CAPÍTULO
1

A proteção de dados no brasil

https://doi.org/10.56238/tecavanaborda-001

Gabriel Gomes da Luz
Acadêmico em Direito pela PUC/MG. Atua como pesquisador voluntário vinculado ao Programa de Iniciação Científica Voluntária (PIC-V) – PUC/MG. Gestor de gabinete no Tribunal de Justiça de Minas Gerais. Membro da ABDC. Autor de artigos jurídicos.
E-mail: amagalhaes@ig.com.br

Matheus Oliveira Maia
Acadêmico em Direito pela PUC/MG. Atua como pesquisador voluntário vinculado ao Programa de Iniciação Científica Voluntária (PIC-V) – PUC/MG. Atualmente é estagiário em gabinete de Juiz no Tribunal de Justiça de Minas Gerais. Autor de artigos jurídicos.
E-mail: amagalhaes@ig.com.br

Rodrigo Almeida Magalhães
Doutor e Metre em Direito pela PUC/MG. Professor do mestrado e doutorado em Direito na PUC/MG, professor da UFMG, advogado.
E-mail: almeidamagalhaesrodrigo@gmail.com

RESUMO
O artigo apresenta os principais conceitos da LGPD e seu contexto histórico, apresentando sua aplicabilidade no Brasil. Há também uma comparação apresentando uma análise na sua aplicabilidade e no continente europeu. O artigo conclui que o mencionado diploma normativo deu início a uma nova cultura de privacidade e proteção de dados no país. Para obtenção de resultados e conclusões, utiliza-se a metodologia de pesquisa integrada, analítica, dedutiva e a técnica de pesquisa bibliográfica.

Palavras-chave: Lei geral de proteção de dados. Marco civil da internet. Vazamento de dados.

1 INTRODUÇÃO

O artigo pretende analisar a Lei Geral de Proteção de Dados (LGPD). Para isso, será construído um raciocínio lógico-argumentativo consistente em demonstrar a relevância da conclusão a que o artigo se propõe: discorrer sobre o surgimento da LGPD e os impactos iniciais que esta causa na sociedade.

Logo, pode-se apontar que a Lei Geral da Proteção de Dados foi promulgada em 2018, com o objetivo de regulamentar a organização de dados pessoais no Brasil. Com isso, o trabalho observa o contexto histórico, apontando de como surgiu a proteção de dados e o contexto na qual foi instaurada para proteger os dados brasileiros.

A aplicabilidade desta lei tem vastos impactos na sociedade e como um dos principais pode-se destacar o consentimento das pessoas ao compartilharem os seus dados pessoais e a vulnerabilidade desta transferência de dados.

Assim o objetivo deste trabalho é demonstrar alguns conceitos para entender melhor os impactos que a LGPD pode causar e analisar a sua eficiência na sua aplicabilidade no Brasil. Inicia-se o artigo com alguns conceitos básicos, passa a descrever o contexto do surgimento da lei no mundo e no Brasil, analisa o Marco Civil da Internet e a elevação da proteção de dados como direito fundamental.

Para essa análise a metodologia de pesquisa adotada é a integrada, analítica, dedutiva e a técnica de pesquisa bibliográfica.

2 CONCEITOS FUNDAMENTAIS

Para discutir sobre a LGPD, é necessário demonstrar o conceito do consentimento, pois este é um dos conceitos fundamentais ao discutir sobre proteção de dados. Isso há muita interferência da história da proteção de dados, onde previamente da promulgação da LGPD, o Marco Civil da Internet (Lei 12.965/14) em pouco tempo reivindicava o consentimento transparente dos titulares para a realização da coleta, utilização e análise dos dados pessoais.

O ponto em que se iniciou a discussão do consentimento, foi quando o projeto de lei 4060/12 foi aprovada e que se tornou a LGPD, isso ocorreu devido no início da PL o objetivo não estava ligado com os padrões da Europa e nem observava sobre o conceito de consentimento, assim sofreu várias alterações com o passar dos anos, se aproximando cada vez mais da regulação Europeia, principalmente atribuindo o consentimento como um dos principais conceitos para o desenvolvimento da proteção de bens.

