ANA FRAZÃO
RICARDO VILLAS BÔAS CUEVA
COORDENAÇÃO

COMPLIANCE E POLÍTICAS DE PROTEÇÃO DE DADOS

Diretora de Conteúdo e Operações Editoriais
JULIANA MAYUMI ONO

Gerente de Conteúdo
MILISA CRISTINE ROMERA

Editorial: Aline Marchesi da Silva, Diego Garcia Mendonça, Karolina de Albuquerque Araújo Martino e Quenia Becker

Gerente de Conteúdo Tax: Vanessa Miranda de M. Pereira

Direitos Autorais: Viviane M. C. Carmezim

Analista de Conteúdo Editorial: Juliana Menezes Drumond

Analista de Operações Editoriais: Alana Fagundes Valério

Analista de Conteúdo Editorial Júnior: Bárbara Baraldi

Estagiárias: Ana Amalia Strojnowski, Mariane Cordeiro e Mirna Adel Nasser

Produção Editorial
Gerente de Conteúdo
ANDRÉIA R. SCHNEIDER NUNES CARVALHAES

Especialistas Editoriais: Gabriele Lais Sant'Anna dos Santos e Maria Angélica Leite

Analistas de Operações Editoriais: Caroline Vieira, Damares Regina Felício, Danielle Castro de Morais, Mariana Plastino Andrade, Mayara Macioni Pinto, Patrícia Melhado Navarra e Vanessa Mafra

Analistas de Qualidade Editorial: Ana Paula Cavalcanti, Fernanda Lessa e Victória Menezes Pereira

Estagiárias: Bianca Satie Abduch, Gabrielly N. C. Saraiva, Maria Carolina Ferreira e Sofia Mattos

Capa: Linotec

Líder de Inovações de Conteúdo para Print
CAMILLA FUREGATO DA SILVA

Equipe de Conteúdo Digital
Coordenação
MARCELLO ANTONIO MASTROROSA PEDRO

Analistas: Gabriel George Martins, Jonatan Souza, Maria Cristina Lopes Araujo e Rodrigo Araujo

Gerente de Operações e Produção Gráfica
MAURICIO ALVES MONTE

Analistas de Produção Gráfica: Aline Ferrarezi Regis e Jéssica Maria Ferreira Bueno

Assistente de Produção Gráfica: Ana Paula de Araújo Evangelista

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Compliance e Política de Proteção de Dados / Ricardo Villas Bôas Cueva, Ana Frazão, coordenação. -- São Paulo : Thomson Reuters Brasil, 2021.

Vários autores.
Bibliografia.
ISBN 978-65-5991-540-8

1. Compliance 2. Direito à privacidade 3. Direito à privacidade - Brasil 4. Programas de compliance 5. Proteção de dados - Leis e legislação 6. Proteção de dados pessoais 7. Risco - Avaliação I. Cueva, Ricardo Villas Bôas. II. Frazão, Ana.

21-88641 CDU-342.721

Índices para catálogo sistemático:
1. Compliance : Proteção de dados pessoais : Direito 342.721

Cibele Maria Dias - Bibliotecária - CRB-8/9427

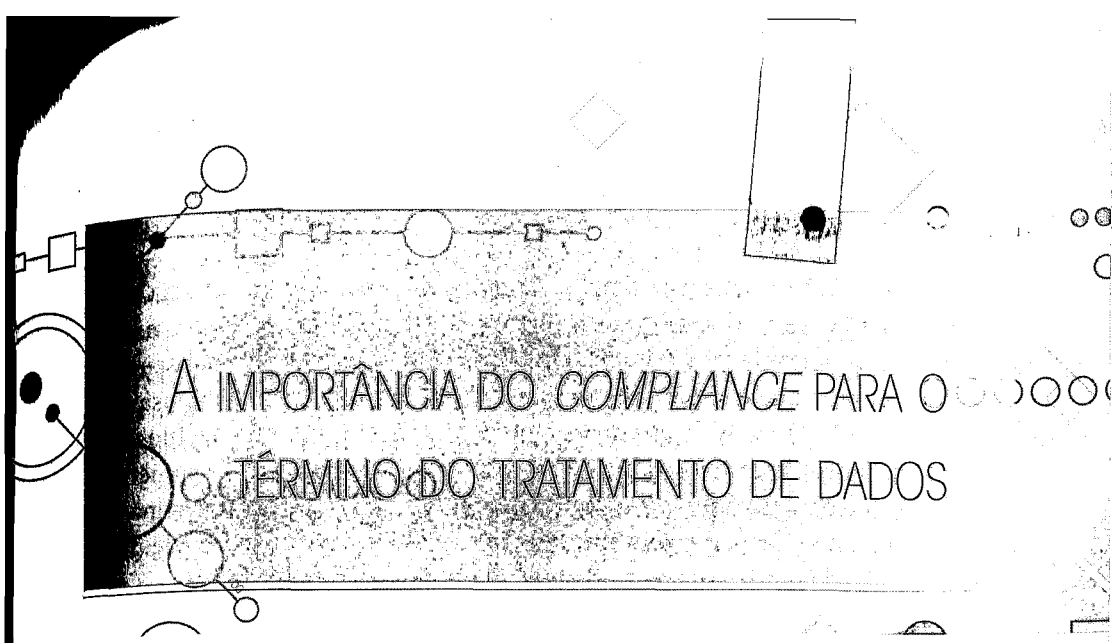
ANA FRAZÃO
RICARDO VILLAS BÔAS CUEVA
COORDENAÇÃO

COMPLIANCE E POLÍTICAS DE PROTEÇÃO DE DADOS

THOMSON REUTERS
REVISTA DOS TRIBUNAIS™

Sumário

Parte III
PRÁTICAS E PROCEDIMENTOS DOS PROGRAMAS DE *COMPLIANCE* E DAS POLÍTICAS DE PROTEÇÃO DE DADOS



A IMPORTÂNCIA DO *COMPLIANCE* PARA O TÉRMINO DO TRATAMENTO DE DADOS

GISELA SAMPAIO DA CRUZ GUEDES[1]

ROSE MELO VENCELAU MEIRELES[2]

Sumário: 1. Introdução; 2. Término do tratamento de dados; 3. O *compliance* no término de tratamento de dados; 4. O impacto dos programas de *compliance* na responsabilidade civil; 5. Conclusão.

"In questo momento storico, il termine 'privacy' sintetiza appunto um insieme di potere che, originati dall'antico núcleo dell diritto a essere lasciato in pace, si sono via via evoluti e diffusi nella società proprio per consentire forme di controllo sui diversi soggetti che exercitanp la sorveglianza".

– Stefano Rodotà, *Il mondo in rete*.

1. Doutora e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ. Professora Adjunta de Direito Civil da UERJ. Professora Permanente do Programa de Pós-Graduação em Direito (Mestrado e Doutorado) da UERJ. Professora dos cursos de pós-graduação da PUC-Rio, do CEPED/UERJ, da EMERJ, da EPM e da AASP. Advogada, parecerista e árbitra.
2. Doutora e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ. Professora Adjunta de Direito Civil da Faculdade de Direito da UERJ. Procuradora da UERJ. Advogada.

1. Introdução

A Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais ou "LGPD") considera dado pessoal qualquer informação relacionada à pessoa natural identificada ou identificável (art. 5º, I); diferenciando o dado pessoal sensível, entendido como aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II). Assim, a LGPD destina-se a tutelar e regulamentar as relações jurídicas que envolvam o tratamento de dados pessoais realizado por pessoa natural ou jurídica que a eles tenham acesso.

