centro universitário
unifacvest

Criptografia, ataques cibernéticos e perícia forense

Conceitos de forense computacional

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer os aspectos de isolamento, coleta e preservação do processo de forense computacional.
- Identificar os exames realizados na computação forense e os documentos processuais.
- Definir defesa cibernética e documentos processuais.

Introdução

Neste capítulo, você vai estudar os principais conceitos de forense computacional. Esse é um ramo da ciência forense aplicada ao mundo digital, no qual as evidências dos crimes são encontradas em computadores, redes de computadores, *sites* e aparelhos de tecnologia móvel, como *smartphones*. A ciência forense digital existe há mais de 40 anos, entretanto vem evoluindo constantemente. Ela cresce à medida que aumenta o volume de crimes digitais, como furto de dados, pedofilia, fraudes e perfis falsos.

Apesar da falsa percepção de impunidade no ambiente digital, os crimes deixam vestígios. Como você vai ver, os métodos de investigação para os crimes digitais incluem técnicas e conhecimentos específicos, permitindo a comprovação dos delitos. Ao longo do capítulo, você vai conhecer os conceitos de isolamento, coleta e preservação. Além disso, você vai estudar os exames realizados na computação forense, a defesa cibernética e os documentos processuais envolvidos.

1 Isolamento, coleta e preservação

Com a evolução da internet, as pessoas ao redor do mundo passaram a usar a maior rede de computadores mundial não apenas para se comunicar, mas também para realizar tarefas do seu dia a dia. Atualmente, as pessoas fazem compras *on-line* em supermercados, farmácias e grandes redes varejistas, além de realizar diversas transações financeiras pela internet, relativas a serviços públicos e privados. Tudo isso acontece por meio de computadores pessoais, corporativos, celulares e *tablets*. Assim, embora tenha muitos pontos positivos, esse novo comportamento abre uma grande janela para o crime digital, tornando as pessoas mais vulneráveis.

Os vestígios de um crime são a chave que permite aos peritos criminais buscar informações que se tornem evidências e, posteriormente, provas judiciais. Nos casos de crimes digitais, o analista ou perito forense é o profissional responsável pela preservação, pelo levantamento de dados e pela análise de evidências, por meio do uso de técnicas e ferramentas. Apesar da vasta quantidade de crimes realizados no ambiente digital, não existem no mercado muitos profissionais especializados para atuar na área forense. Isso ocorre principalmente devido à qualificação exigida para a realização dessa atividade e à necessidade de o profissional forense ter dispositivos similares aos utilizados pelos criminosos digitais.

Segundo Eleutério e Machado (2011, p. 16), diversos profissionais podem estar envolvidos em um procedimento forense computacional: "peritos particulares, auditores de sistemas, profissionais de TI e outros. Além disto, juízes, advogados, delegados, promotores e demais profissionais da área de Direito". O analista ou perito forense deve conhecer profundamente as leis e ter conhecimentos técnicos relativos a sistemas operacionais, redes, programação e técnicas de coleta e análise de dados.

Fique atento

O perito forense computacional atua em crimes que envolvem internet e tecnologia, como exploração sexual, fraudes, clonagem de cartões de crédito e rádios piratas. Ele também executa tarefas que exigem conhecimento tecnológico, como rastreamento de mensagens e ligações. A formação mínima exigida é nível superior.

Apesar de o crime digital ocorrer em um ambiente virtual, ele é um crime como outro qualquer. Em todos os tipos de crime, parte-se da seguinte premissa: havendo vestígios a serem analisados, o exame pericial é obrigatório. É o que consta no Código Penal Brasileiro, art. 158: "Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado" (BRASIL, [1940]).

Além dos conhecimentos técnicos, é de suma importância que o profissional forense tenha uma excelente postura comportamental, realizando análises isentas e imparciais. Como afirma Tomás (2009), o perito não deve ter antecedentes que possam levantar suspeitas a respeito do seu caráter e da sua ética profissional.

