

MANUAL SOBRE LEI GERAL DE PROTEÇÃO DE DADOS

PARA USÚARIOS

**Denilson Miranda
Eduarda Damasceno
Guilherme Araújo**

Súmario

Apresentação	5
Dados Pessoais	
o O que são dados?.....	6
Proteção dos Dados	
o Importância da Proteção de Dados Pessoais.....	9
Crimes Virtuais	
o Crimes Virtuais.....	11
- Phishing	12
- Malware	13
- Ransomware	13
- Farmjacking	13
LGPD - Introdução	
o Introdução à LGPD	14
o Legislação Brasileira	14
- Lei Carolina Dieckman	15
- Marco Civil da Internet	17
LGPD	
o LGPD - Lei Geral de Proteção de Dados	19
o Tratamento de Dados	20
o Proibições	22
o Conceitos Básicos da LGPD	23
Princípios da LGPD	
o Conceitos Básicos da LGPD	24
o Princípios da LGPD	26
Direitos dos Titulares	
o Direitos dos Titulares	30
Dados Sensíveis	
o Dados Sensíveis	34
o Exceções	35
o Exposição e Transferência de Dados Pessoais	36
Referências	



Apresentação

O presente manual foi desenvolvido devido à falta de conhecimento a respeito de segurança de dados pessoais por grande parte da população ao utilizar dispositivos informáticos, principalmente ao navegar na internet e ao contratar serviços, sejam eles físicos ou digitais.

Buscando garantir as pessoas o direito à privacidade, segurança e controle dos seus dados pessoais, uma nova Lei entrou em vigor em 18 de setembro de 2020, a chamada Lei Geral de Proteção de Dados (LGPD).

Esse manual é voltado completamente para os usuários, buscando utilizar uma linguagem simples para o entendimento de todos.

Trataremos de explicar conceitos importantes para o entendimento do que é a proteção de dados e como a LGPD se aplica, apresentando dicas de como os usuários devem se portar para manter seus dados seguros, sem exposições indevidas, assim como, os direitos adquiridos com esta nova lei.

O que são dados?

Um dado é qualquer particularidade de um objeto ou sistema que possa ser registrado, ou seja, um dado por si só, não forma uma informação, mas um conjunto de dados formam, logo, um dado é um fragmento da informação que pode ser armazenado, esse armazenamento pode ser físico ou virtual.

Exemplos de dados:

Alguns nomes de pessoas, animais, objetos, lugares escritos em uma folha de papel, um caderno, um livro entre outros.

Alguns nomes de pessoas, animais, objetos, lugares escritos em um arquivo de texto em qualquer meio informático como celular, computador.

Nesses exemplos, são apenas nomes aleatórios que não possuem um significado para quem o ler.



O que é uma informação?

É um conjunto de dados que possuem um significado, podemos dizer que é o resultado da organização de um conjunto de dados.

Exemplo de uma informação:

A seguinte frase escrita em uma folha de papel “Meu nome é Maria, eu tenho um cachorro como animal de estimação e ele gosta de brincar com uma bola no parque da cidade”.

Usando os dados do exemplo anterior, ao juntarmos esses dados construímos uma informação e atribuímos um sentido para os dados.

O que são os dados e informações pessoais?

São todos os dados e informações que facilitam ou permitem a identificação de uma pessoa natural.



Quais são os dados pessoais?

Nome, sobrenome, apelido de uma pessoa;
CPF;
RG;
Idade;
Data de nascimento;
Endereço;
Endereço de e-mail;
Número de telefone/celular;
Localização (Dados do GPS);
Testemunhos de conexão (cookies);
Retrato em fotografia;
Histórico de compras e pagamentos;
Endereço de IP;
Dados detidos por um hospital ou médico de uma pessoa
(Prontuário de saúde, etc.).

Porque os dados pessoais são importantes?

Os dados pessoais, são a identidade de uma pessoa, logo são suficientes para comprovar sua existência, diretamente ou indiretamente, em um determinado serviço.

Importância da Proteção de Dados Pessoais

A proteção dos dados pessoais, aumenta a segurança, a liberdade e a confiança que o usuário sente ao utilizar os meios digitais e ao contratar um serviço, seja ele contratado fisicamente ou virtualmente.