É válido ressaltar que o tratamento para uso de dados pela LGPD se aplica pelo princípio da segurança, da prevenção e da transparência, uma vez que, na maioria dos casos o uso se dá pelos consentimentos, mas há empresas que não informam normalmente que ao se tratar de dados de tais clientes, estes já possuem o consentimento de que a empresa realiza todas as atividades de forma segura e não dão consentimento para todas as fases de sua aplicabilidade.

Assim pode-se definir o consentimento de acordo com a LGPD (Lei nº 13.709/18, art. 5º, XII) como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Outro conceito fundamental da LGPD e que tem forte influência nas discussões no Congresso Nacional é sobre o dado pessoal. Para conseguir entender e conceituar o dado pessoal de uma forma mais clara é necessário entender que existem duas vertentes cabíveis de interpretação para contextualizar o dado pessoal de forma moderna, ou seja, o embate entre a acepção expansionista sobre pessoas “identificáveis” ou reducionista á uma pessoa identificada. Segundo a teoria reducionista, “somente pode ser classificado como dado pessoal aquele que corresponde a uma pessoa específica, ou seja, um documento de identidade, um dado biológico único. Diferentemente da acepção expansionista, na qual “não demanda uma relação direta e perfeita entre uma pessoa e um dado para que tal dado possa ser caracterizado como um dado pessoal”.

Após ter em vista as duas teorias sobre o dado pessoal, a LGPD adotou o significado expansionista, ou seja, todo dado pessoal é uma informação relacionada a uma pessoa identificada ou identificável, portanto a doutrina brasileira interpreta que os dados pessoais não se limitam.

3 CONTEXTO HISTÓRICO

3.1 MUNDIAL

No início de 2018 havia pouco conteúdo sobre os debates envolvendo a privacidade no Brasil, porém com a implantação da Regulação Geral de Proteção de Dados Europeia (popularmente conhecida como GDPR) e com um momento de desordem com várias situações de violação de dados, podemos afirmar que o caso da Cambridge Analytica mostrou as pessoas em nível mundial o poder e o controle que podem ser adquiridos com a posse de dados.

3.2 CASO CAMBRIDGE

O caso da Cambridge Analytica foi conhecido por uma empresa com este nome, utilizou informações de mais de 50 milhões de pessoas sem o consentimento delas para realizar propaganda política. Estes dados foram retirados do Facebook através de um aplicativo lançado para realizar um teste psicológico nas redes sociais. Logo aqueles usuários que participaram deste teste entregaram afora de suas informações, mas também de todas as pessoas adicionadas como amigas no perfil para esta empresa (Privacidade hacekada, netflix, 2019).

Após dois dias sobre a publicação desta notícia o valor do Facebook foi encolhido em Us$ 35 bilhões (aproximadamente R$ 115,5 bilhões) na bolsa de valores de tecnologia dos EUA. Com isto a empresa começou a ser investigada pelas autoridades dos EUA e do Reino Unido, fazendo com que o CEO do Facebook Mark Zuckerberg testemunhasse diante à um comitê legislativo.

Nesta época muitos se perguntaram como que foi extraído estes dados, e segundo Christopher Wylie ex-funcionário da Cambridge Analytica, relatou que o esquema começou em 2014, ou seja, dois anos antes das eleições americana e três anos antes do Brexit.

A pergunta que estava na maioria das pessoas era como que o aplicativo realizou a coleta de dados e Wylie afirmou que além do conhecimento de que muitos usuários não ficam lendo os longos termos de condição e uso, havia uma brecha do facebook em colher os dados das amizades dos usuários que usaram o aplicativo, ou seja, através de uma pessoa que realizasse o uso do aplicativo havia a coleta não apenas de um dado, mas de vários dados.

