PROTEÇÃO DE DADOS

Jéssica Tainah da Silva Botelho | Guilherme Forma Klafke

Stephane Hilda Barbosa Lima | Tatiane Guimarães

nic.br FGV

REVISÃO TÉCNICA

Victor Doering Xavier da Silveira

Mestre em Filosofia e Teoria Geral do Direito pela Faculdade de Direito da Universidade de São Paulo (FDUSP) e bacharel em Direito pela mesma instituição. Atua como pesquisador no Centro de Ensino e Pesquisa em Inovação da FGV Direito SP.

nic.br FGV

SUMÁRIO

APRESENTAÇÃO DO CURSO

Você lembra onde estava ou o que andou curtindo nas redes sociais, nesta mesma data, há dois anos? E que tal lembrar o último medicamento que você comprou na farmácia? Atualmente, estamos produzindo dados o tempo todo. Dados são um retrato de quem somos – um retrato elaborado a partir dos rastros que deixamos ao utilizarmos tecnologias no nosso cotidiano.

Decisões são tomadas a partir de dados: seja o conteúdo que veremos na internet, seja o desconto que teremos na farmácia. Dessa forma, eles podem influenciar o modo como as pessoas nos enxergam e interagem conosco, a maneira como as empresas oferecem serviços e produtos, e até que tipo de interesses os governos podem ter em cada um de nós. Justamente por isso, devemos proteger nossos dados.

Mas não se desespere! Estamos aqui para aprender o que são dados, que tipos de dado existem, quais são as finalidades do uso e da coleta de dados e, finalmente, de que modo podemos garantir a proteção dos nossos dados, considerando não só a legislação brasileira mas também as configurações dos dispositivos eletrônicos.

Ao final deste curso, esperamos que você, educador, tenha conhecimento suficiente para abordar o tema em sala de aula e para desenvolver práticas educativas que levem os alunos a compreenderem a sua importância e fazer da proteção de dados uma prática cotidiana. Além disso, caso necessário, esperamos que você desenvolva condições de orientar os seus educandos sobre possíveis riscos e danos.

OBJETIVOS

OBJETIVO GERAL

Compreender a importância da proteção de dados e, dessa forma, capacitar-se para pautar o tema na sua escola tanto como debate quanto como prática, compreendendo, para isso, os diferentes tipos de dados os processos de coleta e tratamento, bem como os interesses existentes em cada finalidade de uso de dados pessoais.

OBJETIVOS ESPECÍFICOS

- apresentar conceitos básicos sobre proteção de dados;
- entender que dados pessoais vulneráveis podem ser acessados por outras pessoas;
- compreender as diferentes situações em que ocorrem a coleta e o tratamento de dados, bem como os seus objetivos e
- configurar dispositivos e contas para aumentar o nível de privacidade e proteção de dados.

AUTORES DA APOSTILA

Jéssica Tainah da Silva Botelho
Mestre em Ciências da Comunicação pela Universidade Federal do Amazonas e graduada em Comunicação Social – Jornalismo pela Universidade Federal do Amazonas. Atua como colaboradora no Centro Popular do Audiovisual/Núcleo de Estudos e Práticas em Cibercultura.

Guilherme Forma Klafke

Doutorando (2019) e mestre (2015) em Direito Constitucional pela Universidade de São Paulo e bacharel (2011) em Direito pela Universidade de São Paulo. Atua como colaborador na Sociedade Brasileira de Direito Público desde 2011, onde coordenou a Escola de Formação Pública (2017), e também como líder de projetos e pesquisador no Centro de Ensino e Pesquisa em Inovação da FGV Direito SP. Foi professor de Filosofia do Direito na Faculdade de Direito de São Bernardo do Campo (2017-2018). Atualmente, coordena e desenvolve pesquisas nas áreas de Direito Constitucional, Jurisdição Constitucional, Ensino Jurídico, Ensino Participativo, Direitos Humanos Digitais e Filosofia do Direito.

Stephane Hilda Barbosa Lima

Doutoranda (2019) em Teoria do Estado pela Universidade de São Paulo, mestre (2018) em Direito Constitucional pela Universidade Federal do Ceará, especialista (2016) em Direito Tributário e Processo Tributário pela Escola Jurídica Juris e graduada (2014) em Direito pela Universidade Federal do Ceará. Atua como pesquisadora no Centro de Ensino e Pesquisa em Inovação da FGV Direito SP. Atualmente, desenvolve pesquisas e atividades de ensino nas áreas de Ensino Jurídico, Metodologias Participativas, Direitos Humanos Digitais, Direito Educacional, Educação Digital e Regulação.

Tatiane Guimarães

Graduada (2019) em Direito pela Pontifícia Universidade Católica de São Paulo e atua como pesquisadora no Centro de Ensino e Pesquisa em Inovação da FGV Direito SP.

ESTRUTURA DO CURSO

Neste curso, vamos abordar o conteúdo relativo à proteção de dados por meio da seguinte estrutura:

- **Unidade 1: Os seus dados são você**
  Na unidade 1, compreenderemos o conceito de "dados" e analisaremos as diferenças entre dados pessoais, dados sensíveis, dados tratados e dados brutos. Também entenderemos como os dados são coletados e utilizados no nosso dia a dia sem percebemos.