A regulamentação estabelecida pela LGPD baseia-se, precipuamente, na tutela conferida pela Constituição da República Federal ("CF") à inviolabilidade e à intimidade da vida privada, reconhecidas como verdadeiros direitos fundamentais (art. 5º, X, CF). A tutela dos dados pessoais conferida pela LGPD situa-se, precisamente, nesse amplo aspecto da vida privada. Nesse sentido, o Supremo Tribunal Federal, no julgamento de medida cautelar na ADI n.º 6.389, reconheceu a existência do direito à proteção de dados pessoais como uma garantia fundamental presente na ordem constitucional brasileira.[3]

Dessa forma, toda e qualquer situação que envolva o manuseio e o tratamento de informações pessoais pelo controlador ou operador, há de levar em consideração que a titularidade dos dados tratados pertence à pessoa natural (LGPD, art. 5º, V), que estará amparada pela garantia constitucional da liberdade e privacidade, sob pena de lesão a esses direitos.

Nesse contexto, os programas de compliance mostram-se instrumentos valiosos para adequação das condutas e processos organizacionais à LGPD e, em última análise, ao comando constitucional. Tais programas acompanham todo o fluxo de informações, desde a sua obtenção até a sua eliminação. Não é demais pontuar, ainda de forma introdutória, que a manipulação de dados pessoais com

3. Vide trecho da ementa: "1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos" (STF, ADI 6.389/DF, Rel. Min. Rosa Weber, julg. 07.05.2020).

o garantismo de direitos fundamentais depende da consolidação de uma cultura da informação em que o compliance exerce papel importantíssimo. Com esse viés, o foco deste trabalho situa-se no tratamento de dados no âmbito da atividade econômica, inserida na proteção da dignidade humana.

A princípio, será abordado o término do tratamento de dados. Ora, na medida em que a titularidade dos dados não se transmite ao controlador ou ao operador, o tratamento apresenta-se como ambulatório, tendente a acabar. Por isso, é relevante discorrer sobre a importância dos programas de integridade, sobretudo na fase do término do tratamento de dados, já que as normas trazidas pela LGPD são, na maioria das vezes, genéricas, a depender de regulação interna para seu cumprimento. Além disso, não se poderia deixar de abordar o impacto do compliance na responsabilidade civil. É verdade que a não observância da LGPD pode acarretar sanções administrativas e civis. Nesse sentido, o compliance, ou conformidade, pode auxiliar as organizações a se adequarem a essa nova perspectiva da informação pessoal.

2. TÉRMINO DO TRATAMENTO DE DADOS

Já em 2018, a Lei n.º 12.965, o Marco Civil da Internet, no seu art. 7º, inciso X, previu a exclusão dos dados pessoais como um direito do usuário da internet:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> (...)
>
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei".

A finalidade do dispositivo é a de permitir ao usuário o controle das suas informações, conferindo-lhe o direito de solicitar a exclusão definitiva dos seus dados pessoais ao final da relação entre as partes, caso entenda conveniente.[4] Além dessa previsão específica de exclusão dos dados por requerimento do titular, o Marco Civil da Internet também regulamenta as hipóteses em que a guarda dos dados será vedada, conforme previsto em seu art. 16:

> "Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

4. BITELLI, Marcos Alberto Sant'Anna. "A Lei 12.965/2014 – O marco civil da internet", *Revista de Direito das Comunicações*, vol. 7/2014, pp. 291-333, jan.-jun./2014, p. 11.

> I – dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
>
> II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular".

Observa-se que a previsão do Marco Civil da Internet traz dois aspectos fundamentais quanto à guarda dos dados repetidos na LGPD: i) o consentimento; e ii) a finalidade específica. A eficácia do consentimento condiciona-se à finalidade das operações envolvendo as informações pessoais, atribuindo-se, assim, ao titular maior controle dos dados.[5]

Na LGPD, as hipóteses em que se observará o término do tratamento de dados pessoais (em geral) foram regulamentadas no art. 15:

> "Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> II – fim do período de tratamento;
>
> III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
>
> IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei".

Essas hipóteses de término do tratamento de dados pessoais estipuladas pelo art. 15 da LGPD podem ser organizadas da seguinte forma: i) término pelo esgotamento funcional da utilização dos dados; ii) término pelo prazo; iii) término pela autodeterminação do titular; e iv) término por ilegalidade.[6]

---

5. "Este consentimento pode ser concedido, basicamente, de duas maneiras: por meio do opt-in (sistema por meio do qual o titular tem de dar seu consentimento expressamente antes de haver a coleta e uso de dados) ou o opt-out (sistema por meio do qual o titular opta por não dar o consentimento, após coleta ou eventual uso dos dados)" (RIBEIRO, Juliana Tedesco Racy. "Proteção dos dados pessoais no direito brasileiro". In: *Panorama legal sobre as relações de consumo no Brasil*, São Paulo: Editora Singular, 2017, p. 89). O legislador brasileiro optou pelo sistema opt-in, conforme artigo 8º da LPDP.
6. Como ressalta a doutrina, "um dos requisitos de validade do tratamento de dados é o limite de atuação do procedimento, e tal ideia é relativa tanto ao limite de informações

Em relação ao término pelo esgotamento funcional da utilização dos dados, destaca-se o fato de uma das preocupações centrais da LGPD ser, justamente, a finalidade específica do tratamento que se faz dos dados. Nesse sentido, o art. 6º da referida lei enuncia como norteadores das atividades de tratamento de dados os princípios da finalidade, da adequação e da necessidade. Ora, a realização do tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Além disso, esse tratamento deve ser realizado de forma compatível ou adequada com as finalidades informadas ao titular, de acordo com o contexto do tratamento e, ainda, no limite do mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento. Utiliza-se do princípio da proporcionalidade, ou seja, o tratamento dos dados é protegido na medida em que o meio é adequado e necessário para o fim almejado. No término pelo esgotamento funcional, respeita-se a função (para que serve) do tratamento de dados.

Assim, se a finalidade consiste em coleta de dados para acesso a conteúdos gratuitos de um *blog* ou jornal eletrônico, não podem eles ser mantidos para envio de material de *marketing* não especificado. A finalidade pode ser continuada ou não. O tratamento de dados para uma compra *on-line*, por exemplo, esgota-se com a finalização da própria compra, salvo se o titular autorizar o armazenamento dos dados para compras futuras. Da mesma forma, os dados coletados para a concessão de um financiamento de um imóvel, por exemplo, devem ser eliminados tão logo a análise da concessão seja efetuada. Já na hipótese de término pelo prazo, o tratamento de dados está vinculado a um lapso temporal específico, cujo fim obstará qualquer operação com aqueles dados coletados.

Diante dessas duas hipóteses de término do tratamento, nota-se que é possível, de um lado, haver um lapso funcional e, de outro, um lapso temporal, ao término dos quais devem ser finalizadas as operações dos dados pessoais respectivos. Essas duas primeiras hipóteses decorrem do princípio do consentimento – ou autodeterminação informativa, como foi nomeado na seara da proteção de dados. Isto é, a finalidade e o tempo constituem limites estabelecidos pela autodeterminação. Veja-se que, para os fins da LGPD, consentimento consiste na "manifestação livre, informada e inequívoca pela qual o titular concorda com

---

a serem coletadas quanto à finitude do procedimento no tempo" (PINHEIRO, Patricia Peck. *Proteção de dados pessoais*: comentários à Lei n. 13. 709/2018 (LGPD), 3. ed. São Paulo: Saraiva, 2021, p. 36).

o tratamento de seus dados pessoais para uma finalidade determinada" (LGPD, art. 5º, XII). Significa dizer que o consentimento desvinculado da finalidade ou do tempo para o qual foi concedido não é, de fato, um verdadeiro consentimento e, portanto, não pode ser considerado legítimo.