Os dados coletados eram os nomes, profissões, localização, além de comportamentos habituais que eram retirados da rede de contatos. Muitos acharam que Cambridge tinha utilizado algum hacker para obter dados do Facebook, porém foi relatado que eles utilizaram uma “brecha” que o aplicativo

tinha para se aproveitar da situação. Assim o Facebook observou a "brecha" e corrigiu ela com o passar dos meses, porém acionou a justiça afirmando que a empresa por difamar pela ocultação da "brecha", ou seja, não reportou o problema ao Facebook.

Portanto, a partir deste caso o mundo percebeu a importância dos dados e começaram a realizar vários conhecimentos sobre esta área, um dos principais países que deram esta importância foi o Brasil.

3.3 GDPR (GENERAL DATA PROTECTION REGULATION).

A GDPR (Regulamento Geral de Proteção de Dados da União Europeia) entrou em vigor em 25 de maio de 2018, ela normatiza a proteção dos dados pessoais no âmbito da União Europeia, tendo uma aplicação transnacional. A GDPR é considerada como um marco para garantir aos titulares informações precisas sobre os motivos das decisões automatizadas. Essa garantia pode ser definida como um direito do titular de ser informado sobre como são tomadas as decisões, bem como de solicitar revisão.

O Brasil tem na sua legislação (LGPD) a mesma proporção da GDPR sobre o controle e operação dos dados pessoais. Na GDPR em seu artigo quinto, inciso um, podemos visualizar que:

> Artigo 5. Princípios relativos ao tratamento de dados pessoais
> I. Os dados pessoais são:
> a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.,n.1 («limitação das finalidades»);
> c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

Com isso, pode-se notar que este artigo demonstra a essência dos dados pessoais, ou seja, o titular dos dados possuí direitos de que seus dados devem ser tratados de forma lícita, leal e com transparência, para justamente oferecer o consentimento a ele, o uso necessário dos dados no mundo contemporâneo. Além disto, e notória a limitação das finalidades justamente para o Estado simplificar o sistema de segurança e ter eficácia em suas medidas para o controle de dados dos seus cidadãos.

No artigo 5º da Lei Geral de Proteção de Dados podemos visualizar o conceito de dados, bem como suas espécies. Cuja redação importa transcrever:

> 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;

Portanto, pode-se observar que o Brasil praticamente se espelhou na mesma essência da segurança da GDPR, utilizando vários conceitos para efetivar o controle de dados de forma clara e precisa. Um desses conceitos são do titular, na qual é a pessoa que tem seus dados como objeto de segurança do Estado; Do controlador, na qual se refere aos responsáveis do tratamento dos dados pessoais, ou seja, para compreender analiticamente observa-se como exemplo uma empresa que realiza um pedido de dados ao seu funcionário e geralmente a parte administrativa mantém o controle de dados deste; E por fim o operador, que é justamente quem trabalha no setor administrativo de uma empresa e realmente "opera" com os dados pessoais daquele funcionário para o controle da empresa.

3.4 NACIONAL.

Com a aprovação da Regulamentação Geral de Proteção de Dados (GDPR) feita pela União Europeia e com o vazamento sobre o caso Cambridge, foi necessário por em pautas a relevante necessidade em que o Brasil havia que aprimorar sua legislação de proteção de dados de uma maneira mais rígida. Deste modo, buscando orientar a coleta, os usos, os dados armazenados e o processamento de dados tanto públicos quanto privados, foi necessário enquadrar a legislação de acordo com um padrão internacional.

Danyelle e Aires enfatizam que a inclusão digital no Brasil apresenta-se como um grande desafio no Brasil, uma vez que demanda a aperfeiçoamento da legislação brasileira. Logo, o intuito do Brasil em aprimorar sua legislação sobre a proteção de dados também e estimulado para pleitear seu ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), pois com este ingresso o Brasil iria ter um conhecimento mais robusto sobre a proteção de dados não de forma jurídica, mas na forma de adequar os objetivos do Estado com a sua sociedade, ou seja, para enriquecer e adequar o padrão internacional ao seu sistema (ROVER, PINTO, PEIXOTO, 2020, p. 19).