Os dados possuem um valor maior, a partir do segundo em que eles podem se tornar informações úteis.

Riscos sofridos com a exposição de dados

Um conjunto de dados de uma pessoa específica, ao serem reunidos podem gerar informações concretas a respeito dessa pessoa.

Esse conjunto de informações, podem acarretar, na exposição de quaisquer dados pessoais!

Os dados pessoais comumente descobertos são:

Nome;
Data de Nascimento;
Idade;
CPF;
Endereço de E-mail;
Número de telefone.

Informações da localização do indivíduo como:

Endereço residencial;
Local de trabalho;
Locais mais frequentados;

Em casos onde ocorre um gerenciamento dos dados de localização, pode ser possível identificar padrões, consequentemente, a rotina de uma pessoa.

Dados financeiros, como:

Cartão de credito;
Dados bancários.

Esses são os dados que pessoas más intencionadas focam em adquirir, quando descobertos, causam a danos financeiros com transações não autorizadas.

Crimes Virtuais

São todos aqueles crimes e delitos praticados por meio da internet ou de qualquer dispositivo informático, eles visam manipular ou roubar os dados de suas vítimas.

Os atacantes geralmente tem o objetivo de atingir o equipamento e a própria vítima, em outros casos são praticados contra departamentos públicos ou empresas privadas.

Os crimes que ocorrem em maior frequência são:

- Phishing
- Malware
- Ramsonware
- Formjacking

Phishing

É realizado geralmente através do e-mail e redes sociais, nesse tipo de ataque, o criminoso induz a vítima para que ela faça o download de um programa ou abra um link malicioso, no momento em que a ação é realizada, o criminoso tem acesso as informações do aparelho.

Assim como acontece em uma verdadeira pescaria, há mais de uma maneira fisgar uma vítima, logo vários tipos de golpes de phishing.

O mais comum e que ocorre com maior frequência é:

Quando são enviados vários links divulgando sorteios, lojas oferecendo descontos absurdos, produtos que geralmente possuem alto custo, com valores mínimos, anúncios de vagas de empregos, informações do auxilio emergencial da caixa e vários outros temas que estejam em evidencia para a população.

Nesses links, existem formulários de preenchimentos que solicitam dados pessoais e dados financeiros como cartão de credito e bancários, no momento em que a pessoa preenche e envia os dados, aparece para que ela compartilhe com outras pessoas. No momento em que o link é compartilhado, mais vítimas são atraídas.

Malware

É um código malicioso, ou seja, são programas desenvolvidos com o intuito de executar ações ilícitas no dispositivo infectado, como:

- Causar danos;
- Alterações;
- Roubo de dados e informações.

Uma vez instalado, o malware imediatamente tem acesso ao armazenamento e permissões do dispositivo e pode causar danos irreparáveis.

Ramsonware

É um tipo de malware, que criptografa os dados armazenados em um dispositivo tornando-os inacessíveis, o autor do golpe geralmente exige um pagamento de resgate desses dados.

Formjacking

É outro tipo de malware, é realizado com a injeção de malwares em sites de lojas e instituições para roubar informações bancárias e de cartões de créditos dos clientes no momento da realização dos pagamentos.

Introdução à LGDP

Legislação Brasileira

Na legislação brasileira, existem leis em vigor que buscam aumentar a segurança no mundo digital e proteger os usuários e seus dados pessoais.

Leis existentes:

Lei Carolina Dieckmann;

Marco Civil da Internet;

Lei Geral de Proteção de Dados.

Lei Carolina Dieckmann

Essa lei tem este nome devido ao caso que a originou:

Em maio de 2011, um cracker (criminoso virtual) invadiu o computador pessoal da atriz Carolina Dieckmann, conseguindo ter acesso a várias de suas fotos pessoais de cunho íntimo.

Após esse caso, a lei foi sancionada em 30 de novembro de 2012, tipificando como crime a invasão de um dispositivo informático qualquer com o intuito de obter, excluir ou alterar dados nele presentes, seja no armazenamento, interno, externo ou nuvem.