Ao mesmo tempo, a terceira hipótese de término – pela autodeterminação do titular – busca resguardar o interesse público e consagra o que se chamou de princípio do consentimento qualificado.[7] A respeito da importância do consentimento na disciplina dos atos de conteúdo não patrimonial, sublinha-se constantemente a exigência – mais que isso, a necessidade – de que o consenso do autor do ato seja pleno, efetivo, nunca presumido, atual, espontâneo, consciente, informado: características, essas, nem sempre requeridas com a mesma intensidade para a validade dos contratos, nos quais se registra uma impostação prevalentemente objetiva. Assim, o princípio do consentimento qualificado atribui à vontade interna do declarante uma relevância que nas situações patrimoniais não existe. Note-se que o termo "qualificado" é utilizado para se evidenciar a maior importância dada à vontade subjetiva do declarante.

Como corolário do princípio do consentimento qualificado, tem-se, especialmente, as seguintes consequências para o regulamento das situações jurídicas subjetivas existenciais: i) a vontade interna deve prevalecer sobre a declarada; ii) a manifestação de vontade é pessoal; iii) a manifestação de vontade é revogável. A revogabilidade decorre do princípio do consentimento qualificado, sobretudo quando da disposição resulte limitação ao exercício de direito da personalidade, pois somente a limitação voluntária é admissível. A revogabilidade do consentimento é marcante na LGPD,[8] prevista como uma das hipóteses de término do tratamento de dados pessoais.[9]

---

7. Sobre o ponto, vide MEIRELES, Rose Melo Vencelau. *Autonomia privada e dignidade Humana*, Rio de Janeiro: Renovar, 2009.

8. Sobre a revogação do consentimento na LGPD, o § 5º do art. 8º da LGPD determina que poderá o consentimento ser revogado "a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei". Note-se que o legislador não fixa parâmetros ou limites ao direito de revogar o consentimento, o que parece querer dizer que se trata de ato puramente volitivo do titular.

9. Explica a doutrina que: "A revogação manifestada pelo titular, evidentemente, somente conduz ao fim do tratamento quando o consentimento foi o motivo que o autorizou. Nas outras várias situações em que o tratamento é permitido, especialmente

Imagine-se, por exemplo, o consentimento de uso de dados pessoais para determinada pesquisa científica oferecido por uma pessoa natural quando ainda criança, e, naturalmente, sem conhecimento de todos os riscos inerentes à tal concessão. Nessa hipótese, esse consentimento poderá, mais tarde, ser suprimido, de modo a se excluir os dados pessoais, inclusive da internet. Por envolver direitos da personalidade, ainda antes da maioridade pode ser requerido o término do tratamento[10]. Em contrapartida, eventual conservação dos dados pessoais, como será visto a seguir, poderá ocorrer em situações específicas, nas quais o legislador limitou a autodeterminação do sujeito para tutelar outro interesse que, sopesado com a autonomia, haveria de prevalecer no caso concreto.

Finalmente, a quarta hipótese de término é a determinação da autoridade nacional de proteção de dados nos casos em que houver alguma violação aos preceitos da LGPD.

A consequência do término do tratamento dos dados pessoais é, naturalmente, a sua eliminação que, em regra, deve ser automaticamente realizada.[11] Nesses termos, o art. 16 da LGPD assim dispõe:

> "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I – cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados".

---

quando contra a vontade do titular, não cabe a este proibi-lo, ao menos enquanto perdurarem no tempo os motivos que configuram a autorização legal" (MARCACINI, Augusto Tavares Rosa. "Regras aplicadas ao tratamento de dados pessoais". In: LIMA, Cíntia Rosa Pereira (coord.). *Comentários à lei geral de proteção de dados*. São Paulo: Almedina, 2020, p. 159).

10. MENDES, Jorge Barros. "O novo regulamento de proteção de dados", *Revista luso*, vol. 27, set./2017, Pronta.indd 13, p. 26.

11. Caso os dados não sejam automaticamente eliminados com o término do tratamento, o titular dos dados pessoais poderá pleitear a sua eliminação, nos termos do art. 18, VI, da LGPD.

Admite-se, então, excepcionalmente, a conservação dos dados apenas para se alcançar as finalidades disciplinadas na lei, e, por ser regra de exceção, a interpretação deve ser restritiva, de forma a não admitir outras hipóteses, ainda que análogas. A primeira exceção é a conservação para o cumprimento de dever legal ou regulatório pelo controlador. Da mesma forma, em caso de tratamento realizado para estudo em pesquisa científica, os dados podem ser mantidos, garantida a anonimatização, sendo essa a segunda exceção. Veja-se, nesse caso, o exemplo da pesquisa clínica para desenvolvimento de novos medicamentos, cujas informações pessoais de determinado participante não podem ser removidas do conjunto de dados da pesquisa sem afetar seu resultado estatístico e, portanto, a própria comprovação científica da eficácia e da segurança do medicamento em fase de testes. A terceira exceção apresenta-se na hipótese em que as informações são transferidas a terceiros: desde que respeitados os requisitos para o tratamento de dados, não há eliminação. Por fim, não são eliminados os dados para uso exclusivo do controlador, garantida a anonimatização.

Vale, ainda, mencionar que o legislador não previu qualquer prazo para a conservação dos dados pessoais nas hipóteses do referido artigo. O Marco Civil da Internet, por outro lado, determina que o provedor de aplicações de internet "deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento" (art. 15). Com efeito, na ausência de lapso temporal para a guarda ou conservação dos dados pessoais, poder-se-ia aplicar o prazo previsto no Marco Civil da Internet[12] ou, até mesmo, entender-se que não há qualquer limitação temporal.

Em síntese, a regra geral é a completa eliminação dos dados pessoais pelo controlador quando o tratamento se encerra, nos moldes do art. 16 da LGPD. Trata-se de modelo que visa a diminuir os riscos do uso não autorizado ou indevido das informações pessoais, buscando uma maior tutela do seu titular.

Analisadas as principais características do término do tratamento de dados no âmbito da LGPD, passa-se à análise da importância do compliance nesse momento de eliminação dos dados já tratados pelos controladores.

3. O *COMPLIANCE* NO TÉRMINO DE TRATAMENTO DE DADOS

Os programas de compliance visam fomentar a eticidade e a legalidade no âmbito da gestão empresarial. Com efeito, o art. 170 da Constituição da

12. Nesse sentido, consulte-se RIBEIRO, Juliana Tedesco Racy. "Proteção dos dados pessoais no direito brasileiro", cit., p. 89.

República estabelece que a ordem econômica tem por fim assegurar a todos existência digna, o que, em última análise, concretiza-se também a partir da função social da empresa.[13] Nesse sentir, a atividade empresarial há de se emoldurar a partir do atendimento a valores e a normas voltadas para a garantia da dignidade humana e da justiça social, sendo o compliance valioso meio para a formação dessa moldura normativa.

Trata-se de programa, integrante das boas práticas de governança corporativa, que estabelece ferramentas para a conformidade da atividade empresarial com a normativa vigente, com objetivo de prevenir, identificar ou punir irregularidades praticadas na própria empresa ou por colaboradores. Na medida em que há diversos modelos de negócio, o desenvolvimento do programa de compliance é único para cada empresa, a ser customizado de acordo com as peculiaridades de sua atividade. Não obstante, verifica-se quatro pilares fundamentais na construção de um programa de compliance: i) o comprometimento da alta gestão, ii) o constante mapeamento e análise de riscos, iii) a reunião dos valores e normas em um Código de Conduta e iv) monitoramento constante das atividades empresariais.[14]

A alta gestão da empresa, constituída pelos executivos dos mais altos cargos, deve estar comprometida com o atendimento das conformidades, de modo

13. "Função social da empresa é princípio que decorre de um conjunto de normas presentes no ordenamento jurídico brasileiro, e que tem como objetivo fazer com que o Direito logre êxito na busca pela justiça social preconizada pela Constituição Federal" (SIQUEIRA, Vitor da Costa Honorato de. "O surgimento dos programas de compliance e sua aplicação na seara trabalhista à luz da função social da empresa". *Revista dos Tribunais*, vol. 1019. São Paulo: Revista dos Tribunais, set. 2020, pp. 319-332).