- **Unidade 2: Proteção de dados para quê?**
  Na unidade 2, compreenderemos a importância da proteção de dados. Para tanto, analisaremos os conceitos de privacidade e segurança e, em seguida, trabalharemos o tema da regulação sobre compartilhamento, coleta e tratamento de dados existente na legislação brasileira. Por fim, indicaremos algumas medidas simples que podem aumentar o nosso controle quanto ao acesso e uso dos nossos dados em dispositivos tecnológicos e plataformas *on-line*.

BIBLIOGRAFIA COMENTADA

ALECRIM, Emerson. Análise preditiva: o que é e como as empresas a usam para tomar decisões. *Tecnoblog*, 2018. Disponível em: https://tecnoblog.net/248611/analise-preditiva-o-que-e-definicao/. Acesso em: 6 jan. 2020.

Neste artigo, Alecrim explica a evolução do conceito de análise preditiva, bem como a utilização e as aplicações desse tipo de lógica matemática.

CENTRO DE PESQUISA INTERNETLAB; ELETRONIC FRONTIER FOUNDATION. *Quem defende seus dados?* São Paulo, 2018. Disponível em: http://quemdefendeseusdados.org.br/pt/. Acesso em: 6 jan. 2020.

Nesta pesquisa, são discutidas as políticas de privacidade e proteção de dados das empresas provedoras de conexão à internet no Brasil. O objetivo é chamar a atenção para adoção de boas práticas, promover a transparência e advertir usuários quanto aos usos que representam riscos e danos à sua privacidade e aos seus dados pessoais.

LEMOS, Ronaldo. Lei de dados deve evitar jabuticabas. *Instituto de Tecnologia e Sociedade*, 19 fev. 2019. Disponível em: https://itsrio.org/pt/comunicados/lei-de-dados-deve-evitar-jabuticabas/. Acesso em: 6 jan. 2020.

Nesta nota, Lemos comenta o processo que antecedeu a criação da Lei Geral de Proteção de Dados (GPDR), a legislação brasileira que regulamenta direitos e deveres em relação à coleta de dados no Brasil, com o intuito de proteger a privacidade dos usuários. Aponta ainda impactos da sua implementação no cenário político internacional, tomando como base a aproximação entre a GPDR e a lei europeia que trata do mesmo assunto.

PARISER, Eli. *O filtro invisível:* o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

Nesta recente obra, Pariser explica como filtros invisíveis colocam-nos em bolhas de navegação na internet, alertando para os riscos e danos de vivermos nesses universos particulares que confirmam nossos gostos e preferências. Em seguida, o autor indica o que pode ser feito, nos níveis pessoal e institucional, para que tenhamos uma internet mais diversa e democrática.

VARON, Joana; TEIXEIRA, Lucas. Podemos vigiar os vigilantes? *Medium*, 25 maio 2018. Disponível em: https://medium.com/codingrights/podemos-vigiar-os-vigilantes-ac3fe77e7694. Acesso em: 6 jan. 2020.

Neste artigo, os autores discorrem sobre escândalos envolvendo grandes plataformas de mídias sociais e a exploração de dados pessoais. Alertam ainda para modelos de negócio de empresas de tecnologia cuja essência é o monitoramento intenso do nosso comportamento.

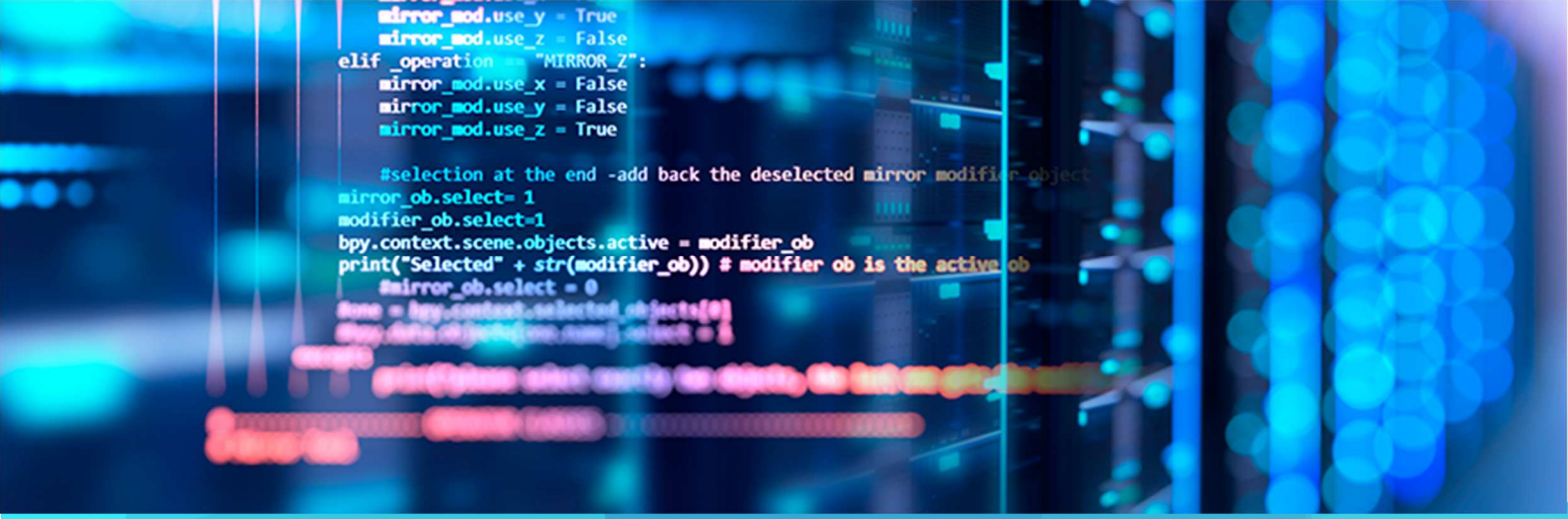
INICIANDO O ESTUDO

Para entendermos o que são dados e como nos influenciam no nosso dia a dia, tenhamos em mente três situações:

I) **Dados no transporte público** – No Rio de Janeiro, para que você possa ter direito ao uso do Riocard (o Bilhete Único carioca) é necessário cadastrar o seu nome, CPF e data de nascimento. Se você usa vale-transporte, então terá de informar a sua profissão, o seu local de trabalho e o número da sua carteira profissional. Caso seja um estudante de Ensino Médio, o sistema terá acesso ao seu nível de escolaridade e à instituição de ensino em que você estuda. Já o Passe Livre Universitário, criado para estudantes de baixa renda da rede pública, exige o cadastro de informações sobre quem compõe e qual é a renda da sua família, e precisa ser atualizado constantemente, para comprovar a necessidade do benefício e garantir o seu uso. Em um dia como qualquer outro, veja só quantas informações sobre você já foram compartilhadas!

II) **Descobri que minha filha estava grávida antes de ela me contar** – Em um famoso caso nos Estados Unidos, um pai descobriu, acidentalmente, a gravidez da filha adolescente por meio de produtos que uma empresa da rede varejista norte-americana enviou à residência da família. Surpreso e revoltado com a situação, o pai se sentiu ofendido pela oferta de produtos para gestantes a uma menina que ainda estava cursando o Ensino Médio. Será que a loja errou o endereço?

III) **Controle escolar por meio de aplicativo** – A escola em que você trabalha passou a organizar as informações de cada aluno em um aplicativo, que pode ser acessado e alimentado com novos dados pela direção, pelos professores e pelos pais. O aplicativo conta também com um espaço de conteúdo educativo para os alunos. Nele constam desde o histórico escolar (boletins, desempenho em cada disciplina) até o comportamento do estudante (questões de saúde e de relacionamento na escola). O que você acha de empresas e universidades terem acesso a esses dados?



UNIDADE I – OS SEUS DADOS SÃO VOCÊ

Mas, afinal, o que são dados? Todos os dias, cedemos dados pessoais para utilizar serviços, usar aplicativos, acessar redes sociais ou até para obter acesso temporário à internet. Tudo isso pode parecer "de graça", mas, na verdade, trocamos essas facilidades pelo acesso a nossas informações.

Figura 1 – Dados digitais

Fonte: Shutterstock

O que é dado?

Um dado é um registro, uma informação, é um rastro que permite obter uma conclusão a respeito de alguém. Sozinho um dado pode não dizer muito, mas, quando interpretado em conjunto com outros dados, pode permitir que alguém que não o conhece deduza os seus hábitos, as suas predileções e as suas características pessoais.

Um grande volume de dados permite a construção de um retrato de quem você é. Sendo assim, não há exagero em afirmar: os seus dados são você.

A diferença entre os tipos de dado está relacionada à informação que cada um deles pode carregar e ao que pode ser feito com cada um deles. De acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD, 2018), existem os seguintes tipos de dado:

a) Dado pessoal:

Dado pessoais são aqueles relacionados à pessoa física identificada ou identificável, e podem incluir números identificativos (como o número do CPF), dados de localização ou identificadores eletrônicos, quando esses estiverem relacionados a uma pessoa.

Ainda que um dado não se refira, claramente, a uma pessoa específica (pessoa identificada), o simples fato de permitir a identificação dessa pessoa quando colocado em conjunto com outros dados (pessoa identificável) faz dele um dado pessoal. Por essa razão, são dados pessoais não só informações muito específicas sobre alguém (nome, RG, CPF, título de eleitor, nome dos pais, conta bancária, etc.) mas também quaisquer informações que façam referência indireta à pessoa (localização, registros de uso de cartão de crédito, trajeto que a pessoa faz de casa até o trabalho, etc.).

b) Dado pessoal sensível:

Dados pessoais sensíveis são dados sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, e dados genéticos ou biométricos.

Esse é um tipo de dado pessoal capaz de ser usado de forma discriminatória, o que torna o seu uso indevido mais perigoso, por ser mais capaz de gerar dano à pessoa.

c) Dado tratado:

Um dado tratado é aquele que foi submetido a procedimentos técnicos ou metodológicos para determinado fim. Por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

d) Dado bruto:

O dado bruto é aquele registrado em qualquer base e que não passou por outros procedimentos de tratamento além desse registro.

Dados são gerados e coletados de diversas formas, tais como:

- cliques que você dá enquanto navega na internet;
- cadastros que você preenche para utilizar um serviço;
- pesquisas a que você responde e
- testes que você faz na internet para descobrir qual é o seu par ideal, de acordo com o seu signo.