Nesse contexto, em 14 de Agosto de 2018 foi sancionada a Lei Federal n 13.709/2018, conhecida como LGPD dispõe que:

> sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

No artigo três em seu inciso três da LGPD demonstra-se que:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
>
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Além disso, em seu artigo quarto a LGPD é bem clara, demonstrando em quais tratamentos de dados em que ela é aplicada, para justamente focalizar e centralizar a segurança das medidas a serem tomadas para ter um controle simples e eficaz dos dados pessoais.

Portanto, podemos observar que há aperfeiçoamentos que devem ser realizados com maior efetividade e simplicidade, uma vez que, há a necessidade de uma inclusão digital rígida para que a sociedade acompanhe as inovações tecnológicas.

Porém, há exemplos de implantações, um dos exemplos desta inclusão foi a implantação do PJE realizada em 2006, em que segundo Barbara:

> Dentre os benefícios trazidos pela implementação pode-se destacar o aumento relativo na celeridade do processo era a principal demanda trazida devido ao fato de que o sistema permite diversas facilidades como, por exemplo, a de acesso aos processos uma vez propiciou que não fosse mais necessário que as partes ou os seus procuradores que tivessem interesse em acessar o processo se deslocassem de modo físico até o fórum. (BRAZ, 2018, p.31)

Logo, pode-se perceber que já possui exemplos de implantações da inovação digital no Brasil que devem ser usadas como exemplo para amplificação e efetivação da legislação digital brasileira.

4 MARCO CIVIL DA INTERNET

O Marco Civil da Internet é uma lei que regula o uso da internet do Brasil, ela entrou em vigor a partir de 2014 e é conhecida como “Constituição da Internet”, na qual foi uma das primeiras legislações instauradas no Brasil com o tema da internet. A finalidade que ela foi instaurada foi para o estabelecimento de garantias, direitos e deveres para disciplinar o uso da internet no Brasil.

Quando havia as discussões sobre as legislações sobre o uso da internet em 2007 e em 2009, já havia um movimento de negação a implementação da lei. Este fato ocorre principalmente pela norma criar muitos encargos e incumbências às empresas fornecedoras de internet. Porém estes encargos geram uma proteção ao usuário e fortificam a liberdade, o respeito e a boa-fé nas redes ondes os usuários usufruem da internet. Com esta proteção se constitui a neutralidade da rede, ou seja, não há uma divisa como nas televisões a cabo em que são adquiridos pacotes de funcionalidades distintas com preços proporcionalmente divididos a quantidade de funcionalidades de cada pacote.

A neutralidade tem como finalidade oferecer maior liberdade ao usuário de usufruir seu produto com maior funcionalidade e fazendo com que seu preço do mercado seja mais acessível, podemos observar isso nos novos serviços lançados nos últimos tempos como Netflix, Youtube e Skype. Estes serviços executam muitos vídeos e geram um consumo de dados acentuado e contínuo, devido a informação ser processada imediatamente no vídeo, ou seja, sem atrasos no procedimento de dados, pois se ocorrer os atrasos, os vídeos não vão carregar e os provedores para acessarem estes dados vão demorar para corrigirem o procedimento.

Tendo o conhecimento das funcionalidades dos procedimentos de como são feitos os serviços de internet, podemos observar como que as empresas podiam se "aproveitar" por não ter uma norma padronizada do serviço. Como o cliente pagava por funcionalidades as empresas tentavam excluir do seu pacote de dados o uso de um serviço ou até mesmo limitavam os dados de conexão para o acesso do programa. Com isso o cliente estava dependente da boa-fé da fornecedora do serviço para usufruir da internet.