14. Acerca da estruturação de um programa de compliance robusto, Ana Frazão, Milena Donato Oliva e Viviane Abílio enumeram 10 pontos centrais: i) avaliação contínua de riscos e atualização do programa, ii) elaboração de códigos de ética e conduta; iii) organização compatível com o risco da atividade; iv) comprometimento da alta administração; v) autonomia e independência do setor de compliance; vi) treinamentos periódicos; vii) criação de uma cultura corporativa de respeito à ética e às leis; viii) monitoramento constante dos controles e processos, inclusive para fins de atualização do programa; ix) canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes; x) detecção, apuração e punição de condutas contrárias ao programa de compliance (FRAZÃO, Ana; OLIVA, Milena Donato; e ABILIO, Vivianne da Silveira. "Compliance de dados pessoais". In: TEPEDINO, Gustavo; FRAZÃO, Ana; e OLIVA, Milena Donato (coord.). *Lei geral de proteção de dados pessoais e suas repercussões no Direito brasileiro*, 2.ª ed., São Paulo: RT, 2020, pp. 687-697).

a transparecer a sua importância para toda a organização. O mapeamento e a análise dos riscos, por sua vez, apresenta-se central porque o objetivo primeiro do compliance é eliminar os riscos próprios da atividade. O Código de Conduta mostra-se relevante por reunir todos os valores, normas, processos e meios de controle, a nortear a conduta de todos, gestores, empregados e colaboradores. Por fim, o compliance requer o acompanhamento constante do atendimento do Código de Conduta estabelecido. Apenas com a verificação do cumprimento das normas é possível amadurecer e aperfeiçoar as normas de compliance.

A instituição de um programa de compliance efetivo – que não seja, obviamente, apenas de fachada, para "inglês ver"[15] – provoca verdadeira mudança de cultura no bojo da sociedade, fomentando entre seus empregados, clientes, parceiros e colaboradores o respeito a uma cultura corporativa séria, com a observância das normas legais.[16] Por estimular o cumprimento dos comandos legais, a implementação de um programa de compliance efetivo normalmente é levada em consideração, por exemplo, pelos órgãos reguladores na dosimetria da pena, servindo como potencial atenuante de sanções administrativas. Atentos a isso, os empresários têm procurado adequar-se a essa nova realidade, até para, aos poucos, construir a reputação das empresas sob o seu comando.

O impacto reputacional de um programa de compliance bem-feito é inegável, tanto mais agora diante da crescente relevância dos fatores ESG.[17] A si-

15. Como já observado, "[a] mera elaboração de políticas de compliance que carecem de efeitos na prática corporativa – os chamados 'programas de papel' – não consiste em mecanismo de efetivo autocontrole. Por consequência, a tendência é que sejam desconsiderados pelos órgãos regulatórios, sem que resultem na atenuação das sanções a serem aplicadas. Um 'programa de fachada', que não preencha os requisitos mínimos ou que preencha apenas formalmente, pode de fato resultar em penalidades maiores do que aquelas que seriam aplicáveis em sua ausência. Com efeito, ressalta-se que um programa de compliance mal concebido, que não envolva suficientemente as lideranças corporativas ou careça do suporte financeiro para seu regular desempenho dissemina entre os funcionários de que o programa é um embuste" (FRAZÃO, Ana; OLIVA, Milena Donato; e ABILIO, Vivianne da Silveira. "Compliance de dados pessoais", cit., p. 678).

16. Há quem entenda, inclusive, que a implementação de um programa de compliance é "condição para o atingimento da função social da empresa" (SIQUEIRA, Vitor da Costa Honorato de. "O surgimento dos programas de compliance e sua aplicação na seara trabalhista à luz da função social da empresa", cit., pp. 324 e seguintes).

17. Para mais informações sobre os fatores ESG, vale conferir: "ESG de A Z: Tudo o que você precisa saber sobre o tema", relatório elaborado pela XP Investimentos, disponível em: < https://conteudos.xpi.com.br/esg/esg-de-a-a-z-tudo-o-que-voce-precisa-saber-sobre-o-tema/>. Acesso em 31.05.2021.

gla "ESG" advém do termo em inglês "Environmental, Social and Governance" (ou, em português, ASG, referindo-se a "Ambiental, Social e Governança"). Nos últimos anos, investidores de toda parte do mundo se engajaram na busca do chamado "investimento responsável", impulsionado pela crescente conscientização de questões como mudanças climáticas, diversidade de gênero, políticas de anticorrupção etc. É no "S", de social, em que se situa o debate sobre proteção de dados pessoas. Embora as discussões acerca dos fatores ESG tenham ganhado notoriedade apenas recentemente no Brasil, quando se volta para o restante do mundo fica evidente que esse assunto não é novo e, mais do que isso, que não se trata de uma tendência passageira, mas antes de uma nova realidade que veio para ficar.[18] Os programas de compliance inserem-se perfeitamente nessa nova realidade em que a palavra de ordem é *prevenção*.

São, enfim, inúmeras as vantagens atribuídas aos programas de compliance, mas aqui, para efeito deste artigo, importa destacar três delas, por estarem mais ligadas à responsabilidade civil: (i) os programas de compliance auxiliam os empresários a realizar uma adequada gestão dos riscos da atividade, porque permitem identificar os chamados pontos sensíveis, em que há maior exposição a riscos e, consequentemente, mais chance de a sociedade vir a ser responsabilizada;[19] (ii) com a identificação das fragilidades, os programas acabam ajudando na implementação de medidas preventivas, que vão diminuir as chances de ocorrerem danos;[20] e, finalmente, (iii) auxiliam também na remediação/mitigação dos danos eventualmente existentes.

---

18. Do lado ambiental, discute-se o uso de recursos naturais, emissões de gases de efeito estufa (CO2, gás metano), eficiência energética, poluição, gestão de resíduos e efluentes. Já em relação aos fatores sociais, a discussão passa pelas políticas adotadas quanto às relações de trabalho, inclusão e diversidade, engajamento dos funcionários, treinamento da força de trabalho, direitos humanos, relações com comunidades, privacidade e proteção de dados. No aspecto da governança, também são inúmeras as discussões: independência do conselho de administração, política de remuneração da alta administração, diversidade na composição do conselho de administração, estrutura dos comitês de auditoria e fiscal, ética e transparência.

