DADOS PESSOAIS

ENUNCIADO

As normas coletivas poderão dispor sobre o tratamento dos dados pessoais no contexto das relações de emprego e regular, de forma específica, as condições e a forma de tratamento dos dados, principalmente no que se refere aos dados sensíveis, envolvendo os temas de saúde e segurança, igualdade e diversidade no trabalho, de forma a trazer segurança na adoção de condutas internas pelos empregadores e incentivar a adoção de boas práticas, sempre em respeito às disposições da Lei Geral de Proteção de Dados e do ordenamento jurídico.

Juliano Maranhão e Tatiana Bhering Roxo

JUSTIFICATIVA

Diante da existência de situações diversas envolvendo o tratamento de dados pessoais dos empregados, no contexto das relações de emprego e da necessidade de aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em consonância com o ordenamento jurídico trabalhista e suas peculiaridades, propõe-se que sindicatos/federações passem a regular pontos potencialmente conflituosos envolvendo o tratamento dos dados dos empregados, de forma a proteger o direito fundamental à proteção dos dados pessoais dos funcionários e, ao mesmo tempo, trazer segurança para os empregadores na adoção de novas condutas, de forma a prevenir conflitos. O Regulamento de Proteção de Dados Pessoais traz o assunto na Considerando 155, que inspirou o enunciado.

BIBLIOGRAFIA

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). Disponível em: https://gdprinfo.eu/pt-pt

AGRADECIMENTOS

Academia Internacional de Direito e Economia (Aide)

Associação Nacional dos Magistrados da Justiça do Trabalho (Anamatra)

DPOnet

GET

Opice Blum Academy

Portal Contábeis

Sindicato das Empresas de Compra, Venda e Administração de Imóveis (Secovi-SP)

Sindicato das Empresas de Serviços Contábeis e das Empresas de Assessoramento, Perícias, Informações e Pesquisas no Estado de São Paulo (Sescon-SP)

Sindicato do Comércio Varejista de Produtos Farmacêuticos no Estado de São Paulo (Sincofarma)

Universidade de São Paulo - Faculdade de Direito

Universidade Mackenzie

AGRADECIMENTO ESPECIAL AOS COORDENADORES DA COMISSÃO CIENTÍFICA

Fabrício Lima Silva
Iuri Pinheiro
Renato Opice Blum
Rony Vainzof
Vólia Bomfim

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)
Aline Graziele Benitez – Bibliotecária – CRB-1/3129

Lei geral de proteção de dados : LGPD : enunciados para auxiliar na garantia da segurança jurídica. – 1. ed. – São Paulo : D. H. Russo : Produções, 2022.
Bibliografia.
ISBN 978-65-993180-2-3

1. Direito à privacidade 2. Proteção de dados 3. Proteção de dados – Direito – Brasil 4. Proteção de dados – Leis e legislação 5. Proteção de dados pessoais.

22-130203 CDU-342.721(81)

Índices para catálogo sistemático:
1. Brasil : Proteção de dados pessoais : Direito
342.721(81)

REALIZAÇÃO

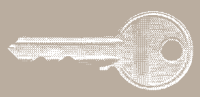
FECOMERCIOSP

PRESIDENTE
Abram Szajman

SUPERINTENDENTE
Antonio Carlos Borges

PRODUÇÃO

TUTU



COLABORAÇÃO

Annette Pereira

Beatriz Puertas P. Rossi

Dayane Oliveira Martins

Débora Maria Lima Machado

Edite Hupsel

Fábio Dacêncio Pereira

Gabriela Souza e Silva

Helena Domingues Paes Landim

Henrique Fabretti Moraes

Jéssica Cabrera Reis

José Emiliano Paes Landim Neto

Juliano Maranhão

Marco Aurélio Fernandes Garcia

Maria Beatriz Previtali

Maria Gabriela Grings

Pedro Luís Ventroni Pereira

Renata Kelly Mercadante

Renata Souto Baião

Tatiana Bhering Roxo

Thamara Consul S. Chaves

Tiago Neves Furtado

Walter Barcellos Duque

REALIZAÇÃO

FECOMERCIOSP

GET
Grupo Educacional Tríade

PARCERIA

OPICE BLUM
ACADEMY

DPOnet
Democratizando a LGPD

Contábeis
www.contabeis.com.br

APOIO

Universidade Presbiteriana
Mackenzie

SINCOFARMA
ESTADO DE SÃO PAULO

ACADEMIA INTERNACIONAL DE DIREITO E ECONOMIA

SECOVI SP
A CASA DO MERCADO IMOBILIÁRIO

45 ANOS ANAMATRA

SESCON-SP

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO

9 786599 318023