Definida segundo a legislação brasileira:

Nº 12.737/2012 - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Em caso de interesse em ler em mais detalhes o que diz a Legislação Brasileira, o site pode ser acessado através do site do planalto.

A lei define que o crime existe a partir do momento em que o aparelho é acessado e as informações alteradas, excluídas ou capturadas sem a autorização do proprietário.

Mas também na ocorrência de atos, como:

Interrupção ou perturbação de serviços telegráficos;

Telefônicos;

Informáticos;

Telemáticos ou de informações de utilidade pública;

Falsificação de documento particular;

Clonagem e falsificação de cartão de crédito.

Marco Civil da Internet

Criado em 23 de abril de 2014, com o objetivo de estabelecer princípios para a utilização da internet no país, determinando os direitos e deveres dos usuários e das instituições que fornecem serviços virtuais, ou seja, qualquer serviço gratuito ou pago que seja ofertado online.

Ele favorece a segurança do usuário e contribui para que o infrator assuma as consequências de seus atos.

Seu maior fundamento, segundo a legislação brasileira:

Nº 12.965 - O respeito à liberdade de expressão, bem como: o reconhecimento da escala mundial da rede; os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa, a livre concorrência e a defesa do consumidor; a finalidade social da rede.

Marco Civil da Internet

O marco civil buscou estabelecer de maneira clara e objetiva os direitos, assim como, os deveres relativos à utilização dos meios digitais, como:

- Maneiras que o usuário deve se portar;
- Maneiras como as instituições devem se portar;
- Evitar condutas inapropriadas;
- Tratar corretamente atos praticados de maneira erradas.

LGPD - Lei Geral de Proteção

A LGPD surgiu para suprir a falta de uma lei para regular a proteção e a privacidade dos dados, com o objetivo garantir as pessoas o direito à privacidade, segurança e o controle sobre seus dados pessoais.

Foi sancionada a em 14 de agosto de 2018.

Entrou em vigor em 18 de setembro de 2020.

Definida segundo a legislação brasileira:

LEI Nº 13.709 - Dispõe sobre o tratamento de dados pessoais, nos meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Explicando de uma maneira mais simples, a Lei busca impor um elevado padrão que garanta a proteção dos dados, punindo de maneiras significativas quem a descumprir.

Ela propõe gerar uma maior transparência, no intuito de estabelecer regras claras, harmônicas e únicas sobre como será realizada a coleta, o tratamento, o armazenamento e o compartilhamento dos dados pessoais.

Tratamento de Dados

O que é o Tratamento dos dados?

É toda operação realizada com os dados pessoais, desde o momento de sua coleta até a exclusão!

Operações como:

- Coleta;
- Acesso;
- Armazenamento;
- Controle;
- Distribuição;
- Utilização;
- E outros.

A quem a LGPD se aplica:

A LGPD se aplica a todos os prestadores de serviços pagos ou não, sejam eles virtuais ou físicos, que utilizem os dados pessoais dos usuários.

Exemplos de serviços:

- Aplicativos;
- Programas;
- Sites;
- Lojas;
- Jogos;

Estabelecimentos de alugueis de serviços;

Restaurantes;

Livrarias;

Hospitais;

Operadoras de Planos de Saúde;

A quem a LGPD se aplica:

TODOS OS TIPOS SERVIÇOS QUE REALIZAM A COLETA, TRATAMENTO E ARMAZENAMENTO DE DADOS PESSOAIS, APLICÁVEL TAMBÉM A EMPRESAS COM SEDE NO EXTERIOR, MAS QUE REALIZAM O TRATAMENTO DOS DADOS EM TERRITÓRIO NACIONAL.

De acordo com a lei, para fazer uso dos dados pessoais dos cidadãos, o fornecedor do serviço deve solicitar o consentimento explícito ao usuário para coleta e uso dos seus dados.

Deve ser explicado claramente e detalhadamente quais dados serão utilizados e para qual finalidade, além de oferecer opções para o usuário visualizar, corrigir e excluir esses dados.

Proibições:

A LGPD proíbe

O tratamento dos dados pessoais para a prática de discriminação ilícita ou abusiva.

Esse tipo de tratamento é caracterizado como utilizar dados e informações do usuário para incentivar decisões comerciais, políticas públicas ou atuações de órgãos públicos.

