A responsabilidade civil na Lei Geral de Proteção de Dados

Walter Aranha Capanema[1]
Advogado e professor

Resumo: Este artigo pretende traçar um panorama sobre as normas relativas à proteção de dados na Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGDP), buscando, também, sugerir formas de aplicação.

Palavras-chave: Responsabilidade Civil. Proteção de Dados. Dados Pessoais. Privacidade. Intimidade. LGPD.

Introdução

O legislador brasileiro, com o seu costumeiro atraso em acompanhar os avanços da sociedade e da tecnologia, somente em 2018 se preocupou em regular com efetividade a proteção de dados pessoais, o que ocorreu com a edição da Lei 13.709/2018, a denominada Lei Geral de Proteção de Dados (LGPD).

É verdade que já existiam outras leis que tratavam, de alguma forma, sobre o tema, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011), dentre outras.

A LGPD coloca o indivíduo (a quem denomina de "titular"[2]), como protagonista das relações jurídicas que envolvam o tratamento de dados[3], não só porque regula a proteção de dados **pessoais**, mas, principalmente, elege como fundamento em seu

[1] Coordenador da Pós-Graduação em Direito Digital do Instituto de Ensino e Pesquisa do Ministério Público do Estado do Rio de Janeiro (IEP-MPRJ). Coordenador do Curso de Extensão em Direito Eletrônico da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Coordenador de Prerrogativas de Processo Eletrônico e Inteligência Artificial da OAB-RJ. Membro da Comissão de Proteção de Dados da OAB-RJ. Diretor de Inovação e Ensino da Smart3. Professor Convidado da Escola Paulista da Magistratura, da Escola Superior da Advocacia do Rio de Janeiro, da Escola Judiciária Eleitoral do Tribunal Superior Eleitoral, da Escola da Magistratura da Regional Federal da 2ª Região e da Fundação Getúlio Vargas.

[2] Art. 5º: "V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

[3] Art. 5º: "X – 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".

art. 2º, II, a **"autodeterminação informativa"**, que consiste no direito de escolher quais dados serão usados, bem como os limites e o prazo dessa utilização[4].

A autodeterminação, portanto, é garantida pela previsão de vários direitos no Capítulo III, especialmente no art. 18, como o de informação (I), de acesso (II), de correção (III), de portabilidade (V), de eliminação (VI), dentre outros.

Por sua vez, esses direitos correspondem a um rol de deveres voltados a quem exerce a atividade de tratamento de dados. A LGPD diferencia esses deveres conforme a relação destes com o tratamento, denominando aquele que exerce a decisão sobre o tratamento de **controlador**[5], enquanto aquele que executa o tratamento, sob as ordens do controlador, de **operador**[6]. Juntos, eles são os **"agentes de tratamento"**[7].

Sob uma visão civilista, o controlador seria o **mandante**, e o operador, o **mandatário**. Talvez possa se aventar a hipótese de que a relação controlador-operador constitua modalidade especial de mandato, própria das relações que envolvam tratamento de dados pessoais.

Há ainda nessa relação jurídica um outro ator: o encarregado[8], pessoa natural ou jurídica, integrante ou não dos quadros do controlador ou do operador, que exerça, dentre outras funções, a intermediação entre os demais atores, especialmente a Autoridade Nacional de Proteção de Dados (ANPD) e, ainda, orienta a aplicação das normas de proteção de dados[9].

Essa complexa relação de múltiplos atores e deveres aqui relatada em resumo evidencia o desafio que as empresas privadas e órgãos públicos encontrarão para estar em conformidade com a LGPD. Os efeitos do não-atendimento passam não só pelas sanções administrativas que podem ser eventualmente impostas pela ANPD, mas em maior escala, por ações de responsabilidade civil.

A questão da responsabilidade civil, por estar relacionada necessariamente a ações judiciais, é talvez o aspecto da LGPD que mais interessa ao Poder Judiciário e, portanto, será analisada neste artigo.

1. A responsabilidade civil na LGPD

A responsabilidade civil está regulamentada na Seção III do Capítulo VI da LGPD, intitulada de "Da Responsabilidade e do Ressarcimento de Danos". É importante ressaltar que tais normas não serão aplicáveis em todos os casos envolvendo responsabilidade civil, podendo, dependendo da relação jurídica, ceder espaço a normas específicas, como o

[4] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 196.