Quando você cede informações a seu respeito, você está compartilhando os seus dados pessoais. Quando você baixa aplicativos e permite que eles acessem, por exemplo, a câmera e o microfone do seu celular, você também está abrindo caminho para que os seus dados pessoais sejam coletados. Em outras palavras, o compartilhamento de dados e o uso da internet estão profundamente ligados.

No quadro a seguir, explicamos as etapas de compartilhamento, coleta e tratamento de dados para que você entenda as circunstâncias de cada uma.

Quadro 1 – Etapas de compartilhamento, coleta e tratamento de dados.

	COMPARTILHAMENTO	COLETA	TRATAMENTO
PROCESSOS	Diferentes processos permitem o compartilhamento de informações sobre cada pessoa.	Processos pelos quais um agente (pessoa física ou jurídica) adquire acesso a dados pessoais.	Processos que compreendem ações de coleta, armazenamento, análise, classificação, utilização de dados, etc.
FINALIDADES E OBJETIVOS	Geralmente, têm finalidade definida, mas nem sempre têm objetivos (ou condições) evidentes.	Geralmente, têm finalidade definida, mas nem sempre têm objetivos (ou condições) evidentes.	Têm finalidade definida, bem como objetivos e metodologia específicos.
AGENTES	O compartilhamento depende de cada pessoa (por exemplo, você ou o seu aluno) e pode ser realizado direta ou indiretamente.	Pode ser realizada por outros agentes que não os titulares dos dados, geralmente por meio de dispositivos tecnológicos (celulares, computadores, *tablets*, etc.).	Pode ser realizado por outros agentes que não os titulares dos dados, incluindo tecnologias.

Finalidades da coleta e do tratamento de dados

Atualmente, diversos serviços e setores da economia são baseados no tratamento de grandes conjuntos dados (*big data*). Esse fenômeno é mais visível na forma pela qual redes sociais, aplicativos de serviços e empresas da chamada Economia de Compartilhamento garantem lucros para os seus modelos de negócio. Por meio do tratamento dados de usuários, essa economia é capaz de oferecer publicidade direcionada e segmentada para determinados públicos e indivíduos específicos, gerar perfis de consumo e até influenciar grandes debates públicos.

Dados podem ser usados para inúmeros fins. Vejamos:

a) Pesquisa ou prospecção:

Na situação hipotética **Dados no transporte público**, em que tratamos da coleta de dados pessoais para uso do transporte público, o Estado poderia disponibilizar os dados dos usuários para pesquisadores e engenheiros de tráfego entenderem como as pessoas se deslocam pela cidade e, dessa forma, buscar soluções ou propor políticas públicas que resolvam problemas de transporte locais.

Nesse caso, dados são fundamentais para subsidiar pesquisas e alcançar avanços científicos, bem como possibilitar a elaboração de políticas públicas que solucionem problemas específicos.

b) Serviços:

Você se lembra da situação hipotética **Descobri que minha filha estava grávida antes de ela me contar**, em que o pai de uma garota ficou ofendido porque uma loja enviou uma caixa de produtos para gestantes? Então, era verdade: a adolescente realmente estava grávida. Mas como a loja sabia disso?

Isso só foi possível porque a loja possuía um sistema preditivo para oferecer produtos aos seus clientes. Esse sistema cria um perfil de cada consumidor a partir da análise do seu histórico de compras e dos seus dados demográficos, somando-os a informações fornecidas, espontaneamente, pelos clientes em campanhas de marketing e descontos. Ao enviar uma caixa de produtos de gestante ao endereço da adolescente, o objetivo da loja era iniciar um novo tipo de serviço de compras, no qual a loja oferece produtos que imagina ser do seu interesse.

Atualmente, há uma gama infinita de serviços facilitados e oferecidos pela internet que coletam dados. Isso pode, inclusive, significar uma melhora na prestação de serviços: no caso **Controle escolar por meio de aplicativo**, é possível que situações que, anteriormente, passariam despercebidas no processo de aprendizagem do estudante venham a receber mais atenção. Nesse caso, a escola pode passar a oferecer outros meios de ensino e cuidado, para além da sala de aula.

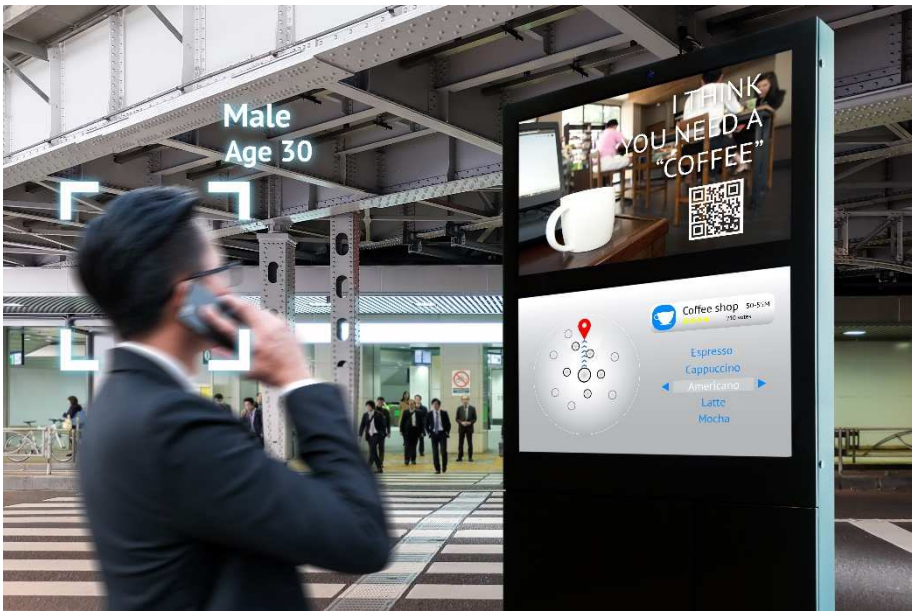
c) Experiência:

Quando navegamos na internet, deixamos rastros sobre tudo o que fazemos. Esses rastros são dados que possibilitam a reconstrução dos nossos hábitos e interesses, os quais sofrem variações de pessoa para pessoa. Na situação hipotética **Controle escolar por meio de aplicativo**, por exemplo, cada aluno terá acesso a um tipo de conteúdo que está ligado às informações do seu perfil na plataforma. Se um estudante está apresentando dificuldade em Matemática, o sistema tenderá a enviar-lhe mais dicas, exercícios e aulas sobre essa matéria.

d) Seleção:

Os dados também podem ser usados como ferramenta para selecionar pessoas em algumas situações. Tanto empresas quanto instituições governamentais utilizam informações sobre as pessoas a partir do tratamento dos seus dados.

Uma empresa de RH pode, por exemplo, acessar os seus dados para traçar seu perfil e verificar se você é um candidato que atende aos critérios de contratação. No caso dos estudantes da situação hipotética **Controle escolar por meio de aplicativo**, é possível que uma instituição de ensino superior decida aprovar ou reprovar um vestibulando com base nos dados do seu histórico escolar.



Resumidamente, um dado é qualquer informação relacionada a uma pessoa que venha a permitir a sua identificação, seja sozinho, seja em conjunto com outros dados. O uso de dados pessoais desperta, portanto, interesses e, por isso, requer proteção jurídica, tema da nossa próxima unidade.

UNIDADE II – PROTEÇÃO DE DADOS PARA QUÊ?

Privacidade e segurança

Suponha que você seja o pai da adolescente na situação hipotética **Descobri que minha filha estava grávida antes de ela me contar**. Depois que descobriu a situação da sua filha, você percebeu que aparecem propagandas de itens para bebês em todos os *site* que visita. Mas, se você não chegou a publicar nada em redes sociais, como isso é possível?

Quando uma loja realiza a coleta e o tratamento dos seus dados sem o seu consentimento, nada impede que ela também compartilhe esses dados com outras empresas que tenham o interesse de ter você como cliente ou com outros agentes que possam ter outros usos e finalidades para os seus dados.

Importante!

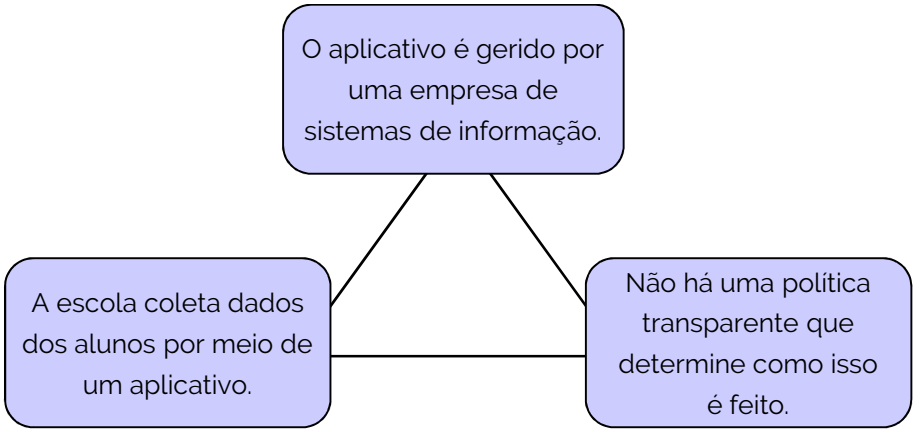
Gestores de bancos de dados de cadastro negativo, como Serasa, SPC e Boa Vista, nem precisam do seu consentimento para obter os seus dados (conforme o artigo 7º da LGPD, 2018). Sendo assim, podemos afirmar que existem fins econômicos e riscos associados ao uso dos seus dados que vão além de fazer publicidades direcionadas e, embora não precisemos falar sobre todos eles aqui, é bom entender que esse não é o único risco relevante ou possível.

Autodeterminação informativa e regulamentos dispostos em lei

A compreensão sobre a importância da proteção de dados é necessária para saber lidar com situações como essa. Dessa forma, você poderá questionar a finalidade do uso e autorizar (ou não) a coleta e o tratamento dos seus dados.

Saber que dados pessoais são informações que permitem a descoberta de fatos sobre os seus hábitos e preferências, bem como passar a ter mais controle sobre quem tem acesso e o que faz com seus dados, sentindo-se assim mais seguro, é um direito reconhecido e protegido pelo artigo 2º, inciso II, da Lei Geral de Proteção de Dados Pessoais. Esse direito é chamado de autodeterminação informativa.