Na investigação de crimes computacionais, há a necessidade intrínseca de busca e apreensão dos equipamentos. Para isso, é fundamental a prévia emissão de mandados de busca e apreensão pelos órgãos públicos competentes. Com o mandado em mãos, o perito faz a identificação do local, conduz a ele, seleciona os equipamentos e os apreende.

Durante todo o procedimento de investigação forense, o manuseio das informações deve ser realizado dentro de padrões, garantindo que os vestígios criminais sejam preservados para a correta análise. Para que o processo investigativo se inicie, é necessário:

- possuir mídias esterilizadas ou uma nova mídia instalada, evitando possíveis contaminações;
- utilizar ferramentas/*softwares* para análise forense devidamente licenciadas;
- garantir que nenhuma fonte de dados seja alterada até a chegada do perito (caso haja alterações no ambiente, isso deve ser reportado no laudo);
- fazer toda a análise por meio de imagem ou de disco duplicado, ou seja, o material original jamais deve ser manipulado (deve permanecer intacto);
- caso o equipamento esteja ligado, mantê-lo ligado para evitar possíveis perdas de dados;
- apresentar o resultado do exame pericial de forma clara, elucidativa e em uma linguagem acessível;
- providenciar fotos e filmes do local onde ocorreu o crime, assim como cópias dos *sites*, para garantir a coleta de mais detalhes.

Conforme Sousa (2016), as boas práticas em procedimentos periciais recomendam as fases listadas a seguir.

Coleta

O ambiente que receberá os dados coletados deve ser adequado a parâmetros que permitam a transferência fidedigna para a posterior análise. A parte de infraestrutura, como discos, deve estar funcionando corretamente. Em casos específicos, quando há orçamento suficiente, é possível copiar as informações. Para isso, podem ser utilizados duplicadores de disco ou soluções de *software* específicas para perícia.

Ao final da fase de coleta, o dispositivo para o qual os dados foram copiados deve ser devidamente lacrado e armazenado em local apropriado até a Justiça autorizar o seu descarte ou a sua devolução. Nesse momento, deve ser preenchido o formulário de cadeia de custódia, com os dados dos equipamentos apreendidos, como: mídia, marca, modelo, número de série e disco rígido. A data, a hora e o responsável pelo manuseio e pelo processo forense também devem ser registrados.

Na Figura 1, a seguir, veja um exemplo de um formulário de cadeia de custódia. A cadeia de custódia é uma das principais obrigações do perito e é um documento exigido nas análises forenses computacionais, funcionando como uma garantia de autenticidade do processo.

Modelo de formulário de Cadeia de Custódia

Case No.				
Responsável				
Natureza do caso				
Endereço do local da coleta				
Item #	Descrição	Fabricante	Modelo	Serial
Cópia de segurança realizada por			Data e hora	
Recuperação realizada por			Data e hora	
Evidência processada por	Localização da evidência		Data e hora	

Figura 1. Formulário de cadeia de custódia.

Fonte: Reis (2013, documento *on-line*).

Exame

Essa etapa é considerada a mais trabalhosa da investigação. Isso se deve à quantidade de dados para análise, que geralmente têm diferentes formatos, como: arquivos criptografados, áudios, vídeos, imagens, arquivos compactados, entre outros. Os dados coletados na fase anterior devem ser recuperados e catalogados, permitindo uma análise científica que não seja posteriormente questionada.

O perito deve realizar uma investigação profunda dos fatos no sistema operacional, assim como considerar todas as hipóteses possíveis, como buscar arquivos que já tenham sido eliminados do sistema. Esse procedimento se chama *data carving*. De acordo com o National Institute of Standards and Technology (2014, p. 3, tradução nossa), *carving* é

> o processo de reconstrução de arquivos deletados, de um espaço de armazenamento não alocado, ou extração de arquivos embutidos em um contêiner de arquivos, baseada no conteúdo do arquivo; metadados do sistema de arquivos devem ser considerados de forma secundária ou completamente ignorados.

Análise

Nessa fase, o perito analisa os dados coletados e examinados nas fases anteriores. O objetivo é encontrar evidências que comprovem o crime digital. A análise pode ser a fase mais demorada de todas as que compõem a investigação.

