Coordenação:
HIGOR VINICIUS NOGUEIRA JORGE

MANUAL DE EDUCAÇÃO DIGITAL, CIBERCIDADANIA E PREVENÇÃO DE CRIMES CIBERNÉTICOS

UM GUIA PARA JOVENS, ADULTOS, EMPRESAS, INSTITUIÇÕES E AUTORIDADES

Professores:
RODRIGO NEJM

Apresentação:
MICHELE NEPOMUCENO

Autores:
AUGUSTO EDUARDO DE SOUZA ROSSINI
CLAUDIO JOEL BRITO LÓSSIO
CLEÓRBETE SANTOS
CORIOLANO DE ALMEIDA CAMARGO
DENIZE DOS SANTOS ORTIZ
GISELE TRUZZI
HÉLIO MOLINA JORGE JÚNIOR
HIGOR VINICIUS NOGUEIRA JORGE
IVANA DAVID
JAHYR GONÇALVES NETO
JANIO KONNO JÚNIOR
JOAQUIM LEITÃO JÚNIOR
LETÍCIA SABBADINI MULLER
MARCOS VINÍCIUS ALVES E SILVA FILHO
MAURO ROBERTO DE SOUZA JÚNIOR
PAULO REYNER CAMARGO MOUSINHO
PAULO SUMARIVA
RICARDO MAGNO TEIXEIRA FONSECA
ROSANGELA TREMEL
VALÉRIA CHEQUE GRANATO
WAGNER MARTINS CARRASCO DE OLIVEIRA
WALTER MARTINS MULLER
WILLIAM GARCEZ

2021

EDITORA JusPODIVM
www.editorajuspodivm.com.br

12

CYBERBULLYING E EDUCAÇÃO DIGITAL

Higor Vinicius Nogueira Jorge[1]

1. INTRODUÇÃO

Muitos imaginam que violência signifique unicamente agressão física contra outras pessoas, ou seja, que violência seja sinônimo de infligir uma dor corporal contra as vítimas, como por exemplo, decorrente de um tapa, um empurrão, um soco ou uma facada.

O que as pessoas geralmente não levam em consideração é que existem modalidades de violência que podem ser produzidas de forma diferente. Um exemplo é a agressão moral e mais recentemente esse tipo de ofensa praticada por intermédio de recursos tecnológicos (ou no ambiente cibernético).

As ofensas praticadas por meios eletrônicos se assemelham com as outras modalidades e seus efeitos podem ser irrecuperáveis e perdurar por toda a vida da vítima.

---

1. Delegado de Polícia e professor da Academia de Polícia na Polícia Civil do Estado de São Paulo, titular da cadeira 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e membro da Associação dos Delegados de Polícia do Estado de São Paulo. Também é membro da Associação Internacional de Informática Forense (Asiif), da Associação Interna-cional de Investigação de Crimes de Alta Tecnologia (Htcia) e da Associação Internacional da Polícia (Ipa - Brasil), professor de inteligência cibernética do Ministério da Justiça, professor da pós-graduação Advocacia no Direito Digital e Proteção de Dados na Escola Brasileira de Direito (Ebradi), professor da pós-graduação em *Compliance* e Direito Anticorrupção e da pós-graduação em Direito Político e Eleitoral do Complexo de Ensino Renato Saraiva (Cers), professor da espe-cialização Direito Digital Aplicado e *Compliance* Digital do MeuCurso, professor da pósgraduação em direito penal e processo penal na Escola Superior de Advocacia da OAB-SP (ESAOAB/SP), pro-fessor de formação continuada da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), professor da especialização da Associação dos Diplomados da Escola Superior de Guerra, mem-bro do grupo de estudos de direito digital e compliance da Federação das Indústrias do Estado de São Paulo (Fiesp) e investigador digital forense certificado pela REDLIF. Em 2017, 2019 e 2020 foi escolhido na categoria "Jurídica" entre os melhores Delegados do Brasil pelo Portal Nacional dos Delegados & Revista da Defesa Social. É coautor das obras "Manual de Interceptação Telefô-nica e Telemática" e "Fake News e Eleições – O Guia Definitivo" e coordenador dos livros "Enfren-tamento da Corrupção e Investigação Criminal Tecnológica" e "Tratado de Investigação Criminal Tecnológica", publicados pela editora Juspodivm, além ser autor/coautor de outras obras jurídi-cas. Possui o site www.higorjorge.com.br.