Pode-se observar como foi feita toda proibição pela Lei do Marco Civil em questão de os dados ficarem cientes apenas para as empresas fornecedoras de serviços, mas precisamos entender a essência, na qual, deve-se pautar o motivo na qual o Marco Civil interrompeu esta metodologia do uso de dados.

O motivo pode ser dividido em duas partes, a primeira é observada a forma de consumo do ciente, na qual, a empresa fornecedora de serviços de internet, não buscava oferecer muitas opções aos clientes, ou eram insuficientes ou eram exacerbadas as opções de compra do serviço, o cliente não conseguia ter uma satisfação de fato por pagar o serviço. Logo, o domínio da fornecedora era exacerbado e não havia espaço para que o cliente desfrutasse do serviço prestado.

A segunda parte é o modo em que a fornecedora realiza uma "censura" nos dados do ciente, na qual ela limitava arbitrariamente quais sites ou programas o consumidor poderia acessar, sem permitir que este discordasse.

De acordo com Rayssa Allves podemos observar que o objetivo da neutralidade da rede é evitar a concorrência desleal:

> Além disso, a neutralidade de rede busca evitar a concorrência desleal, pois normalmente o provedor de internet também é a empresa que fornece telefonia. Neste caso, ela não poderia limitar ou impedir o acesso a programas que façam ligações telefônicas, como é o caso do Skype, que também faz ligações nacionais e internacionais, normalmente a preços mais módicos. Afinal, a Lei do Marco Civil busca sempre manter a liberdade e proteção do usuário. (ALVES, RAYSSA, 2017, p.90)

A autora relata que já ocorreu uma situação interessante no Brasil, sobre um possível delito da neutralidade de rede. Acerca de 2015 a empresa TIM estabeleceu uma campanha publicitária chamada "TIM Whatsapp", em que seus clientes poderiam ter o acesso gratuito do aplicativo Whatsapp e que

poderiam mandar suas mensagens sem o consumo de nenhum dado de sua franquia de internet ou mesmo sem precisar de ter créditos no celular para tanto.

Neste caso, podemos observar que a Tim privilegia o Whatsapp, pois há outros aplicativos que realizam o mesmo serviço, porém são necessários dados para ter o acesso, logo podemos observar a grande relevância que o Marco Civil da Internet realizou e observamos a necessidade que a lei se expanda para diversas ocasiões para acompanhar dinamicamente a Era digital.

5 EMENDA CONSTITUCIONAL Nº 115/22. A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

A constituição da república Portuguesa já dispunha em seu texto desde o ano de 1976 a proteção em face do uso da informática e, em parte, também a questão dos dados pessoais.

Partindo-se da premissa portuguesa foi promulgada a EC nº 115 de 22, no Brasil, a qual dispunha sobre a conveniência e oportunidade da inserção de um direito à proteção de dados pessoais na CF, ficou, de certo modo, superada. De acordo com o texto da EC 115, foi acrescido um inciso LXXIX ao artigo 5º, CF, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (Incluído pela Emenda Constitucional nº 115, de 2022).

Ora, tal direito fundamental já era possível se abstrair de uma leitura ampla acerca do disposto no artigo art. 5º, X, da Carta Cidadã, direito à privacidade- ligado ao princípio da inviolabilidade, sobretudo das comunicações.

Portanto, a inserção de tal direito de forma autônoma possibilitou um maior reforço à aplicação da Lei Geral de Proteção de Dados, bem como a sua utilização com respaldo na própria constituição federal, o que legitima de forma dobrada a sua aplicabilidade.

A EC 115/22 também incluiu os incisos XXVI e XXX, respectivamente, aos artigos 21 e 22 da Carta Magna, atribuindo à União competência para organizar e fiscalizar a proteção e o tratamento de dados pessoais, bem como competência privativa para legislar sobre a matéria.