Dependendo do número de dados e arquivos envolvidos, é necessário identificar prioridades e definir o que será analisado. Caso contrário, o processo de análise pode ser inviável, devido ao tempo que se levará para analisar todos os documentos.

Para analisar os arquivos criptografados, o perito deve utilizar algum programa de quebra de senha. Ele também pode fazer buscas na memória de acesso aleatório (Random Access Memory [RAM]) a fim de localizar as senhas digitadas. Além disso, existem fontes de consulta como a Biblioteca Nacional de Referência do *Software* (RDS), que consiste em assinaturas digitais de arquivos conhecidos e rastreáveis até sua origem. Esse tipo de ferramenta facilita o procedimento e pode diminuir o número de arquivos que deverão ser analisados.

Resultado

Nessa etapa final, o perito redige o laudo pericial, apresentando provas e evidências, que deverão ser utilizadas nos processos judiciais. O laudo deve conter todos os detalhes que auxiliem o Judiciário na análise do crime. Ele deve ser claro e apresentar todas as evidências necessárias.

No Quadro 1, a seguir, veja uma síntese dos procedimentos periciais.

Quadro 1. Ciclo de análise forense

Etapa	Procedimento	Principais atividades
1	Coleta (mídias)	■ Isolar a área ■ Coletar as evidências ■ Garantir a integridade ■ Identificar equipamentos ■ Embalar e etiquetar evidências ■ Preencher o formulário de cadeia de custódia
2	Exame (dados)	■ Identificar ■ Extrair ■ Filtrar ■ Documentar
3	Análise (informações)	■ Identificar pessoas, eventos e locais ■ Correlacionar pessoas, eventos e locais ■ Reconstruir a cena ■ Documentar
4	Resultados obtidos (evidências)	■ Redigir laudo ■ Anexar evidências e demais documentos

Fonte: Adaptado de Processo... ([20--]).

2 Exames e documentos processuais

Na etapa de exames, o perito deve definir o modelo ideal de abordagem para cada tipo de caso, preservando sempre as condições iniciais, que vão garantir a melhor análise dos vestígios. Nessa etapa, os peritos têm acesso aos equipamentos apreendidos que foram violados ou que aplicaram qualquer tipo de violação legal. Assim, o objetivo dos profissionais é analisar, identificar e localizar todos os arquivos, sistemas e aplicativos que podem conter indícios de crimes.

Veja o que Eleutério e Machado (2011, p. 51) destaca a respeito dos materiais questionados, ou seja, dos materiais apreendidos e submetidos a exames forenses:

> Os materiais questionados mais comuns nesse tipo de exame são os discos rígidos, seguidos pelos CDs e DVDs. No entanto, tais procedimentos devem ser seguidos para qualquer tipo de equipamento de armazenamento computacional, incluindo *pen drives*, cartões de memória, disquetes, *blu-rays*, entre outros a serem ainda inventados pelo homem.

Um dos itens mais importantes em uma investigação criminal computacional é a identificação do IP (Internet Protocol) do criminoso. O IP é o número atribuído durante o tempo de conexão à internet. Esse número pertence a determinado acesso durante a conexão na rede de computadores mundial, porém, após a desconexão, ele é utilizado por outro usuário da internet. Por esse motivo, o perito precisa identificar a data e o horário da conexão, além do fuso horário e do provedor. Com base na identificação desses dados, o perito deve providenciar um mandado judicial para buscar, junto ao provedor, o responsável pela conexão no dispositivo em que foi cometido o crime.

Para identificar o dispositivo utilizado para o crime, o perito precisa descobrir o endereço de controle de acesso à mídia, também chamado de "endereço MAC" (Media Access Control). Esse número identifica a placa de rede e é único para cada dispositivo.

Independentemente do dispositivo utilizado para a realização do crime, durante a fase de exame, o perito deve buscar responder a quatro perguntas: o quê? Quando? Onde? Como? O exame pode ser realizado em diferentes tipos de dispositivos, com seus respectivos tipos de análise. A seguir, veja quais são os principais dispositivos.