2. *BULLYING* E *CYBERBULLYING*

Independente do tipo de agressão, quando se torna reiterada, a vítima pode estar diante do *bullying*, uma palavra originada da língua inglesa, que significa valentão e que se caracteriza pela prática de agressões físicas ou psicológicas de forma habitual, traumática e prejudicial contra as vítimas.

Mais recentemente surgiu o *cyberbullying* que consiste no mesmo tipo de agressão, porém praticada por meios tecnológicos (eletrônicos, virtuais), ou seja, por intermédio de computadores ou outros recursos (exemplos: tablet, celular, *smartwatch*, redes sociais, aplicativos de comunicação etc.). Essas ofensas podem ser praticadas pelas formas mais variadas e, uma das principais características, é a rápida disseminação pela rede, ou seja, em pouco tempo são disponibilizadas em uma infinidade de sites, redes sociais, blogs e grupos do *Whatsapp*. Dificilmente a vítima consegue extirpar a informação de todos os locais aonde se encontra.

Dentre os recursos que podem ser utilizados pelos autores de *cyberbullying* temos o envio de e-mails ofensivos para a vítima ou conhecidos dela, envio de mensagens para grupos ou perfis pessoais do *Whatsapp*, postagem de textos, áudios ou vídeos no Facebook, Instagram ou outras redes sociais, publicação de ofensas em sites, blogs, fóruns de discussão, mensageiros instantâneos, jogos eletrônicos, hotéis virtuais (haboo) etc.

O *cyberbullying*, de forma semelhante ao *bullying*, é muito frequente nos ambientes escolar e universitário, entre jovens, porém pode ser praticado também no ambiente corporativo, no seio familiar, em templos religiosos, entre vizinhos, amigos ou em outros ambientes.

Em nosso dia a dia temos visto o *cyberbullying* ser praticado pelos mais variados motivos, desde diferenças entre características físicas das pessoas, como por exemplo, um indivíduo que usa óculos, que é obeso, que tem alguma deformidade física ou em relação a outras características, como nos casos em que um jovem se destaca muito intelectualmente ou que possui uma religião, etnia ou preferência sexual diferente da maioria.

Esse tipo de problema tem proporcionado diversas consequências, como traumas, baixo desempenho escolar, depressão, sentimento de inferioridade, dificuldade nos relacionamentos e outros malefícios.

3. *CYBERBULLYING* E CRIMES CIBERNÉTICOS

Cabe ainda destacar que alguns casos de *cyberbullying* rompem os limites da licitude, pois se enquadram em previsões penais. Surgem nestes

casos os crimes cibernéticos, que se caracterizam pela prática de crimes fazendo uso de recursos tecnológicos, especialmente celulares e computadores. Neste tipo de situação também é deflagrada a atuação dos órgãos de persecução penal e na sua primeira fase pode atuar a Polícia Civil ou a Polícia Federal que possuem a função de apurar infrações penais, conforme consta no artigo 144 da Constituição Federal.

Dentre os principais exemplos de *cyberbullying* considerado criminoso destacamos:

1. **Calúnia**[2]: afirmar que a vítima praticou algum fato criminoso. Um exemplo comum é o caso de mensagens deixadas no perfil de um usuário do Facebook ou outra rede social que imputa a ele a prática de determinado crime, como por exemplo, que certa pessoa praticou um estupro ou que estaria comercializando drogas ilícitas na residência. A pena para este tipo de delito é de detenção de seis meses a dois anos e multa.