19. FRAZÃO, Ana; OLIVA, Milena Donato; e ABILIO, Vivianne da Silveira. "Compliance de dados pessoais", cit., p. 678.

20. Nesse sentido: "Diante desta nova premissa, o Compliance, que é compreendido como um sinônimo de prevenção, pode assumir um importante papel na sociedade. O conceito de Compliance pode ser ampliado, ao ser pensado um programa de Criminal Compliance como busca de enquadramento ético de uma entidade empresarial, face à nova sociedade globalizada, inclusive quanto ao fato de buscar isenção de responsabilidades em fatos, que ainda não estejam previstos em lei, como por exemplo, as

Antes mesmo da elaboração do programa de compliance, há uma primeira fase em que serão identificados os pontos mais vulneráveis da empresa, tornando-se possível avaliar os riscos aos quais ela mais constantemente se submete. Nessa fase, tenta-se antecipar todas as questões mais delicadas, com potencial de gerar contingências futuras. O propósito dessa fase, que antecede a própria elaboração do programa, não é outro senão o de mapear possíveis problemas com potencial de gerar a responsabilização da pessoa jurídica. É essa fase que "garante que os programas não sejam reduzidos a medidas meramente profiláticas, orientadas por *standards* universalmente válidos que, na maioria dos casos, diz pouco ou nenhum respeito à dinâmica concreta dos negócios e às especificidades das empresas ou grupos econômicos nos quais se implementam os programas".[21]

Identificados os problemas, passa-se, então, para uma segunda fase de análise mais pormenorizada dos riscos, que permitirá a elaboração de um programa de compliance personalizado, capaz de antecipar questões concretas e apontar possíveis soluções. Ainda antes do programa de compliance, serão elaborados códigos de ética e de conduta que expressem, por escrito, os valores e os princípios da entidade, a serem observados não só pelos seus funcionários, mas também pelos seus parceiros e colaboradores. Esses códigos servirão como espécie de guia, verdadeira norma de conduta que deverá conduzir aquela comunidade que gira em torno da empresa.

Apenas na terceira fase é que o programa de compliance é elaborado, com o objetivo de criar uma cultura corporativa compatível com a legislação que regula o setor. O programa deve trazer regras objetivas e concretas para aquela realidade, aptas a prevenirem situações com potencial de gerar danos e estabelecerem as correspondentes sanções em caso de descumprimento. O programa deve criar também um canal de comunicação seguro dentro da empresa para receber denúncias, identificadas ou anônimas, de casos que contrariem as normas estabelecidas. A alta administração precisa participar desse processo não só para dar o exemplo, mas também para garantir que o programa será implementado e cumprido.

---

nanotecnologias" (TONIN, Alexandre Baraldi. "*Compliance*: uma visão do compliance como forma de mitigação de responsabilidade", *Revista dos Tribunais*, vol. 983. São Paulo: RT, set. 2017, p. 268).

21. Saad-Diniz, Eduardo. "Análise qualitativa sobre a implementação dos programas de compliance no Brasil (2014-2019)". *Revista dos Tribunais*, vol. 1027. São Paulo: RT, mai. 2021, p. 46.

Na quarta fase, passa-se para a implementação propriamente dita do programa de compliance. É nessa quarta fase que o programa será posto a teste, então é importante que seja criado um setor de compliance com autonomia suficiente para acompanhar toda essa mudança de cultura e monitorar os processos de controle e a aplicação das sanções cabíveis. O programa precisa ser constantemente atualizado e os funcionários da empresa treinados para seguir sempre na direção certa, afastando-se das situações que contrariem as regras instituídas.[22] Os programas de compliance difundiram-se no Brasil, mas ainda há poucos dados a respeito da sua efetividade, sob o ponto de vista da modificação dos padrões éticos na atividade empresarial.[23]

O cuidado com a proteção dos dados pessoais, desde a sua coleta até o término do tratamento e sua posterior eliminação, deve permear todas essas quatro fases. Já na primeira fase, quando serão mapeados os pontos mais vulneráveis da empresa, será necessário avaliar em que situações e como a empresa colhe os dados pessoais, quais são esses dados, se e como esses dados são armazenados, em que momentos tais dados são utilizados, quais são os tipos de tratamento realizados com esses dados – lembrando aqui que, para a LGPD, a mera coleta dos dados já é, em si, considerada um tipo de tratamento[24] –, como esses dados se relacionam com a atividade da empresa, em que circunstâncias esses dados ficam mais expostos a risco, como ocorre o encerramento do tratamento e, finalmente, se e como os dados pessoais são descartados.

O programa de compliance precisa ter regras expressas e muito claras para orientar como deve ocorrer o encerramento do tratamento de dados e como deve se dar o seu descarte, prevendo também as sanções para o caso de

22. Apesar do custo de implementação, o programa "evitará não apenas as sanções previstas na LGPD e a judicialização de demandas, mas também reduzirá os custos sociais, pois, ao prevenir o tratamento inadequado de dados, promoverá o desenvolvimento e bem-estar no ambiente laboral, ao mesmo tempo em que protegerá direitos fundamentais" (Wervloet, Sabrina. "A incidência da lei geral de proteção de dados e o compliance nas relações de trabalho como instrumentos para a proteção de dados pessoais do trabalhador na 4ª revolução industrial". *Revista dos Tribunais*, vol. 1022. São Paulo: RT, dez. 2020, pp. 255-270).

23. Sobre o ponto, vide SAAD-DINIZ, Eduardo. "Análise qualitativa sobre a implementação dos programas de compliance no brasil (2014-2019)", cit., *passim*.

24. De acordo com o art. 5º, inciso X, da LGPD, considera-se tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

descumprimento. Com isso, o próprio programa poderá criar o *standard* de conduta que deverá ser sempre observado no encerramento do tratamento e, posteriormente, no momento em que haverá o descarte dos dados, prevenindo potenciais situações lesivas. Quanto mais precisas e claras forem as regras, mais efetivo será o programa; quanto mais suas regras e medidas preventivas forem observadas, menor será o risco de ocorrer algum incidente de segurança.

O art. 50 da LGPD[25] estabelece diretrizes para as boas práticas e governança, a serem definidas pelos controladores e operadores de dados pessoais,

25. "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I – implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II – demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade

As regras de compliance devem atentar para a organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, entre outros aspectos. Entre os critérios para a criação das normas de compliance, destacam-se a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

No que tange ao término de dados pessoais, como visto acima, há de se verificar as quatro hipóteses previstas na lei: i) o esgotamento da finalidade; ii) a observância do período; iii) a revogação do consentimento; iv) a determinação da autoridade nacional, por violação à LGPD. O desenvolvimento das regras de compliance deve pautar-se, portanto, nessa linha. Vale dizer, estabelecer os processos e os meios de controle adequados para definir quando ocorre o término do tratamento de dados naquela dada atividade e como acontecerá a sua eliminação,[26] isto é, a exclusão de dado ou de conjunto de dados armazenados.

Como se sabe, a LGPD entrou em vigor em 01.05.2021.[27] A ausência de normas de conduta que indiquem procedimentos para o término do tratamento de dados certamente poderá acarretar infrações à LGPD, na medida em que a eliminação constitui consequência resultante do próprio término. Assim, se no âmbito da gestão não for possível delimitar quando ocorre o término, também não haverá a eliminação dos dados, a configurar infração administrativa,[28] além de outras sanções.

---

responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional".

26. Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I – cumprimento de obrigação legal ou regulatória pelo controlador;
II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

27. Com exceção dos artigos 52, 53 e 54, que entram em vigor a partir de 01/08/2021.

28. Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

O programa de compliance, portanto, deve mapear quando se dá o esgotamento da finalidade do tratamento de dados, a fim de que possa estabelecer procedimentos para a identificação dessa hipótese de término, e indicar qual o método a ser utilizado para a eliminação dos dados, por exemplo, a informação ao titular, ou atribuição de prazo para coleta dos dados antes da sua eliminação. Se há um período para o tratamento de dados, o programa de compliance deve indicar as condutas para o controle do prazo e sua regular eliminação ao fim desse período.

Há de se observar ainda que a LGPD atribui centralidade ao titular dos dados. Sobretudo em relação aos dados sensíveis, o consentimento livre e atual do titular mostra-se necessário, salvo poucas exceções. Desse modo, o compliance também se ocupa em criar procedimentos para o consentimento e sua revogação; e sendo dados sensíveis, cuidar para que seja fornecido de forma específica e destacada, para finalidades específicas, ao fim das quais o tratamento igualmente finda.