Computador

Nesse caso, é necessário analisar toda a estrutura do equipamento, plataformas físicas ou servidores, buscando arquivos, dados e acessos que podem caracterizar vestígios de crimes digitais. O grande desafio é o acesso aos computadores utilizados, que podem estar em território nacional ou em outros países. Também é desafiador identificar os usuários e atentar ao sincronismo de horário e ao uso de criptografia complexa para manter o anonimato.

O perito deve buscar: mensagens eletrônicas, imagens, planilhas, programas de computador, rastros de navegação, etc. Os principais tipos de crimes cometidos por meio desses dispositivos são: compartilhamento de arquivos de pornografia infantojuvenil, roubo de senhas (*malware*) e instalação de programas de roubo de dados bancários.

Sites

Nesse caso, os peritos analisam *sites* existentes, avaliando conteúdos, publicações, domínio da internet e endereço IP. Conforme Eleutério e Machado (2011, p. 20), o exame em *sites* consiste "principalmente na verificação e cópia de conteúdo existente na Internet, em *sites* e servidores remotos dos mais variados serviços. Além disso, trata-se da investigação do responsável por um domínio de um *site* e/ou endereço IP".

O perito deve: identificar o serviço *web*, identificar o *site* hospedeiro, preservar as evidências, analisar as *logs* e analisar os aplicativos e serviços da rede. Os principais tipos de crimes cometidos por meio desses dispositivos são: ataques a *sites*, invasões, plágio, *phishing* (páginas falsas), *malware*, pornografia e furto de dados.

Mensagens eletrônicas (*e-mails*)

A análise de mensagens eletrônicas envolve mensagens transmitidas, remetentes, endereços IP, domínios da internet e conteúdos. Conforme Eleutério e Machado (2011, p. 20), o exame em *e-mails* corresponde "basicamente à análise das propriedades das mensagens eletrônicas, a fim de identificar hora, data, endereço IP e outras informações do remetente da mensagem".

Nesses casos, o grande desafio é relativo à disponibilidade de registros (*logs*) suficientes. O perito ainda precisa garantir que os horários estejam sincronizados e lidar com diversos tipos de tecnologias. Em síntese, o perito deve: identificar a mensagem eletrônica, identificar o ambiente, preservar as evidências, verificar a origem da mensagem (cabeçalho) e analisar o corpo do *e-mail*. Os principais tipos de crimes cometidos por meio desses dispositivos são: questões trabalhistas, calúnia, difamação, desonra, concorrência desleal, ameaças anônimas e espionagem.

Aparelhos móveis (celulares)

Os aparelhos celulares, devido à sua amplitude tecnológica, já podem ser comparados a computadores portáteis. Assim, a análise de celulares é similar à análise realizada em computadores. Ela envolve a análise de mensagens enviadas, incluindo remetentes, números de telefone, datas, horários e dados relacionados a chamadas. Os dados analisados dizem respeito a mensagens enviadas por Short Message Service (SMS) e WhatsApp, por exemplo. Além disso, o perito deve buscar dados deletados.

Conforme Eleutério e Machado (2011, p. 20), o exame em celulares abrange "basicamente a extração dos dados desses aparelhos, a fim de recuperar e formalizar as informações armazenadas em suas memórias (lista de contatos, ligações, fotos, mensagens etc.), de acordo com a necessidade de cada caso".

O grande desafio aqui é manter-se atualizado em relação às ferramentas *mobile*, que estão em constante modificação. É necessário possuir os equipamentos adequados para a análise (*software* e *hardware*) e atentar à diversidade de funcionalidades existentes. Os principais tipos de crimes cometidos por meio desses dispositivos são: invasões, espionagem, calúnia, difamação e pornografia.

Redes de computadores

A análise de dados trafegados na rede tem foco no trânsito da informação, e não no armazenamento, independentemente do dispositivo emissor e do dispositivo receptor. Nesse caso, é necessário utilizar técnicas e ferramentas para: reconstrução de sessões, análise de protocolos, manipulação de arquivos, identificação de origem e destino, identificação de protocolos e dados, além de recuperação de arquivos capturados no tráfego.