2. **Difamação**[3]: propagar fatos ofensivos a reputação da vítima. O cidadão que divulgou no Instagram uma foto de um empresário saindo do motel acompanhado da sua vizinha praticou o crime de difamação. Mesmo que a foto publicada no Instagram e outros elementos sejam capazes de provar que realmente o empresário estava no local com a vizinha, o crime subsistirá, pois independe do fato ser verdadeiro ou falso, o que importa é que prejudicou a reputação da vítima. O delito tem a pena de detenção de três meses a um ano e multa.

3. **Injúria**[4]: ofender a dignidade ou o decoro de outras pessoas. Geralmente se relaciona com xingamentos, exemplo, escrever no Facebook da vítima ou publicar na Wikipédia que ela seria vagabunda, furtadora, assassina, proxeneta e dependente de drogas. A pena é de detenção e varia entre um a seis meses ou multa. Se a injúria for composta de elementos relacionados com a raça, cor, etnia, religião, origem ou condição de pessoa idosa ou portadora de deficiência o crime se agrava e a pena passa a ser de reclusão de um a três anos e multa.

4. **Ameaça**[5]: ameaçar a vítima de mal injusto e grave. É corriqueiro a vítima procurar a Delegacia de Polícia para informar que recebeu e-mails,

2. Art. 138 do Código Penal – "Caluniar alguém, imputando-lhe falsamente fato definido como crime".

3. Art. 139 do Código Penal – "Difamar alguém, imputando-lhe fato ofensivo à sua reputação".

4. Art. 140 do Código Penal – "Injuriar alguém, ofendendo-lhe a dignidade ou o decoro".

5. Art. 147 do Código Penal – "Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave".

mensagens pelo Messenger do Facebook, pelo Telegram, publicações na internet ou telefonemas com ameaças de morte, de agredir a vítima ou causar danos em seu veículo. A pena consiste na detenção de um a seis meses ou multa.

5. **Constrangimento ilegal**[6]: em relação ao *cyberbullying*, o crime de constrangimento ilegal pode ocorrer se for feita uma ameaça para que a vítima faça algo que não deseja fazer e que a lei não determine, por exemplo, se uma pessoa manda uma mensagem para as redes sociais da vítima dizendo que vai agredir um familiar dela caso ela concorra em uma concurso de beleza. Também comete este crime aquele que obriga a vítima a não fazer o que a lei permita, como no caso da garota que manda um e-mail para uma conhecida e ameaça matar seu cachorro caso continue a namorar o seu ex-namorado. A pena para este delito é a detenção de três meses a um ano ou multa.

6. **Falsa identidade**[7]: ação de atribuir-se ou atribuir a outra pessoa falsa identidade para obter vantagem em proveito próprio ou de outro indivíduo ou para proporcionar algum dano. Tem sido frequente a utilização de perfis falsos em sites de relacionamentos ou em redes sociais, como no caso de um homem que criou um perfil falso para poder se passar por pessoa solteira e conhecer outras mulheres. Também recentemente uma pessoa utilizou a foto de um desafeto para criar um perfil falso em uma rede sociais direcionada a encontros e passou a mandar mensagens para outras pessoas, informando o telefone da vítima. Outro caso recente foi do cidadão que criou um perfil no Instagram com fotos e dados de uma outra pessoa e começou a proferir ofensas e ameaças contra outros usuários da rede sociais que elaboraram Boletins de Ocorrência e, ao final da investigação, os fatos foram esclarecidos e o autor do crime foi identificado. A pena prevista para este tipo de ilícito é de três meses a um ano ou multa se o fato não for considerado elemento de crime mais grave.