Agora, voltemos à situação hipotética **Controle escolar por meio de aplicativo**, na qual a escola resolve utilizar um sistema de gestão e educação baseado em dados sobre os estudantes. Nesse caso, temos o seguinte cenário:



Existe uma diferença entre aquilo que você escolhe compartilhar, ciente dos riscos e danos possíveis, e aquilo que é coletado sem a sua autorização. Nesse caso, os questionamentos que surgem são os seguintes:

- Quem controla o uso desses dados?
- O que pode ser feito com eles?
- No caso de crianças e adolescentes, é certo coletar dados sem que os seus pais ou responsáveis sejam informados sobre os detalhes desse processo?

Temos, portanto, um problema de privacidade e proteção de dados. É um problema porque são dados pessoais e dados pessoais sensíveis sobre os alunos que poderão ser coletados e tratados por terceiros sem que haja transparência sobre os processos envolvidos, o que pode prejudicar a capacidade de a escola (e os pais) lidar com a situação.

Um caminho para implementar ferramentas digitais educacionais ao cotidiano da escola é entender os direitos e deveres de cada um nesse cenário. O Brasil dispõe de leis e regulamentos que tratam, especificamente, de questões relacionadas aos dados pessoais de crianças e adolescentes.

O Estatuto da Criança e do Adolescente (ECA), por exemplo, é um marco legal significativo para proteção, em geral, de pessoas em desenvolvimento. O ECA regulamenta questões de controle dos pais e responsáveis em relação ao acesso a tecnologias de informação, bem como a aplicação de medidas para defesa da privacidade de crianças e adolescentes.

Já o artigo 14 da Lei Geral de Proteção de Dados Pessoais estabelece que o tratamento de dados de crianças e adolescentes deve ser:

- realizado no seu melhor interesse e nos termos da legislação;
- realizado com o consentimento específico e em destaque fornecido pelo responsável e
- feito com transparência, inclusive quanto a informações sobre os tipos de dado coletados, à forma da sua utilização e aos procedimentos para o exercício dos direitos dos usuários.

Proteger o uso e a coleta de dados de crianças e adolescentes significa protegê-los de situações a que eles não possuem amadurecimento e conhecimento suficiente para responder sozinhos e, dessa forma, também minimizar os riscos da sua exposição.

Importante!

Devemos observar que as recomendações dadas não significam que crianças e adolescentes devam ser proibidos de usar qualquer tipo de nova tecnologia.

É essencial construir um diálogo pautado pela empatia para compreender os seus usos e demandas e, a partir disso, orientá-los sobre como lidar com questões de privacidade e segurança. Uma educação orientada para o uso seguro e responsável é sempre o melhor caminho a ser tomado quando falamos de juventude e internet.

Direitos do titular: exercícios e garantias

Titular é o "dono" dos dados coletados. Segundo a LGPD (2018), titular é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento."

As regras sobre privacidade e proteção de dados estão mudando aos poucos, em conjunto com o debate sobre o uso das tecnologias de informação e comunicação. A situação hipotética **Dados no transporte público** ocorreu antes da aprovação da LGPD, legislação que regulamenta, especificamente, os direitos de pessoas físicas sobre os seus dados pessoais, garantindo mecanismos de proteção para usuários de serviços digitais e dispositivos eletrônicos.

Para que usufrua o seu direito à privacidade e à proteção de dados pessoais, você precisa entender em que momento pode autorizar ou desautorizar a coleta dos seus dados, quais são as possibilidades de coleta sem autorização e quais são os fundamentos que estruturam a legislação.

As regulamentações legais existem para nos proteger do uso indevido dos nossos dados pessoais e para que possamos ter mais controle sobre o que acontece com eles: como são armazenados, com quem são compartilhados e com que finalidade.

Antes que leis mais específicas surgissem, o Direito brasileiro protegia a privacidade e garantia a proteção de dados pessoais por meio de dois instrumentos fundamentais. Vejamos:

a) Código Civil:

O Código Civil (2002) estipula que a intimidade, a vida privada, a honra e a imagem de cada pessoa são invioláveis, cabendo indenização a quem sofrer violação desses direitos. Essa disposição, que trata da proteção dos direitos da personalidade, era aplicável para proteger a privacidade em casos de coleta e tratamento de dados pessoais.

b) Código de Defesa do Consumidor:

Por garantir a proteção aos direitos de pessoas em relações de consumo, o Código de Defesa do Consumidor (1990) também era aplicado à proteção de usuários de serviços digitais, garantindo-lhes, por exemplo, o direito à informação e à transparência sobre a qualidade, o preço e os riscos do serviço em si.

Com a evolução do uso de tecnologias digitais e, consequentemente, o aumento do uso de dados pessoais sem o devido controle, dentre outros fatores, o Brasil observou a necessidade de criar legislações específicas. Vejamos:

a) Marco Civil da Internet:

A primeira legislação brasileira pensada e construída para regular temas digitais de forma mais clara e específica foi o Marco Civil da Internet (MCI), aprovado em 2014. O projeto de lei foi construído coletivamente por representantes do governo, do setor privado, da academia e da sociedade civil, e define os direitos e responsabilidades dos usuários e provedores de serviços.