[5] Art. 5º: "VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

[6] Art. 5º: "VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

[7] Art. 5º: "IX – agentes de tratamento: o controlador e o operador. Numa aparente contradição, as normas relativas ao encarregado estão na Seção II do Capítulo VI, intitulado 'Dos Agentes de tratamento de dados pessoais'".

[8] Art. 5º: "VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

[9] Art. 41: "§ 2º As atividades do encarregado consistem em: [...] III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais".

Código de Defesa do Consumidor, o que, inclusive, é expressamente reconhecido pela LGPD em seu art. 45[10].

A responsabilidade surge do exercício da atividade de proteção de dados que viole a **"legislação de proteção de dados"**. Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Deve-se aqui fazer uma analogia com o conceito de "legislação tributária" do art. 96 do CTN[11], para incluir não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades[12].

Mas a responsabilidade civil na LGPD não surge apenas da violação do microssistema jurídico de proteção de dados. É preciso interpretar o art. 42, *caput* em conjunto com o art. 44, parágrafo único, que assim dispõe:

> *Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.*

O art. 46, por sua vez, estabelece que os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas visando a proteção de dados pessoais[13]. Tais normas podem ser editadas, inclusive, pela ANPD[14].

Pela complexidade da atividade de segurança da informação, devem ser consideradas apenas aquelas medidas previstas em padrões devidamente reconhecidos, como as denominadas normas ISO[15].

Dessa forma, é possível identificar duas situações de responsabilidade civil na LGPD:

a) violação de normas **jurídicas**, do microssistema de proteção de dados;
b) violação de normas **técnicas**, voltadas à segurança e proteção de dados pessoais.

E, evidentemente, só caracterizará a responsabilidade civil, se a violação de norma jurídica ou técnica ocasionar dano material ou moral a um titular ou a uma coletividade.

---

[10] "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

[11] "Art. 96. A expressão "legislação tributária" compreende as leis, os tratados e as convenções internacionais, os decretos e as normas complementares que versem, no todo ou em parte, sobre tributos e relações jurídicas a eles pertinentes".

[12] BANCO CENTRAL DO BRASIL. *Resolução nº 4.658, de 26 de abril de 2018*. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://bit.ly/369JHql. Acesso em: 27 set. 2019.

[13] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

[14] Art. 46: "§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei".

[15] ISO é o acrônimo de International Organization for Standardization, uma entidade internacional que estabelece normas e padrões. O padrão ISO 27001, por exemplo, é destinado à segurança da Informação. Seu sítio está disponível em: https://bit.ly/2G75cO2. Acesso em: 21 jan. 2020.

O art. 42 restringe a responsabilidade civil ao controlador **ou** ao operador. A presença da conjunção alternativa "ou" estabelece a alternância entre um (controlador) ou o outro (operador). Obviamente, se a relação jurídica do titular com o controlador e o operador for de natureza consumerista, serão aplicadas as normas de responsabilidade solidária dos arts. 12 e 18 do CDC.

O § 1º excepciona a regra de alternância do *caput*, permitindo a solidariedade em dois casos específicos, com vistas a "assegurar a efetiva indenização ao titular dos dados".

No inciso I, o operador responderá solidariamente em duas situações: caso descumpra a legislação de proteção de dados ou se não seguir "as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador". É muito semelhante, nesse caso, na situação do mandatário que descumpre as instruções do mandante, conforme o art. 679, CC[16].

Já no inciso II, ocorrerá a solidariedade entre "os controladores que estiverem diretamente envolvidos no tratamento", ou seja, aqueles que estabelecerem, em conjunto, decisões que violem o microssistema da proteção de dados ou às normas técnicas cabíveis.

Tais hipóteses de solidariedade estarão afastadas caso presentes as hipóteses de exclusão de responsabilidade, previstas no art. 43.

A LGPD não fala na responsabilidade civil do encarregado, contudo ela poderá surgir, por exemplo, quando essa função for exercida por uma pessoa natural ou jurídica destacada do controlador e do operador em uma relação consumerista. Por se estar diante de alguém que está na cadeia de produção, poderá ser responsabilizado de forma solidária pelo dano causado.

O § 2º admite a inversão do ônus da prova, a critério do juiz, a favor do titular de dados, desde que verossímil a alegação, haja hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular for excessivamente onerosa. Há normas sobre a redistribuição/inversão do ônus da prova em outras leis: uma muito semelhante no art. 373, § 1º do CPC[17] e outra no art. 6º, VIII do CDC[18], aplicável nas ações de natureza consumerista, exigindo menos requisitos.