Os programas de compliance, portanto, apresentam-se como meio eficaz para o cumprimento da LGPD, inclusive no término e na eliminação dos dados pessoais. É preciso que se respeitem as hipóteses legais que levam ao término do tratamento de dados, bem como mecanismos para controle e sanção no caso de descumprimento.

I – advertência, com indicação de prazo para adoção de medidas corretivas;
II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III – multa diária, observado o limite total a que se refere o inciso II;
IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI – eliminação dos dados pessoais a que se refere a infração;
VII – (Vetado);
VIII – (Vetado);
IX – (Vetado);
X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

4. O IMPACTO DOS PROGRAMAS DE *COMPLIANCE* NA RESPONSABILIDADE CIVIL

Diante da pouca valia da simples reparação – incerta e, no mais das vezes, excessivamente onerosa –, a prevenção quase sempre é a melhor, quando não a única, solução. De fato, inúmeros são os danos irreparáveis ou de difícil reparação, pelo que nem sempre o Direito pode contentar-se com meras indenizações.[29]

No campo de incidência da LGPD, com mais razão, *prevenir* sempre será melhor do que *remediar*, tanto mais em se tratando de dados sensíveis. Afinal, depois de ocorrido o vazamento ou o mau uso dos dados, por exemplo, é bem mais complicado conter as possíveis consequências e desdobramentos que podem advir do incidente.[30] Ao estabelecer o procedimento a ser seguido para o encerramento do tratamento de dados, o objetivo do programa de compliance deve ser o de estabelecer verdadeira referência normativa para as práticas da empresa, com especial atenção para a identificação da cadeia de responsabilidade, para a adoção de medidas de prevenção em relação a potenciais condutas que infrinjam a lei e para as formas de remediação/mitigação dos danos.

O compliance atua, portanto, tanto no *ex ante*, estabelecendo medidas preventivas, como no *ex post*, aplicando as sanções cabíveis e direcionando a remediação dos prejuízos causados. Considerando que a LGPD é permeada de conceitos jurídicos indeterminados, que precisam ser necessariamente concretizados, tomando por base a realidade de cada agente econômico, "(...) é fundamental que, ao lado do papel regulamentador da autoridade nacional, os agentes econômicos possam também ter a iniciativa de dar concretude aos comandos legais, adaptando-os à sua realidade a partir dos incentivos e dos esclarecimentos que recebem do próprio Estado".[31]

---

29. O dano moral, por exemplo, não se sujeita a "ressarcimentos", mas antes se "compensa", como o dano extrapatrimonial de maneira geral. A dificuldade reside no fato de essa compensação ser feita, na maioria dos casos, por meio da deflagração do dever de indenizar – de cunho estritamente patrimonial –, como se essa fosse a única resposta possível do ordenamento jurídico para as inúmeras lesões à dignidade humana, vale dizer, aos interesses existenciais.

30. Em outro campo, exemplo de comportamento preventivo, que merece especial destaque, é o procedimento conhecido por *recall*, cada vez mais comum na prática, em que o próprio fabricante de produtos de consumo duráveis conclama seus consumidores a comparecerem às agências concessionárias para que as peças defeituosas de seus produtos sejam trocadas gratuitamente. O procedimento de *recall* tem sido muito utilizado não só pelos fabricantes de veículos, mas também de aparelhos eletrodomésticos.

31. FRAZÃO, Ana; OLIVA, Milena Donato; e ABILIO, Vivianne da Silveira. "Compliance de dados pessoais", cit., p. 677.

As medidas de prevenção serão fiscalizadas pela autoridade nacional de proteção de dados, que assume, nesse cenário, papel de enorme relevância. Em outras searas, quando, por exemplo, as autoridades incumbidas da fiscalização de certo setor produtivo impedem ou, simplesmente, não autorizam a fabricação de determinado medicamento cujo fator de risco supera eventuais benefícios, "então aí se terá obtido o efeito preventivo de proteção à saúde do público consumidor em geral".[32] Nem sempre, porém, a fiscalização acerta. Se falharem tais mecanismos, ainda é possível, em alguns casos, evitar ou, pelo menos, mitigar os efeitos do *eventus damni*, preventivamente por meio das ações cautelares. Já as sanções administrativas, bem como as infrações penais, atuam repressivamente, isto é, *a posteriori*.

Quanto às sanções administrativas, previstas no art. 52 da LGPD,[33] nota-se que, ainda que o programa de compliance não tenha impedido ou prevenido o *eventus damni*, ele poderá impactar de forma relevante na apreciação e na aplicação da sanção pela autoridade nacional. Isso porque, o próprio art. 52, em seu parágrafo primeiro, deixa expresso que as sanções serão aplicadas de acordo

32. FILOMENO, José Geraldo Brito. In: GRINOVER, Ada Pelledrini *et al* (Org.). *Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto*. 5. ed. Rio de Janeiro: Forense Universitária, 1998, p. 117.

33. Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
I – advertência, com indicação de prazo para adoção de medidas corretivas;
II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III – multa diária, observado o limite total a que se refere o inciso II;
IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V – bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI – eliminação dos dados pessoais a que se refere a infração;
VII – (vetado);
VIII – (vetado);
IX – (vetado);
X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

com as peculiaridades do caso concreto, considerados alguns parâmetros e critérios, entre eles: a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; a adoção de política de boas práticas e governança; e a pronta adoção de medidas corretivas.

Dessa forma, a existência de um programa de compliance eficaz, que regulamente de forma clara e objetiva as diretrizes para a rápida remediação de eventuais prejuízos causados ao longo do tratamento, e mesmo após o seu término, será relevante para a apreciação das sanções aplicáveis. E isso poderá ocorrer não só no âmbito da responsabilidade administrativa, como também na responsabilidade civil.

Como se sabe, na esfera da responsabilidade civil, a reparação do dano deve ser integral. Nesse sentido, o *caput* do art. 944 do Código Civil, ao disciplinar que a indenização se mede pela extensão do dano, consagra o princípio da reparação integral, afastando qualquer escopo punitivo da responsabilidade civil.[34] Contudo, o parágrafo único desse art. 944 positiva o abrandamento desse princípio, permitindo que o juiz reduza, equitativamente, a indenização "se houver excessiva desproporção entre a gravidade da culpa e o dano".

Apesar de o dispositivo mencionar o "grau de culpa" para a análise da excessiva desproporção, o elemento a ser analisado há de ser o nexo causal e a adequação dos efeitos produzidos por certo ato, e não a culpa do agente e suas

34. Nas últimas décadas, tem-se identificado, sobretudo nos tribunais estaduais, tentativa de se atribuir à responsabilidade civil função punitiva, ao lado da reparatória/compensatória, o que tem sido feito, de regra, por meio da majoração do valor devido a título de danos morais, seja afirmando-se expressamente a existência dessa pretensa função punitiva, seja utilizando-se de parâmetros tipicamente punitivos para a quantificação da indenização, a exemplo da situação patrimonial do ofensor e da reprovabilidade de sua conduta. Não obstante a prática judicial reiterada, o ordenamento jurídico pátrio, *de lege lata*, não admite a condenação do ofensor à verba punitiva, que, a rigor, vai de encontro à repersonalização do direito civil. É possível destacar diversos fatores que afastam a função punitiva da responsabilidade civil, entre eles: (i) a responsabilidade civil brasileira tem como regra fundamental a indenização de acordo com a extensão do dano; (ii) a indenização punitiva implicaria punição sem prévia cominação legal visto que não é prevista em lei; (iii) muitos dos ilícitos civis também configuram ilícitos penais e/ou administrativos, e, com isso, a indenização punitiva levaria o agente a ser punido em diferentes esferas pelo mesmo fato, configurando *bis in idem*. Para um estudo completo do assunto, v. BODIN DE MORAES, Maria Celina. "*Punitive damages* em sistemas civilistas: problemas e perspectivas". *Revista trimestral de direito civil*, v. 18. Rio de Janeiro: Padma, abr./jun. 2004, pp. 45-78.