O Marco Civil está estruturado em 10 princípios que tratam a internet como um espaço que deve garantir liberdade de expressão e transmissão de conhecimento. De modo geral, o MCI introduziu na legislação brasileira a preocupação com a proteção de dados pessoais e algumas regras preliminares, como transparência e a exigência de consentimento livre, expresso e informado para o fornecimento de dados pessoais a terceiros, salvo hipóteses legais. Além disso, estabeleceu que é necessário que os usuários recebam informações claras e completas sobre a coleta, o uso, o armazenamento, o tratamento e a proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades elencadas pela legislação.

b) Lei Geral de Proteção de Dados Pessoais:

Em 2018, o Brasil aprovou a Lei Geral de Proteção de Dados Pessoais, que entra em vigor em 2020. O principal objetivo de criar uma legislação exclusiva para proteção de dados foi buscar garantir a privacidade dos nossos dados pessoais e permitir que tenhamos um maior controle sobre eles por meio da criação de regras para processos de coleta, tratamento e compartilhamento de informações. Desse forma podemos, em geral, consentir ou negar consentimento à sujeição dos nossos dados pessoais a determinados processos ou, até mesmo, solicitar a sua exclusão.

Importante!

Advogados e instituições como Ministério Público, Procon e Defensorias Públicas podem defender você em caso de violação do uso dos seus dados pessoais, com base na Lei Geral de Proteção de Dados Pessoais, no Marco Civil da Internet e no Código de Defesa do Consumidor. Além disso, a LGPD prevê a criação de uma Autoridade Nacional de Proteção de Dados, encarregada de realizar essa proteção e responsabilizar agentes pelo tratamento indevido de dados pessoais.

Um ponto muito importante da LGPD refere-se ao fato de que ela se aplica a todos os setores da economia. Sendo assim, toda empresa que tiver negócios no País deve adequar-se a essa lei – ainda que sua origem seja estrangeira, como ocorre com o Google e o Facebook.

Até aqui, já entendemos que a coleta e o armazenamento de dados pessoais pelas tecnologias pode ter diversas finalidades. No entanto, o intenso uso que se faz desses dados provocou um ambiente de monitoramento cujo controle não foi pensado pelos usuários (titulares de dados).

A segurança digital é necessária para proteger os usuários, garantir a sua privacidade e estabelecer relações de confiança entre tais usuários e as organizações estatais, comerciais e científicas, como a relação existente entre você – enquanto educador –, a escola em que trabalha, os seus alunos e os pais deles.

Mão na massa

Já vimos que existem mecanismos jurídicos a que você pode recorrer para assegurar que os seus dados sejam tratados e utilizados de acordo com o seu consentimento. Vimos também que os operadores do Direito podem defendê-lo em caso de violação da sua privacidade. Esses são fatores essenciais para que você compreenda como agir ao buscar proteger dados pessoais.

Agora, vamos tratar da necessidade de rever como os seus dados estão sendo coletados nos dispositivos e serviços digitais (redes sociais, *sites*, aplicativos) que você acessa. Vamos lá?

Para criar uma conta em redes sociais, baixar aplicativos ou acessar *sites*, você precisa, antes de tudo, de um celular, computador, *tablet* ou similar que tenha conexão com a internet. A forma

mais prática e direta de proteger os seus dados pessoais na internet e aumentar a sua segurança é entender as configurações gerais (aquelas que definem como a plataforma funciona) e, em seguida, as configurações de privacidade e segurança. As configurações de privacidade e segurança são justamente aquelas que nos interessam quando falamos em segurança digital – ou cibersegurança.

Lembrete

Toda vez que cria uma conta em redes sociais, aplicativos ou sites, você está cedendo e gerando dados tanto pelas informações que preenche quando realiza o cadastro quanto por meio da sua interação com outros usuários.

No momento em que você cria uma conta em um site ou baixa um aplicativo, esses serviços lhe informam que, para usufruir todos os benefícios e facilidades, você precisa conceder permissão a recursos e funções do dispositivo que está usando: câmera, agenda telefônica, localização (GPS), etc. Sendo assim, é necessário refletir sobre que tipo de consentimento você dará a cada aplicativo ou site pelo qual navega.

Importante!

Cada plataforma possui um documento (ou mais) que regulamenta o seu funcionamento. Conhecer os termos de uso e as políticas de privacidade é, portanto, fundamental para que você, como usuário, saiba exatamente o que a plataforma vai acessar no seu dispositivo ao oferecer um serviço ou experiência, e com que finalidade. Esses documentos estipulam, por exemplo, a idade mínima para utilizar a plataforma, que, geralmente, é de 13 anos.

Para saber mais sobre esse assunto, acesse o curso *Termos de uso e políticas de privacidade.*

Guias de segurança digital e proteção de privacidade

Se você ficou curioso para saber o que permite ou não nas configurações dos seus dispositivos, das suas redes sociais e dos demais sites que acessa, leia os dois guias rápidos a seguir. Eles foram elaborados para que você reveja os seus padrões de segurança digital e proteja a sua privacidade.

a) Passo a passo para aparelhos:
   1. encontre as configurações do dispositivo que você usa;
   2. percorra a lista de opções até encontrar um item relacionado a “aplicativos” ou “apps”;
   3. escolha um aplicativo e leia todas as informações sobre ele;
   4. identifique o tópico sobre “permissões”;
   5. analise a lista de funções do seu aparelho que o aplicativo pode acessar;
   6. pondere sobre cada permissão concedida e a real necessidade de concedê-la e
   7. ative ou desative cada uma das permissões que achar necessário.