7. **Molestar ou perturbar a tranquilidade**[8]: neste caso não há um crime e sim uma contravenção penal que permite punir aquele que passa a molestar ou perturbar a tranquilidade de outra pessoa por acinte ou motivo reprovável, como por exemplo, nos casos em que o autor passou a

6. Art. 146 do Código Penal – "Constranger alguém, mediante violência ou grave ameaça, ou depois de lhe haver reduzido, por qualquer outro meio, a capacidade de resistência, a não fazer o que a lei permite, ou a fazer o que ela não manda".

7. Art. 307 do Código Penal – "Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem".

8. Art. 65 da Lei das Contravenções Penais – "Molestar alguem ou perturbar-lhe a tranquilidade, por acinte ou por motivo reprovável".

enviar mensagens desagradáveis e capazes de incomodar a vítima, tendo enviado diariamente centenas de mensagens para ela. Neste caso chamou a atenção o fato de que as mensagens eram enviadas pelo WhatsApp e, quando a vítima bloqueava o investigado, ele adquiria outro número de celular pré-pago, habilitava um novo WhatsApp e passava a enviar as mensagens, até que foi identificado em razão da realização da denominada "investigação criminal tecnológica" que permitiu a adequada apuração dos fatos. Há alguns anos ocorreu um caso de um indivíduo que passava o dia inteiro realizando ligações telefônicas e enviando centenas de mensagens SMS com frases românticas para a vítima. O caso foi esclarecido e o autor foi enquadrado nesta contravenção penal. A pena para essa figura delitiva é de prisão simples, de quinze dias a dois meses ou multa.

A prática deste tipo de crime pela internet não é sinônimo de impunidade, muito pelo contrário, a Polícia Civil e a Polícia Federal possuem instrumentos adequados e profissionais capacitados para que, por intermédio da investigação criminal, a autoria e a materialidade sejam comprovadas.

Nestas hipóteses muitas vezes a investigação criminal envolve a utilização da "investigação criminal tradicional" em conjunto com o que denominamos "investigação criminal tecnológica", que torna mais eficaz a atuação das polícias judiciárias.

4. EFEITOS CIVIS DO CYBERBULLYING

A prática destas ofensas também desencadeia diversos efeitos no âmbito civil, como por exemplo, a obrigação de reparar os danos morais ou materiais proporcionados pelos autores das ofensas.

De acordo com o artigo 927 do Código Civil "aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

Cabe citar o artigo 186 do Código Civil ao estabelecer: "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" e o artigo 187: "também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes".

A decisão infra apresentada, oriundo do Tribunal de Justiça de São Paulo oferece um exemplo de condenação por danos morais em razão de ofensas publicadas no Facebook:

> Responsabilidade civil. Danos morais. Ofensas e ameaças perpetradas pela ré via "facebook". Violação aos direitos de personalidade da autora. Dano moral carac-

> terizado. Quantum indenizatório mantido. Apelação não provida. (...) Perpetração de ofensas e ameaças pela ré através de sua página pessoal no "facebook". Contexto fático e conjunto probatório existente nos autos que permitem aferir-se que o conteúdo injurioso se dirigia à pessoa da autora. 3. Expressões proferidas pela ré que ultrapassam o limite do mero aborrecimento, violando o direito à honra (subjetiva e objetiva) da autora. Dever de indenizar. 4. Quantum indenizatório. Razoabilidade. Manutenção. Valor que serve como fator desestimulante e sancionatório à imprudência da ré, sem implicar em enriquecimento ilícito da apelada. 5. Apelação da ré não provida (TJ/SP, 6ª Câmara de Direito Privado, Apelação Cível n.º 0.016.624-67.2012.8.26.0564. Rel. Des. ALEXANDRE LAZZARINI. Sexta. J. 18-04-2013.)

5. LEI Nº 13.185, DE 06 DE NOVEMBRO DE 2015

A Lei Nº 13.185, de 06 de novembro de 2015, instituiu o Programa de Combate à Intimidação Sistemática (Bullying) e passou a conceituar Bullying como "todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas".