subjetivas e proscritas gradações. Esse dispositivo revela a preocupação do legislador com a reparação justa, sobrepondo à disciplina do dano uma espécie de limite de causalidade legítima, de modo a autorizar o magistrado a eliminar da indenização o *quantum* que transcenda os efeitos razoavelmente atribuídos, na percepção social, à conta de determinado comportamento. Como já se teve a oportunidade de explicar em outra obra:

> "A redução da indenização decorre, por conseguinte, da ausência de nexo causal direto e imediato entre a conduta do agente e a parcela desproporcional de dano causado. Tendo-se em conta o resultado razoavelmente esperado para certas condutas, por vezes corriqueiras, da atividade humana, o legislador admite hipótese em que o resultado danoso excede a causalidade que se pode esperar. O resultado mais grave, portanto, decorreria da presença de concausa externa e excepcional não imputável ao agente. Trata-se de concausa que, extrapolando a causalidade razoavelmente esperada para determinado comportamento, conduz à extraordinária majoração do dano. Se o agente deve suportar o dano na medida em que o tenha produzido, isto é, na proporção em que sua conduta interferiu no evento danoso, não será responsável pela parcela extraordinária do dano decorrente da concausa".[35]

Nesses termos, é possível que os efeitos da aplicação do programa de compliance influenciem na adoção de comportamentos que funcionem para afastar, ainda que não totalmente, pelo menos parte da responsabilidade do agente de tratamento pelos eventuais danos envolvendo o término do tratamento e a eliminação dos dados pessoais, com base na redução equitativa da indenização. Trata-se, evidentemente, de medida excepcional, que cria uma exceção à regra geral da reparação integral.

Não fosse só isso, a possibilidade de mitigação dos danos por meio da aplicação de um programa de compliance eficaz parece também afastar a utilização da técnica *in re ipsa* para a reparação do dano moral no âmbito da LGPD.[36]

---

35. TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do direito civil,* v. 3, 2. ed. São Paulo: GEN Forense, 2021, p. 125.

36. Sobre a questão do dano moral *in re ipsa* no âmbito da LGPD, remete-se o leitor a GUEDES, Gisela Sampaio da Cruz. "Dano moral *in re ipsa* e a Lei Geral de Proteção de Dados Pessoais: 'presunção e água benta, cada um toma a que quer'". No prelo a ser publicado em obra coletiva coordenado por Felipe Palhares.

Diante de uma situação em que ocorra um vazamento de dados pessoais, por exemplo, é possível que o responsável/controlador, baseado em programa de compliance, tenha tomado diversas providências específicas que lhe cabiam não só para evitar, como também para minimizar os prejuízos desse vazamento, de tal forma que até mesmo inexista, no caso concreto, razão para uma responsabilização por danos morais.[37]

Em precedente julgado pelo Tribunal de Justiça do Rio Grande do Sul,[38] foi justamente a mitigação do dano que determinou a inexistência de dano moral. Ao analisar situação em que houve um vazamento de dados cadastrais de alunos em um grupo de e-mail de um curso de uma universidade, o Tribunal levou em consideração que a universidade comprovou ter tomado todas as providências pertinentes a fim de minimizar os prejuízos decorrentes do vazamento de informações, lançando nota em jornal local, registrando Boletim de Ocorrência, advertindo os alunos que receberam o e-mail com os dados para que não os repassassem, anotação junto ao SPC e SERASA por meio de intervenção judicial, entre outras. Por fim, o Tribunal ainda ressaltou que "a ocorrência de divulgação de dados – diga-se, não sigilosos – por si só, não evidencia dano moral, uma vez que à míngua de comprovação específica, por não ser presumido, não resta caracterizado".

A aplicação do artifício *in re ipsa*, tão utilizado quando se trata, por exemplo, de uso indevido de imagem,[39] parece não se adequar à miríade de situações que podem decorrer da LGPD. A conclusão a que se chega é a de que, se, em razão do exercício de atividade de tratamento de dados pessoais ou de um incidente de segurança ocorrido na fase final de descarte dos dados, uma pessoa natural tiver

37. Diante da realidade atual dos dados digitais, como já se observou, "não faria sentido adotar uma interpretação da responsabilidade civil que fosse calcada em um ideal fantasioso de precaução ilimitada e segurança absoluta. Com dados circulando em uma velocidade estonteante, além de hackers dispostos a usar de todos os artifícios possíveis (digitais ou não), é fundamental ter uma perspectiva real, inclusive considerando penas e multas estipulados na legislação para não inibir a atividade produtiva e empreendedora que é o motor da sociedade" (CORRÊA, Leonardo; CHO, Tae. "Responsabilidade civil na LGPD é subjetiva". Disponível em: https://www.conjur.com.br/2021-jan-29/correa-cho-responsabilidade-civil-lgpd-subjetiva#author. Acesso em: 02.06.2021).

38. TJ/RS, 1ª Turma Recursal Cível, Recurso Cível n.º 71004371027, Rel. Des. Marta Borges Ortiz, j. 26.11.2013.

39. Vide o Enunciado da Súmula 403 do STJ, segundo o qual: "Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais".

seus dados pessoais indevidamente divulgados, não necessariamente ela sofrerá dano moral. E, ainda que reste configurado o dano, não é recomendável que o julgador aplique, *ipso facto*, a técnica das presunções para deixar de avaliar a configuração e a extensão do dano no caso concreto.[40]

Afastar a metodologia *in re ipsa* não fragiliza a aplicação da LGPD no que diz respeito à responsabilização dos agentes de tratamento. Permanecem esses vinculados à proibição de utilização indevida e irregular dos dados pessoais, fundada na tutela da privacidade e intimidade dos titulares dos dados, os quais, no entanto, não farão jus a uma reparação extrapatrimonial automática, sem maiores considerações ao caso concreto, quando aquela vedação for descumprida. A ocorrência e a reparação de eventual dano moral sofrido pelo titular dos dados vazados continua plenamente possível, sendo apenas necessária, para a sua aferição, uma ponderação mais concreta, que não se baseie na sensível metodologia das presunções.

No Brasil, a reparação do dano moral enfrenta diariamente diversos desafios. A reparação *in natura* se mostra particularmente eficaz tendo em vista os valores relativamente baixos das indenizações arbitradas para os danos extrapatrimoniais, sobretudo nos casos mais grave, o que faz com que a vítima não se sinta devidamente reparada. Com a reparação *in natura*, o pagamento da indenização pode eventualmente ser substituído ou cumulado com medidas de retratação ou da publicação da sentença de procedência do pedido de indenização por dano moral,[41] tornando mais efetiva a compensação[42] e desestimulando a difusão das ações meramente mercenárias.

---

40. Na linha do Enunciado n.º 455, da V Jornada de Direito Civil, organizada pelo Conselho da Justiça Federal: "Embora o reconhecimento dos danos morais se dê, em numerosos casos, independentemente de prova (*in re ipsa*), para a sua adequada quantificação, deve o juiz investigar, sempre que entender necessário, as circunstâncias do caso concreto, inclusive por intermédio da produção de depoimento pessoal e da prova testemunhal em audiência".