Além da inversão do ônus probatório, o reconhecimento da hipossuficiência do titular também se verifica no fato de que a responsabilidade civil da LGPD ser da modalidade objetiva, onde não há discussão sobre a culpa do agente.

[16] Art. 679: "Ainda que o mandatário contrarie as instruções do mandante, se não exceder os limites do mandato, ficará o mandante obrigado para com aqueles com quem o seu procurador contratou; mas terá contra este ação pelas perdas e danos resultantes da inobservância das instruções".

[17] Art. 373: "§ 1º Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído".

[18] Art. 6º: "VIII – a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências".

2. Exclusão da responsabilidade civil

2.1. Hipóteses de exclusão

As hipóteses de exclusão da responsabilidade civil estão previstas no art. 43 da LGPD.

O inciso I trata da situação em que o agente não realizou o tratamento de dados a que lhe foi atribuído. Ou seja, houve um tratamento de dados, mas o réu não tem qualquer vínculo com ele. Aproxima-se muito da figura da ilegitimidade passiva, que a LGPD trata como matéria de mérito.

Já o inciso II exclui a responsabilidade na situação em que o agente realizou o tratamento, mas "não houve violação à legislação de proteção de dados". Aqui, o dano ocorreu por um ato lícito.

Seria o caso, por exemplo, de uma decisão automatizada, baseada em critérios transparentes, informados (presentes em termos de uso) e sem viés, que negue um empréstimo a um possível consumidor. O presente inciso prevê expressamente apenas a situação em que não houve violação à proteção de dados. Deve-se interpretar este artigo em conjunto com os arts. 42, 44, 46 e parágrafo único, conforme as razões já apresentadas, de modo a admitir, também a alegação de ausência de violação de **norma técnica**.

A alegação de culpa exclusiva do titular ou de terceiro está prevista no inciso III do art. 43. Serão os casos em que o dano for causado por exclusiva ingerência do titular, por terceiro, ou por uma atuação conjunta do titular com o terceiro.

Mas, ainda assim, caberão alguns questionamentos.

Imagine a situação em que houve a invasão da conta de e-mail de um usuário, com a destruição de todas as suas mensagens. Tal fato só ocorreu porque a senha utilizada pelo titular era fraca, com apenas quatro caracteres, e foi facilmente descoberta. Poder-se-ia aqui falar em culpa exclusiva do titular? Caberia aos agentes de tratamento verificar a segurança da senha criada pelo usuário e impedir o uso daquelas que fossem frágeis? Existe norma técnica estabelecendo essa obrigação?

2.2. Vulnerabilidades e *0-day*

Vale a pena trazer para a discussão um tema relacionado à segurança da informação e que certamente repercutirá na aplicação da lei: a vulnerabilidade, um conceito da tecnologia, entendido como a "condição que, quando explorada por um atacante, pode resultar em uma violação de segurança"[19].

As vulnerabilidades, quando eventualmente descobertas, são documentadas e catalogadas em sites como o *Common Vulnerabilities and Exposures* – CVE[20], permitindo que os responsáveis pela segurança da informação das empresas e órgãos públicos adotem medidas técnicas para prevenir tais incidentes.

[19] HOEPERS, Cristine; STEDING-JESSEN, Klaus. *Fundamentos de Segurança da Informação*. [*S. l.*]: Escola de Governança da Internet no Brasil. Disponível em: https://bit.ly/2unOasd. Acesso em: 27 set. 2019.

[20] Disponível em: https://bit.ly/30KTguP. Acesso em: 21 jan. 2020.

Dessa forma, se houve um dano a dados pessoais decorrentes do não-atendimento de uma norma técnica, relativa a uma vulnerabilidade já conhecida e documentada, fica, assim, evidenciada a negligência do agente de tratamento.

Contudo, é possível que o dano seja causado pelo emprego das chamadas "vulnerabilidades não-documentadas", também conhecidas como *0-day*[21]. Nesse caso, seria incabível a responsabilização civil, afinal, se não se sabe ainda da sua existência, não tem como exigir o dever de segurança.

Logo, não é possível se atribuir aos agentes de tratamento o dever de segurança/proteção dos dados pessoais em toda e qualquer hipótese, mas apenas no estado da arte/técnica existente à época.