Portanto, conclui-se que, além da nova LGPD, Código de Defesa do Consumidor, Código Civil, Lei de Acesso à Informação, Lei do Cadastro Positivo e Marco Civil da Internet, impõe-se ao Estado (isso já independentemente da inserção do direito à proteção de dados pessoais no texto constitucional, mas com ainda mais razões com a sua positivação expressa!), por força de seus deveres de proteção, não apenas zelar pela consistência constitucional do marco normativo infraconstitucional (inclusive da LGPD) no tocante aos diplomas legais isoladamente considerados, mas também de promover sua integração e harmonização produtiva, de modo a superar eventuais contradições e assegurar ao direito fundamental à proteção de dados, sua máxima eficácia e efetividade (Sarlet, 2022).

Discute-se se uma emenda constitucional pode alterar os direitos fundamentais, porque, se puder incluir, pode também retirar? O debate é muito mais acadêmico do que prático porque a proteção de dados já estava na Constituição Federal.

6 CONSIDERAÇÕES FINAIS

No entanto, esse cenário mudou em 14 de agosto de 2018, com a entrada em vigor da lei de 2018. 13.709/2018, a lei Geral de Proteção de Dados Pessoais - LGPD, que dispõe sobre o tratamento de dados pessoais por pessoas físicas ou jurídicos de direito público ou privado, inclusive os portadores de dados digitais, com o objetivo de resguardar o princípio da liberdade e da confidencialidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Além de ser a primeira lei geral nacional sobre o tema, a importância da Lei Geral de Proteção de Dados está na introdução de regras para o tratamento de dados pessoais. Estas regras vão desde os princípios que regem a proteção de dados pessoais, aos fundamentos legais que podem justificar o tratamento de dados, às verificações e responsabilização dos envolvidos no tratamento de dados pessoais.

A referida lei também proporciona à pessoa física a quem os dados pessoais se referem a possibilidade de solicitar informações como confirmação da existência do tratamento de seus dados pessoais, acesso a dados, correção de dados incompletos, eliminação de dados desnecessários e portabilidade de dados pessoais dados para outro fornecedor de produtos e serviços.

Em resumo, o mencionado diploma normativo deu início a uma nova cultura de privacidade e proteção de dados no país, logo reforçada pela Emenda Constitucional nº 115/22, que exigia a conscientização de toda a sociedade sobre a importância dos dados pessoais das pessoas físicas, bem como jurídicas, como liberdade, privacidade e livre desenvolvimento da personalidade.

BIBLIOGRAFIA

Alves, rayssa. “a lei do marco civil, a internet e as startups”. Legal talks: startups à luz do direito brasileiro. [recurso eletrônico] / anna fonseca martins

Barbosa; eduardo goulart pimenta; maurício leopoldino da fonseca (orgs.) – porto alegre, rs: editora fi, 2017.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Diário oficial da união, brasília, 1, dez.2018 .disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm/>. Acesso em: 27 dez. 2022.

Braz, barbara. “processo judicial eletrônico como meio de acesso a justiça”, acesso a justiça, formas de solucao de conflitos e a tecnologia”, recaj-ufmg, junho de 2018.

Bechara, gabriela e rodrigues, horacio. “ marco civil da internet no brasil: conquistas e desafios”, direito, governança e novas tecnologias”, equipe editorial index law journal, junho de 2020.

Gdbr. Disponível em: <https://gdpr-info.eu>. Acesso em: 27 dez. 2022.

Entenda o escândalo de uso político de dados que derrubou valor do facebook e o colocou na mira de autoridades. Disponível em: <https://www.letras.mus.br/skank/72339/>. Acesso em: 27 dez. 2022.

Privacidade hackeada – netflix. Disponível em: <https://www.netflix.com/br/title/80117542/>. Acesso em: 27 dez. 2022.

Sarlet, ingo wolfgang. A ec 115/22 e a proteção de dados pessoais como direito fundamental. Disponível em: < https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental#:~:text=de%20acordo%20com%20o%20texto,n%c2%ba%20115%2c%20de%202022/ >. Acesso em: 27 dez. 2022.