O artigo 2º da referida Lei passou a caracterizar a intimidação sistemática "quando há violência física ou psicológica em atos de intimidação, humilhação ou discriminação" e também passou a considerar intimidação sistemática as seguintes condutas:

I - ataques físicos;

II - insultos pessoais;

III - comentários sistemáticos e apelidos pejorativos;

IV - ameaças por quaisquer meios;

V - grafites depreciativos;

VI - expressões preconceituosas;

VII - isolamento social consciente e premeditado;

VIII - pilhérias.

Outro ponto relevante da Lei é que estabeleceu o *cyberbullying* (intimidação sistemática na rede mundial de computadores) "quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência,

adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial".

O artigo 3º da Lei passou a classificar a intimidação sistemática (*bullying*) conforme as ações praticadas, como:

I - verbal: insultar, xingar e apelidar pejorativamente;

II - moral: difamar, caluniar, disseminar rumores;

III - sexual: assediar, induzir e/ou abusar;

IV - social: ignorar, isolar e excluir;

V - psicológica: perseguir, amedrontar, aterrorizar, intimidar, dominar, manipular, chantagear e infernizar;

VI - físico: socar, chutar, bater;

VII - material: furtar, roubar, destruir pertences de outrem;

VIII - virtual: depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social.

Outro aspecto relevante da Lei é que passou a prever expressamente o dever da escola (estabelecimento de ensino), além dos clubes e agremiações recreativas desenvolverem medidas que permitam "assegurar medidas de conscientização, prevenção, diagnose e combate à violência e à intimidação sistemática (*bullying*)".

6. COMO A VÍTIMA PODE COLABORAR?

Para que a Polícia tenha condições de prestar um serviço adequado e eficiente é necessário que a vítima forneça o maior número possível de informações, que se cerque de precauções para colaborar com a polícia na persecução penal do delito que foi deflagrado por intermédio do recurso tecnológico e também para evitar que possa vir a ser responsabilizada nos casos em que noticia o fato criminoso, mas não consegue comprovar o delito. Se a vítima não conseguir comprovar o crime pode inclusive ser punida pelo crime de comunicação falsa de crime ou contravenção[9] (detenção de

9. Art. 340 do Código Penal – "Provocar a ação de autoridade, comunicando-lhe a ocorrência de crime ou de contravenção que sabe não se ter verificado".

um a seis meses ou multa) ou denunciação caluniosa[10] (reclusão de dois a oito anos e multa e nos casos de utilização de anonimato ou nome suposto a pena é aumentada).

A vítima deve procurar uma Delegacia de Polícia e, no local, é importante que um policial civil visualize o conteúdo das ofensas, promova a coleta das evidências do crime e constate que acessou e coletou o conteúdo. Uma recomendação é que constate os fatos por um "auto de materialização de evidência eletrônica" sobre os fatos, com o maior número de informações, incluindo endereços (URLs) dos sites e perfis de redes sociais, cópias das publicações, telefones, e-mails etc. utilizados para a prática delitiva.

Se a ofensa estiver armazenada no e-mail da vítima o correto é que ela acesse o e-mail diante do policial civil, visualize o cabeçalho completo do e-mail, além do corpo do e-mail, sendo que o policial deverá elaborar um "auto de materialização de evidência eletrônica" sobre o conteúdo acessado.

Também é possível registrar uma ata notarial em um cartório de notas. Nestes casos, o cartorário acessa e imprime o conteúdo ofensivo.

Como demonstrado por JORGE, FREITAR JÚNIOR e GARZELLA (2020, 134-135):

> Outro caminho é realizar a captura/preservação técnica dos fatos ocorridos no ambiente *on-line* por intermédio de ferramentas, como por exemplo, o que é realizado pela Verifact. A ferramenta possui uma interface amigável e fácil, permitindo que pessoas comuns, sem um conhecimento técnico especializado, consigam operar e realizar registro de provas digitais em sites como Whatsapp Web, Facebook, Instagram, lojas virtuais, webmails e diversos outros. O usuário navega no conteúdo dentro da plataforma registrando vídeo capturas da tela (com áudio), imagens estáticas da tela (screenshots) e download de arquivos, enquanto o sistema coleta automaticamente diversos metadados técnicos relativos ao conteúdo e a origem dos dados. Pode ser usada por órgãos públicos, força policial, advogados e até pelas próprias vítimas de crimes virtuais, criando um material de alta confiança probatória quanto a sua existência, origem e autenticidade.