E, mais, deve-se entender que a obrigação de segurança é de meio, e não de resultado. É impossível ao agente de tratamento garantir, com 100% de certeza, que os dados dos titulares estarão seguros contra qualquer incidente. É preciso, portanto, razoabilidade.

3. Critérios para a definição do *quantum* indenizatório

O art. 944 do Código Civil dispõe que "A indenização mede-se pela extensão do dano". E a extensão de um dano relativo à proteção de dados poderá levar em consideração os seguintes critérios:

a) a quantidade de dados pessoais afetados;
b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis[22], por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos;
c) a reincidência da conduta;
d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados;
e) a ausência de notificação dos usuários da ocorrência do incidente[23];
f) a comprovada utilização dos dados pessoais vazados de titulares por terceiros.

4. Exemplos pontuais de responsabilidade civil na LGPD

Embora a LGPD ainda não esteja em vigor, é possível pensar em alguns exemplos de responsabilidade civil.

[21] "A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals". ZERO-DAY vulnerability: what it is, and how it works. *Norton*, [*s. l.*], [s. d.]. Disponível em: https://nr.tn/2G7038G. Acesso em: 27 set. 2019.

[22] Art. 5º: "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".

[23] "Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

4.1. Vazamentos/*data leaks*

Um dos maiores pesadelos da modernidade consiste no vazamento de dados, normalmente por falhas de segurança. São relatados, todos os dias, diversos casos, desde abrangendo dados bancários[24], *logins* e senhas do Netflix[25], redes sociais[26] e biométricos[27].

O dano poderá ser potencializado com o posterior uso dos dados pessoais por criminosos, para a criação de identidades falsas, exploração de *logins* e acesso aos dados das vítimas.

4.2. O não-atendimento dos direitos do titular

O Capítulo III, como já foi dito, estabelece um rol de direitos para o titular. O não-atendimento a esses direitos poderá ensejar, a princípio, a configuração de um dano moral, sendo possível, inclusive, cumulá-lo com um dano patrimonial, caso a impossibilidade de exercício do direito tenha trazido lucro cessante ou dano emergente.

4.3. O *spam* e o tratamento ilegal

O spam, entendido como o envio de publicidade ou propaganda eletrônica não autorizada, não era expressamente vedado pela legislação. O Superior Tribunal de Justiça, em precedente de 2009, entendeu que não se constitui ilícito, "por ausência de previsão legal", e que há métodos de evitá-lo[28].

---

[24] TOZZATO, Luiza. Vazam quase 250 GB de dados bancários: saiba como se proteger. *Olhar Digital*, [*s. l.*], 22 jul. 2019, 18:20. Disponível em: https://bit.ly/37dCruV. Acesso em: 27 set. 2019.

[25] VAZAMENTO de senhas do Netflix: saiba o que fazer para se proteger. *O Globo*, [*s. l.*], 12 dez. 2017, 07:42. Disponível em: https://glo.bo/38sSw0c. Acesso em: 27 set. 2019. dez.

[26] POZZEBOM, Rafaela. Arquivo com 2,2 bilhões de logins e senhas vaza na internet. *Oficina da Net*, [*s. l.*], 5 fev. 2019. Disponível em: https://bit.ly/2NlmBRm. Acesso em: 27 set. 2019.

[27] LIMA, Bruna. *Falha de segurança expõe dados biométricos de 1 milhão de pessoas*. Olhar Digital, [*s. l.*], [s. d.]. Disponível em: https://bit.ly/2NND8nf. Acesso em: 27 set. 2019.