Como exemplo podemos citar, a utilização de dados de busca dos usuários para exibir ofertas de bens e serviços nas redes sociais do usuário, incentivando-o a adquiri-lo.

Punições em caso de descumprimento da LGPD

A LGPD determina severas punição para a não conformidade e violações por parte dos prestadores de serviços. Como:
Advertências;

Multas que chegam até 2% do faturamento, limitando-se a R\$ 50 milhões por infração, descumprimento, vazamento de dados pessoa;

Em casos mais severos, pode ocorrer a proibição parcial ou total do exercício de atividades que sejam relacionadas ao tratamento de dados.

Conceitos Básicos da LGPD

Dado Pessoal

Dados e informações relacionadas a uma pessoa natural identificada ou identificável.

Dados Sensíveis

São dados que podem levar a discriminação de uma pessoa, logo, recebem um tratamento diferenciado, esses dados são sobre convicções religiosas, origem racial ou étnica, opiniões políticas e vários outros que trataremos mais à frente.

Dados Anonimizados

São os dados passaram por um processo de anonimização, logo, não ser associados a nenhum indivíduo específico.

Anonimização

Processo de tratamento dos dados que utiliza técnicas e dispositivos que modificam os dados tratados, de forma que esses dados perdem a possibilidade de serem associados a alguém, logo, não podem contribuir para a identificação direta ou indireta de uma pessoa.

Conceitos Básicos da LGPD

Consentimento

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais e tem ciência de para que aquele dado será utilizado.

Titular

Pessoa natural a quem se referem os dados pessoais que são objetos de tratamento, em outras palavras, o proprietário dos dados.

Controlador

Uma pessoa natural ou jurídica, de direito público ou privado, responsável por realizar as decisões referentes ao tratamento dos dados pessoais.

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Conceitos Básicos da LGPD

Controlador

Encarregado ou DPO (Data Protection Officer)

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).

Autoridade Nacional de Proteção de Dados (ANPD)

Órgão público que será responsável por gerenciar a LGPD em todo o território nacional, logo fica a cargo da ANPD zelar pela proteção de dados, implementar e fiscalizar o cumprimento da Lei.

Princípios da LGPD

**A principal base da LGPD é o
CONSENTIMENTO!**

Para que um prestador de serviço dê início ao tratamento dos dados do titular, é necessário que o titular autorize, logo o consentimento deve ser cedido de forma explícita e inequívoca.

Os princípios que devem ser seguidos na hora de tratar dados pessoais são os seguintes:

1 - Finalidade

Deve ser informada de forma explícita e objetiva ao titular, como o tratamento será realizado e seus propósitos.

2 - Adequação

O tratamento deve ser realizado de acordo com a finalidade acordada e informada ao titular.

3 - Necessidade

O tratamento deve ser limitado ao uso de dados essenciais para alcançar a finalidade, de modo que deve ser evitado obtenção de dados desnecessários.

Princípios da LGPD

4 - Livre Acesso

Deve ser disponibilizado acesso fácil e gratuito para que as pessoas possam visualizar a forma e finalidade com que os seus dados são tratados, assim como duração do tratamento.

5 - Qualidade dos Dados

Os dados devem ser mantidos atualizados, exatos, claros e relevantes de acordo com a finalidade do tratamento.

O titular possui por direito, solicitar a correção dos dados que estejam incompletos, inexatos ou desatualizados.

Possui direito também ao acesso à informação sobre as entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados e sobre a possibilidade de não fornecer consentimento pra o uso desses dados.

6 - Transparência

As informações sobre o tratamento dos dados e seus responsáveis devem se manter claras e acessíveis ao titular.

Princípios da LGPD

7 – Segurança

Devem ser utilizadas medidas administrativas e técnicas adequadas para garantir a proteção dos dados existentes na base para tratamento, evitando que situações acidentais ou ilícitas ocorram, como destruição, invasão, perda e outros riscos que os dados correm.

8 – Prevenção

Adoção de medidas para prevenir situações de risco, que causem danos aos dados, ao titular e aos demais envolvidos.