Outro caminho que recomendamos, considerando a volatidade das evidências, que podem desaparecer rapidamente, é que se no momento que tomar conhecimento do crime, não for possível realizar as sugestões acima apresentadas, que a vítima grave as informações em uma mídia não regravável e também as imprima e entregue na Delegacia de Polícia quando for elaborar o Boletim de Ocorrência, para, em seguida, realizar as me-

10. Art. 339 do Código Penal - "Dar causa à instauração de investigação policial, de processo judicial, instauração de investigação administrativa, inquérito civil ou ação de improbidade administrativa contra alguém, imputando-lhe crime de que o sabe inocente".

17

A LEI GERAL DE PROTEÇÃO DE DADOS NA ERA DIGITAL E OS REFLEXOS NAS INVESTIGAÇÕES CRIMINAIS

Joaquim Leitão Júnior[1]

Impactos da Lei Geral de Proteção de Dados em sede das investigações criminais - Qual a intensidade e grau de interferência da Lei Geral de Proteção de Dados no âmbito das investigações criminais?

1. CONSIDERAÇÕES INICIAIS

Vivemos na era digital em que somado a isto, os efeitos da pandemia trazida pelo coronavírus (Covid-19) fizeram acelerar várias realidades do mundo virtual - que ainda viriam à tona paulatinamente adiante -, mas que agora em decorrência da pandemia são reais, patentes e expostas a ponto de causarem preocupações importantes, no que tange à educação digital com vistas ao atingimento da cidadania digital, os efeitos práticos da Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) e os seus reflexos nas investigações criminais.

A Lei Geral de Proteção de Dados entrou em vigor no dia 18 de setembro de 2020, criando um cenário de maior segurança a todos no plano digital dentro do país e fora dele, inclusive no que diz respeito à conceituação e definição de dados pessoais e outros pontos afetos à pessoa humana.

Com isto, a lei em tablado sob o prisma da segurança jurídica acaba por padronizar as normatizações e práticas conferidas à proteção aos dados pessoais de forma igual dentro do país e no mundo. Assim, **dado pessoal** para a lei é qualquer "informação relacionada a pessoa natural identificada ou identificável (art. 5º, inciso I)".

1. Email: juniorleitaoadv@hotmail.com | Delegado de Polícia em Mato Grosso desde 2012, atualmente na função de Diretor Adjunto da Academia da Polícia Civil de Mato Grosso. Colunista do site Justiça e Polícia, coautor de obras jurídicas, autor de artigos jurídicos, palestrante e professor de cursos preparatórios para concursos públicos.

A Lei Geral de Proteção de Dados definiu também que, parcelas de alguns dados estão sujeitos a tutelas mais específicas ainda, como os dados sensíveis e os dados atinentes às crianças e adolescentes[2], assegurando que os dados tratados nos meios físicos e digitais devem ser curvar perante a lei em estudo. A lei definiu **dado pessoal sensível**[3] como o "dado

2. **Seção III**
Do Tratamento de Dados Pessoais de Crianças e de Adolescentes
Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo 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 consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

3. **Seção II**
Do Tratamento de Dados Pessoais Sensíveis
Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I - a portabilidade de dados quando solicitada pelo titular; ou

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

pessoal 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, inciso II)".