[28] "Trata-se de ação de obrigação de fazer cumulada com pedido de indenização por danos morais em que o autor alega receber e-mails (spam com mulheres de biquíni) de restaurante que tem show de streaptease e, mesmo tendo solicitado, por duas vezes, que seu endereço eletrônico fosse retirado da lista de e-mail do réu (recorrido), eles continuaram a ser enviados. Entre os usuários de internet, é denominada spam ou spammers mensagem eletrônica comercial com propaganda não solicitada de fornecedor de produto ou serviço. A sentença julgou procedente o pedido e deferiu tutela antecipada para que o restaurante se abstivesse do envio da propaganda comercial sob pena de multa diária, condenando-o a pagar, a título de danos morais, o valor de R$ 5 mil corrigidos pelo IPC a partir da data do julgamento, acrescidos de juros de mora, contados a partir do evento lesivo. Entretanto, o TJ proveu apelação do estabelecimento e reformou a sentença, considerando que o simples envio de e-mails não solicitados, ainda que dotados de conotação comercial, não configuraria propaganda enganosa ou abusiva para incidir o CDC e não haveria dano moral a ressarcir, porquanto não demonstrada a violação da intimidade, da vida privada, da honra e da imagem. Para o Min. Relator, que ficou vencido, o envio de mensagens com propaganda, quando não autorizada expressamente pelo consumidor, constitui atividade nociva que pode, além de outras consequências, gerar um colapso no próprio sistema de internet, tendo em vista um grande número de informações transmitidas na rede, além de que o spam teria um custo elevado para sociedade. Observou que não há legislação específica para o caso de abusos, embora existam projetos de lei em tramitação no Congresso. Daí se aplicar por analogia o CDC. Após várias reflexões sobre o tema, reconheceu a ocorrência do dano e a obrigação de o restaurante retirar o autor de sua lista de envio de propaganda, e a invasão à privacidade do autor, por isso restabeleceu a sentença. Para a tese vencedora, inaugurada pelo Min. Honildo de Mello Castro, não há o dever de indenizar, porque existem meios de o remetente bloquear o spam indesejado, aliados às ferramentas disponibilizadas pelos serviços de e-mail da internet e softwares específicos, assim manteve a decisão do Tribunal *a quo*. Diante do exposto, a Turma por maioria não conheceu do recurso" Resp. 844.736-DF, Rel. originário Min. Luis Felipe Salomão, Rel. para acórdão Min. Honildo Amaral de Mello Castro (Desembargador convocado do TJ-AP), julgado em 27/10/2009.

Com a vigência da LGPD, tal entendimento necessitará ser revisto.

O envio de mensagem, portanto, constitui hipótese de tratamento de dados, pois precisa de dados pessoais para ser efetivado (normalmente, endereço de e-mail ou número telefônico, no caso do WhatsApp).

E, assim, necessitará do consentimento do titular-destinatário, ou alguma outra base legal.

Logo, o tratamento de dados pessoais sem o consentimento do titular ou fora das previsões legais poderá configurar dano moral.

Conclusão

É fundamental que os operadores do Direito conheçam as regras da LGPD. A complexidade dessas normas é um desafio, mas é necessária a sua compreensão da parte do titular, para defender seus direitos em juízo e, por parte dos agentes, para a prevenção e minimização dos riscos de eventuais ações judiciais.

É preciso, portanto, conjugar a adequação à lei com uma mudança de cultura nas empresas e órgãos públicos. Os titulares e os seus dados merecem respeito.

Bibliografia

BANCO CENTRAL DO BRASIL. *Resolução nº 4.658, de 26 de abril de 2018*. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://bit.ly/369JHql. Acesso em: 27 set. 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. *Fundamentos de Segurança da Informação*. [*S. l.*]: Escola de Governança da Internet no Brasil. Disponível em: https://bit.ly/2unOasd. Acesso em: 27 set. 2019.

LIMA, Bruna. *Falha de segurança expõe dados biométricos de 1 milhão de pessoas*. Olhar Digital, [*s. l.*], [s. d.]. Disponível em: https://bit.ly/2NND8nf. Acesso em: 27 set. 2019.

ZERO-DAY vulnerability: what it is, and how it works. *Norton*, [*s. l.*], [s. d.]. Disponível em: https://nr.tn/2G7038G. Acesso em: 27 set. 2019.

VAZAMENTO de senhas do Netflix: saiba o que fazer para se proteger. *O Globo*, [*s. l.*], 12 dez. 2017, 07:42. Disponível em: https://glo.bo/38sSw0c. Acesso em: 27 set. 2019. dez.

POZZEBOM, Rafaela. Arquivo com 2,2 bilhões de logins e senhas vaza na internet. *Oficina da Net*, [*s. l.*], 5 fev. 2019. Disponível em: https://bit.ly/2NImBRm. Acesso em: 27 set. 2019.

TOZZATO, Luiza. Vazam quase 250 GB de dados bancários: saiba como se proteger. *Olhar Digital*, [*s. l.*], 22 jul. 2019, 18:20. Disponível em: https://bit.ly/37dCruV. Acesso em: 27 set. 2019.