Importante!

É importante lembrar que algumas permissões são essenciais para o funcionamento dos aplicativos. Para utilizar o Uber, por exemplo, o aplicativo precisa acessar o GPS do seu aparelho. No entanto, alguns aplicativos podem solicitar acesso a dados desnecessários. Fique atento!

b) Passo a passo para redes sociais (Facebook, Instagram, Whatsapp, etc.):
   1. entre na conta da rede social cujas questões de privacidade e segurança você pretende rever – aquele momento em que você digita o usuário e a senha;
   2. busque as configurações gerais da plataforma. Geralmente, elas ficam em um dos cantos superiores, onde tem a sua foto em miniatura;
   3. invista algum tempo explorando as configurações gerais, pois é importante saber como cada plataforma funciona;
   4. identifique algo como "privacidade" ou "configurações de segurança" – esses termos costumam estar em destaque;
   5. analise o que a rede social mostra de ações e funções que podem ser alteradas. Por exemplo: quem pode ver cada informação sua, quem pode ver as suas publicações, etc. e
   6. verifique o que é oferecido como mecanismo de segurança e opte por funções que aumentem a sua segurança na plataforma, como enviar um SMS para o seu celular em caso de movimentação estranha na sua conta.

O que pode ser feito na escola?

O caminho para combater a coleta e o uso indevido de dados envolve uma gestão (junto a toda comunidade escolar) preocupada em proteger os dados pessoais dos seus alunos e, principalmente, ciente da necessidade de conhecer os direitos e deveres referentes ao tema.

Nesse sentido, são bem-vindas ações que:

- conscientizem a comunidade escolar acerca da importância da proteção de dados;
- levem à elaboração de uma política institucional sobre a coleta e o tratamento de dados;
- aproximem pais e responsáveis da discussão sobre o tema;
- orientem os alunos quanto aos danos e riscos envolvidos no compartilhamento de dados na internet.

RECAPITULANDO

A coleta e o tratamento de dados pessoais é fundamental para o funcionamento das tecnologias que utilizamos no nosso cotidiano. No entanto, apesar dos benefícios e facilidades que essas tecnologias possam oferecer, é importante sabermos como informações sobre quem somos, o que gostamos e o que fazemos são acessadas e usadas, de forma que as possamos proteger.

Sendo assim, dialogar sobre privacidade, conhecer direitos e deveres, bem como entender como funcionam os processos de coleta e tratamento de dados é fundamental não só para que saibamos como e quando nos proteger, mas também para que possamos oferecer esse conhecimento àqueles que não compreendem os riscos e danos possíveis.

Fonte: Shutterstock

BIBLIOGRAFIA

ALECRIM, Emerson. Análise preditiva: o que é e como as empresas a usam para tomar decisões. *Tecnoblog*, 2018. Disponível em: https://tecnoblog.net/248611/analise-preditiva-o-que-e-definicao/. Acesso em: 6 jan. 2020.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, DF, 23 abr. 2014.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *Diário Oficial da União*¸ Brasília, DF, 8 jul. 2019.

CENTRO DE PESQUISA INTERNETLAB; ELETRONIC FRONTIER FOUNDATION. *Quem defende seus dados?* São Paulo, 2018. Disponível em: http://quemdefendeseusdados.org.br/pt/. Acesso em: 6 jan. 2020.

LEMOS, Ronaldo. Lei de dados deve evitar jabuticabas. *Instituto de Tecnologia e Sociedade*, 19 fev. 2019. Disponível em: https://itsrio.org/pt/comunicados/lei-de-dados-deve-evitar-jabuticabas/. Acesso em: 6 jan. 2020.

PARISER, Eli. *O filtro invisível*: o que a internet está escondendo de você. Rio de Janeiro: Zahar, 2012.

VARON, Joana; TEIXEIRA, Lucas. Podemos vigiar os vigilantes? *Medium*, 25 maio 2018. Disponível em: https://medium.com/codingrights/podemos-vigiar-os-vigilantes-ac3fe77e7694. Acesso em: 6 jan. 2020.

GLOSSÁRIO

Algoritmo – na internet, refere-se ao conjunto de regras que define como os seus dados serão interpretados e, posteriormente, que tipo de conteúdo lhe será oferecido.

Provedor – nos termos do Marco Civil da Internet, entende-se como provedor as aplicações de internet constituídas legalmente como pessoa jurídica, com fins econômicos e que exerçam atividade na internet de forma organizada e profissional. Por exemplo, redes sociais são provedores de aplicações de internet e, portanto, estão sujeitas à regulamentação da lei.

Sistema preditivo – resumidamente, é uma operação de base matemática aplicada a grandes conjuntos de dados que resulta em padrões capazes de identificar previsões. Atualmente, esse tipo de sistema tem o auxílio da tecnologia, facilitando a criação de possíveis cenários e tendências. Dessa forma, as empresas podem utilizar sistemas preditivos para analisar os padrões de consumo dos seus clientes.