Indiscutivelmente, temos de agora em diante, um marco legal para regular o uso, a proteção e a transferência de dados pessoais no Brasil e no exterior dentro das hipóteses legais. Em síntese, a Lei Federal nº 13.709/2018 (LGPD) garante um maior controle por parte dos cidadãos sobre suas informações pessoais, exigindo em regra o consentimento explícito para coleta e uso dos dados pessoais e também obriga a oferta de opções para o usuário ter acesso na visualização, com possibilidade de correção e exclusão destes dados.

Caminhando à frente e em avanço às exposições, a Lei Geral de Proteção de Dados criou um órgão fiscal centralizador, a cargo da Autoridade Nacional de Proteção dos Dados Pessoais (ANPD), bem como em termos de responsabilidade, definiu as funções e responsabilidades dos agentes de tratamento de dados.

A título exemplificativo baseado na lei supra, o controlador adotará às decisões sobre o tratamento; enquanto o operador realizará o tratamento, em nome do controlador. Já ao encarregado caberá a tarefa de interagir com cidadãos e autoridade nacional (podendo ou não ser exigido, diante do caso concreto que vai depender também do tipo ou porte da organização e do volume de dados tratados).

No que toca à gestão de riscos e falhas, a Lei Geral de Proteção de Dados encarregou de quem gere a base de dados, encetar as ações de gestões para gerir os dados sob seus cuidados.

Um ponto muito elogiado textualmente encontrado na Lei Geral de Proteção de Dados, é no quesito da transparência, diferente do que se tinha até então, agora com a vigência da mencionada lei, quando houver vazamento de dados, os indivíduos afetados deverão ser avisados.

A apontada lei em estudo também previu multas pesadas por eventuais falhas de segurança dos dados pessoais, com isso, a lei em suas en-

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

trelinhas conclama aos responsáveis pela gestão de dados pessoais que venham reforçar a segurança nos dados armazenados e que transitam no mundo digital.

Na ótica da necessidade e finalidade, a lei em abordagem disciplina que estas (necessidade e finalidade) são quesitos do tratamento dos dados pessoais que devem ser informadas de maneira prévia ao cidadão.

Passaremos a analisar mais detidamente a Lei Geral de Proteção de Dados.

2. A LEI GERAL DE PROTEÇÃO DE DADOS

Como já dito, com o advento da Lei Geral de Proteção de Dados se projetou um cenário de maior segurança jurídica a todos no plano digital dentro do país e fora dele, mormente quanto à conceituação e definição de dados pessoais relacionados à pessoa humana.

Dentro de um espírito constitucional para o exercício da cidadania e da dignidade da pessoa humana, a Lei Geral de Proteção de Dados traz o consentimento do cidadão como a base para a tutela dos dados a serem objetos de tratamento dentre outros.

Mas o quê isto significa? Isto corresponde ao fato de que os dados pessoais do indivíduo pela nova Lei Geral de Proteção de Dados, só poderão em regra serem tratados e compartilhados, com o consentimento do cidadão. Afora isto e senão tiver dentro das exceções legais, haverá responsabilizações aos atores legais da iniciativa privada e pública.

Todavia, como já assinalado, há exceções em que estes dados poderão ser tratados ou compartilhados, quais sejam, nas hipóteses de indispensabilidade para cumprir obrigações legais. Assim, em outras palavras, sem o consentimento do usuário, apenas quando for indispensável para atender aos ditames da lei é que será possível tratar e fornecer os dados pessoais. Exemplo prático, seria aquele em que o Poder Judiciário requisita dados pessoais de um indivíduo. Outro exemplo prático é aquele em que o Delegado de Polícia dentro da lei, requisita dados pessoais cadastrais de um alvo investigado.

Outras exceções estão também quando os dados forem necessários para executar política pública prevista em lei; para estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular;

proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

Os fundamentos da proteção de dados estão catalogados no art. 2º da lei em voga:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A Lei Federal nº 13.709/2018 traz definições importantes além das já explanadas, como dado anonimizado, banco de dados entre outros previstos no art. 5º que pedimos vênia para transcrevê-lo:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal 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;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
>
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> 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;