9 – Não Descriminação

É proibida a realização de tratamento com fins discriminatórios abusivos ou ilícitos.

Portanto, não é permitido realizar exclusões de titulares de dados pessoais no momento tratamento de dados utilizando como justificativas determinadas características, como, opinião política, origem racial ou étnica, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, geolocalização, os chamados dados sensíveis.

Princípios da LGPD

10 – Responsabilização

Os agentes que tratam os dados pessoais (controlador ou operador), devem implantar e demonstrar todas as medidas eficazes e capazes de comprovar que a LGPD está sendo devidamente cumprida, assim como, comprovar a eficácia das medidas utilizadas no tratamento.

Direitos dos titulares

1 – Autoridade sobre seus Dados Pessoais

O titular possui total autonomia e autoridade sobre seus dados pessoais, portanto, possui direito à privacidade e intimidade, logo não existe nada que lhe obrigue a fornecer seus dados pessoais.

Mas ao contratar um serviço, para que exista o vínculo entre você e a empresa, a empresa exige alguns dados, esses dados devem ser fornecidos quando justificada sua finalidade.

2 – Consentimento para o tratamento de dados pessoais

Para que seus dados pessoais sejam tratados, é necessário que o prestador do serviço lhe explique para qual finalidade esses dados serão utilizados e também como será realizado o tratamento desses dados, de maneira clara.

Assim, é necessário que o titular forneça de forma explícita e inequívoca que concorda e autoriza o tratamento. Esse consentimento pode ser revogado a qualquer momento se o titular assim desejar, assim como pode solicitar que seus dados sejam excluídos da base dados.

Direitos dos titulares

3 – Direito a Informação

Esse direito é um correspondente ao princípio da Transparência, onde o titular possui o direito à informação sobre a finalidade do tratamento de seus dados fornecidos antes de realizar o consentimento.

O titular também possui o direito de ser informado caso seus dados sejam fornecidos a terceiros.

A utilização dos dados estará estritamente vinculada ao propósito informado. Caso ocorra uma mudança de finalidade ao decorrer do tratamento, é necessário que o titular seja informado e forneça um novo consentimento para o tratamento desejado.

4 – Direito ao Livre Acesso

O titular possui o direito à informação sobre o tratamento de seus dados fornecidos a qualquer momento que desejar, essas informações devem estar disponíveis de forma clara e objetiva, de maneira gratuita e de fácil acesso.

Já a empresa deve armazenar e fornecer os dados em formato acessível e de fácil consulta, pois o titular poderá solicita-los a qualquer momento ao agente responsável pelo tratamento, via eletrônica ou impressa, com um prazo máximo de 15 dias para que seja atendida sua requisição.

Direitos dos titulares

5 – Direito a segurança dos Dados Pessoais

O titular possui direito a ter seus dados seguros, logo, a empresa deve assegurar essa segurança com técnicas e procedimentos que garantam proteção dos dados contra acesso indevido por terceiros, destruição, perda, alteração, difusão ou comunicação.

No caso de qualquer incidente de segurança, o titular tem o direito de saber o que aconteceu com seus dados.

6 – Responsabilidade dos Agentes de Tratamento

Caso ocorra algum fator decorrente do tratamento de dados que cause danos ou riscos ao titular, os agentes de tratamento devem se responsabilizar por tal infração e o titular tem direito a uma indenização correspondente ao dano sofrido.

7 - Direito à revisão de decisões automatizadas

Os dados pessoais fornecidos pelo titular podem ser utilizados por algoritmos que calculam decisões de forma automatizada, com a finalidade de realizar definições do perfil pessoal, profissional, de consumo ou de crédito do titular, que podem afetar seus interesses.

Caso aconteça isso, o titular possui o direito a informações sobre os critérios e procedimentos utilizados nos processos de decisões e de solicitar a revisão dessas decisões.

Direitos dos titulares

8 - Direito à Não-Discriminação

O titular possui o direito a não ser discriminado de forma ilícita ou abusiva com base em seus dados pessoais fornecidos.

9 - Direito à Retificação, Anonimização, Eliminação ou Bloqueio dos Dados Pessoais

O titular possui o direito à retificação, ou seja, correção e alteração de dados incorretos ou incompletos.