41. O que não necessariamente precisa ocorrer no Diário de Justiça; a depender do caso, a reparação será mais efetiva se a sentença for publicada em informativo local, que circule mais pelo público diante do qual o lesado ficou exposto.

42. Na legislação brasileira, a Lei de Imprensa (Lei n.º 5.250/67) prevê algumas formas de reparação que têm sido consideradas modalidades de reparação *in natura*, como a retratação do ofensor, o desmentido, a retificação da notícia injuriosa, a divulgação da resposta e, até mesmo, a publicação da sentença condenatória. Vale observar que, em 30 de abril de 2009, o Supremo Tribunal Federal brasileiro, por maioria, julgou procedente a Arguição de Descumprimento de Preceito Fundamental – ADPF n.º 130/DF, ajuizada pelo Partido Democrático Trabalhista – PDT em face da Lei de Imprensa,

Tão sedutora é a reparação *in natura* que, por vezes, se chega mesmo a afirmar o caráter subsidiário da "reparação" (compensação) pecuniária, que só seria chamada a atuar quando a reparação *in natura* se revelasse insuficiente para tutelar a vítima. O que se tem observado, contudo, é justamente o contrário: a reparação pecuniária tem sido a regra, e a *in natura,* a exceção, tendo em vista, sobretudo, os acanhados mecanismos dessa modalidade de reparação, que não oferecem tutela satisfatória à compensação de diversos danos extrapatrimoniais.[43]

Nos poucos casos em que a reparação *in natura* é posta em prática, as decisões, de regra, limitam-se a condenar o agente ofensor a alguma medida de retratação, quando viável, ou a providenciar a publicação da sentença, o que pode mesmo criar um efeito reverso (ou perverso) para a vítima.[44] Em casos tais, a reparação pecuniária, à míngua de outro mecanismo de reparação *in natura* mais eficiente, parece o melhor instrumento de compensação dos danos sofridos.

No caso dos dados pessoais, a LGPD desafiará novos mecanismos de tutela, com o fito de garantir, em meio ao fomento à inovação e às novas tecnologias, a autodeterminação do titular dos dados. Agora prevenir, tal como a experiência popular tem demonstrado, sempre será melhor do que remediar e, nesse

---

declarando que a referida lei não havia sido recepcionada pela ordem constitucional de 1988, por ferir os princípios da Constituição Federal. Apesar disso, tais formas de reparação *in natura*, ali previstas, continuam sendo aplicadas na prática. A doutrina indica também como exemplo a retirada do mercado do livro supostamente ofensivo à honra de uma pessoa pública (para outros exemplos, cf. ASSIS, Araken de, "Liquidação do dano", *Revista dos Tribunais*, vol. 759, São Paulo: RT, jan./1999, pp. 14-23). Na opinião do Min. Paulo de Tarso Vieira Sanseverino, tais "(...) medidas previstas na nossa legislação ou indicadas pela doutrina não constituem propriamente casos de reparação natural, pois não se consegue apagar completamente os prejuízos extrapatrimoniais, sendo apenas tentativas de minimização dos seus efeitos por não ser possível a recomposição dos bens jurídicos sem conteúdo econômico atingido, como ocorre com os direitos da personalidade" (SANSEVERINO, Paulo de Tarso Vieira, *Princípio da reparação integral*, São Paulo: Saraiva, 2010, pp. 34-40/275-277).

43. Assim, "[n]ão obstante seu caráter subsidiário, a indenização em dinheiro é mais frequente, dadas as dificuldades opostas, na prática, à reparação natural pelas circunstâncias e, notadamente, em face do dano, pela impossibilidade de restabelecer a rigor a situação anterior ao evento danoso" (DIAS, José de Aguiar, *Da responsabilidade civil*, 11. ed., Rio de Janeiro: Renovar, 2006, pp. 985-988).

44. Pense-se, por exemplo, na situação da pessoa cuja vida privada tenha sido exposta em matéria jornalística falsa. A depender das circunstâncias do caso concreto, a publicação da sentença de procedência do pedido de indenização por dano moral pode submeter a vítima a nova exposição na mídia, trazendo, uma vez mais, à tona assunto já adormecido aos olhos do grande público.

aspecto, os programas de compliance se alinham perfeitamente com essa nova realidade. Para além da responsabilidade civil, na medida em que a personalidade não se esgota no aspecto negativo (dever de não violar), os programas de compliance tem muito a oferecer à chamada tutela positiva das situações jurídicas existenciais, instituindo mecanismos voltados à autodeterminação informativa, em colaboração com a realização desse valor.[45] É a chamada "mudança de cultura" apregoada nos programas efetivos de compliance.

5. CONCLUSÃO

A LGPD tem a finalidade de permitir o controle do tratamento de dados pessoais pelo com próprio titular, eis que o consentimento não implica a transferência da titularidade para o controlador ou operador, que tem limites a serem atendidos. O art. 15 da lei enuncia as hipóteses de término do tratamento de dados pessoais, que podem ser organizadas da seguinte forma: i) pelo esgotamento funcional da utilização dos dados; ii) pelo término do prazo; iii) pela autodeterminação do titular; e iv) por ilegalidade. Em síntese, a regra é a eliminação dos dados pessoais quando seu tratamento se encerra, nos moldes do art. 16. Trata-se de modelo que visa a diminuir os riscos do uso não autorizado ou indevido dos dados pessoais.

A importância desse modelo é evidente quando se percebe que a lógica da reparação dos danos não se mostra suficiente quando ocorre a violação dos direitos do titular dos dados pessoais. Em sua maioria, trata-se de violação a situações existenciais cujo retorno ao estado anterior é impossível, e o valor do dano imensurável. É exatamente por esse motivo que a tutela positiva das situações existenciais há de ser reforçada, aqui com a garantia da autodeterminação informativa, que confere ao titular o poder de decisão sobre os seus dados pessoais.

Os programas de compliance se adequam perfeitamente a esse modelo, já que têm a finalidade precípua de implementar medidas preventivas para reduzir a ocorrência de danos, além de criarem procedimentos para a contenção dos prejuízos. A ideia de prevenção reflete as novas correntes filosóficas que criticam

45. Consulte-se sobre o tema: MEIRELES, Rose Melo Vencelau, *Autonomia privada e dignidade humana*, Rio de Janeiro: Renovar, 2009, pp. 53-61, valendo trazer a distinção entre tutela positiva e negativa: "A tutela positiva das situações existenciais permite que a autonomia privada possa ser também instrumento de regulação de interesses existenciais, a fim de garantir o livre desenvolvimento do seu titular. É chamada *positiva* porque realizada mediante a autodeterminação do titular, muitas vezes, com colaboração de outrem; enquanto que a tutela *negativa* diz respeito a comportamentos omissivos gerais, os quais tem repercussão jurídica apenas depois da lesão", p. 57.

as carências e as limitações da responsabilidade civil clássica. Propugna-se, com isso, a passagem do "dever de reparar" ao "dever de prevenir". A responsabilidade pelo dano injusto praticado vai, pouco a pouco, cedendo lugar, ou melhor, sendo alargada, por uma responsabilidade orientada para a prevenção de novos impactos e para o controle das atividades, de modo a garantir maior proteção aos titulares de dados pessoais.

Para além da prevenção do dano, o compliance exerce função de extrema relevância para a tutela da pessoa humana, que consiste na construção de processos voltados para a promoção da dignidade, escapando dos moldes tradicionais de inviolabilidade da vida privada. Isso porque o enfoque deixa de ser a violação (preventiva ou repressiva), passando a estruturar *standards* de comportamento voltados para a cultura da autonomia na seara dos dados pessoais. Acrescente-se ao "dever de prevenir" o "dever de colaborar".