Sempre que possível, os dados devem ser Anonimizados.

Devem ser eliminados os dados considerados desnecessários ou excessivos, ou seja, aqueles que não atendem às finalidades informadas para o tratamento.

O titular possui o direito a solicitar sua eliminação dos dados caso eles não sejam de manutenção obrigatória por exigência legal.

10 - Direito à Portabilidade dos Dados

O titular possui o direito de poder levar seus dados para outro fornecedor de serviço ou produto quando desejar, contanto que a transferência dos dados não cause violação de segredos comerciais e industriais.

Para isso, o titular deverá realizar uma requisição expressa e clara, de acordo com a regulamentação da ANPD.

Dados Sensíveis

Os dados considerados sensíveis entre o conjunto de dados pessoais, são os que se encaixam com princípio da Não-Discriminação, que protege os usuários de serem discriminados garantindo sua liberdade de opinião e expressão.

Assim como que seus dados sejam utilizados de formas ilícitas ou ilegais, podendo causar algum dano ao titular, logo esses dados, devem ser tratados com uma atenção extra.

O consentimento deve ser solicitado de forma mais destacada e direta, do que quando se trata os dados pessoais considerados normais e deve ser informada a finalidade de forma explícita.

Tipos de dados que são considerados sensíveis:

Origem racial ou étnica;

Opinião política;

Convicção religiosa;

Dado genético ou biométrico, quando vinculado a uma pessoa natural;

Filiação a sindicato ou a organização de caráter: religioso, filosófico ou político;

Dado referente à saúde;

Dado referente à vida sexual.

Exceções

O tratamento de dados sensíveis poderá ser realizado sem o consentimento do titular nas seguintes situações:

- Cumprimento de obrigação legal ou regulatória pelo controlador sem surpresas;
- Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas que estejam previstas em leis ou regulamentos;
- Auxiliar na realização de estudos por órgão de pesquisa, que devem garantir, sempre que for possível, a anonimização dos dados pessoais sensíveis utilizados e esses dados não podem ser divulgados de maneira que o titular seja identificado;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Para garantir a proteção da vida ou da integridade física de uma pessoa, seja ele titular do dado ou não;
- Tutela da saúde, em procedimentos realizados por profissionais da área da saúde ou por entidades sanitárias;
- Garantia da prevenção à fraude e à segurança do titular.

Exposição e transferência de dados pessoais

- Não é permitido em qualquer hipótese a revelação dos dados pessoais na divulgação dos resultados de pesquisas ou qualquer parte do estudo. Não há exceções. Isso significa que se os dados pessoais de pesquisas e estudos da área de saúde pública forem revelados, estamos diante de um ilícito.
- Em qualquer hipótese, a transferência de dados a terceiros. A responsabilidade dos dados pessoais é do órgão de pesquisa ou estudos, que responderá civil e penalmente pelo uso indevido deles. Os dados corretamente anonimizados não serão mais considerados dados pessoais.
- Os dados pessoais em pesquisas de saúde será objeto de regulamentação pela ANPD e pelos órgãos de saúde e sanitários, cada qual na sua esfera de competência administrativa. Dependendo de uma regulamentação complementar a ser feita no futuro.

Referências

BARRETO FILHO, Marcelo Vandré Ribeiro. Os Contornos Jurídicos da Lei Geral de Proteção de Dados Frente ao Consumo no Ambiente Virtual. 2019.

Cartilha de Segurança para Internet – Disponível em: <<https://cartilha.cert.br/>>.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.

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

Lei nº 12.737, de 30 de novembro de 2012. Lei Carolina Dieckmann. Brasilia, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasilia, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

Lei nº12.965 de 23 de abril de 2014. Marco Civil da Internet. Brasilia, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

NUCCI, Guilherme de Souza. Manual de direito penal. 9.ed. São Paulo: Revista dos Tribunais, 2013.

OAB - Comissão Especial de Proteção de Dados. Lei Geral de Proteção de Dados: uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Minas Gerais, 2018.

SETZER, Valdemar W. Dado, informação, conhecimento e competência. DataGramZero Revista de Ciência da Informação, n. 0, p. 28, 1999.