Os grandes desafios são: o acesso aos computadores conectados dentro de uma rede, a identificação dos usuários e o sincronismo de horários. Os principais tipos de crimes cometidos por meio de redes são: invasões, plágio, pornografia e furto de dados.

Internet das Coisas (IoT)

Essa área é muito recente. Ela tem crescido bastante à medida que os dispositivos conectados à internet (televisão, carros, refrigeradores, etc.) abrem uma gama de possibilidades de crimes digitais. A investigação forense para tratar da IoT (do inglês Internet of Things) está sendo desenvolvida para coletar e analisar evidências nesses dispositivos.

Nesses casos, o desafio é imenso, pois está em jogo uma tecnologia emergente: não existe um único dispositivo, e sim uma rede hiperconectada. O perito deve: identificar o dispositivo, preservar as evidências, analisar as *logs* e analisar os aplicativos e serviços da rede. Os principais tipos de crimes cometidos por meio desses dispositivos são: invasões, furto de dados e *malware*.

Banco de dados

A análise ocorre em dados e metadados armazenados em bancos de dados, disponibilizados ou não em servidores. O objetivo é identificar a manipulação de dados armazenados, como possíveis fraudes financeiras e fiscais praticadas em uma empresa.

Nesses casos, os grandes desafios são a identificação das tabelas, a busca por dados excluídos e a identificação das transações realizadas. O perito deve: identificar as bases de dados envolvidas, preservar as evidências e analisar as *logs*. Os principais tipos de crimes cometidos por meio desses dispositivos são: invasões, furto de dados e vazamento de informações.

Algumas considerações

Conforme Freitas (2003), em todos os tipos de dispositivos digitais, a análise pode ser física e/ou lógica. A seguir, veja como cada uma dessas análises se caracteriza.

- **Análise física:** tem como objetivo analisar os dados do dispositivo de armazenamento. Isso ocorre da seguinte forma: pesquisa de sequência, busca e extração, inclusive de espaço subaproveitado e livre de arquivos. Esse tipo de análise consiste em buscar todas as URLs, *e-mails* encontrados e partes inacessíveis do disco.

- **Análise lógica:** essa análise é feita arquivo por arquivo. O perito analisa o conteúdo dos arquivos com o apoio de aplicativos que ajudam nesse tipo de extração de dados.

A análise forense exige o uso de algumas ferramentas, como:

- *software* de imagem de disco;
- *software* ou *hardware* de escrita;
- ferramentas de *hashing*;
- *software* de recuperação;
- *software* de peneira;
- *software* de decodificação de criptografia.

O volume de crimes digitais tem crescido diariamente; percebe-se um aumento significativo de um ano para outro. Isso demonstra uma mudança comportamental, ou seja, as vítimas têm denunciado os crimes. Para compreender melhor esse contexto, veja o trecho de uma matéria publicada pelo jornal Correio Braziliense em 4 de agosto de 2019:

> Diariamente, são registrados pelo menos 366 crimes cibernéticos em todo o país. O levantamento mais recente, feito em 2018 pela associação SaferNet Brasil, em parceria com o Ministério Público Federal (MPF), contabilizou 133.732 queixas de delitos virtuais, como pornografia infantil, conteúdos de apologia e incitação à violência e crimes contra a vida e violência contra mulheres ou misoginia e outros. Em comparação ao ano anterior, a quantidade de ocorrências deu um salto de quase 110% — em 2017, a associação registrou 63.698 denúncias. Um fator que contribui para a ação criminosa, na visão de especialistas, é o descuido da população quanto à utilização de ferramentas que protejam os aparelhos celulares das invasões de *hackers*. Apesar de ser impossível estar 100% protegido, o mínimo de precaução pode reduzir as ameaças à privacidade de cada um (FERNANDES, 2019, documento *on-line*).

Na Figura 2, a seguir, você pode ver um mapa mental (diagrama que representa, a partir de um tema central, todos os itens envolvidos) que exemplifica a variedade de elementos implicados em uma análise forense computacional. A profissão de um perito criminal é muito ampla, envolvendo conhecimentos técnicos e legais em uma grande variedade de assuntos.

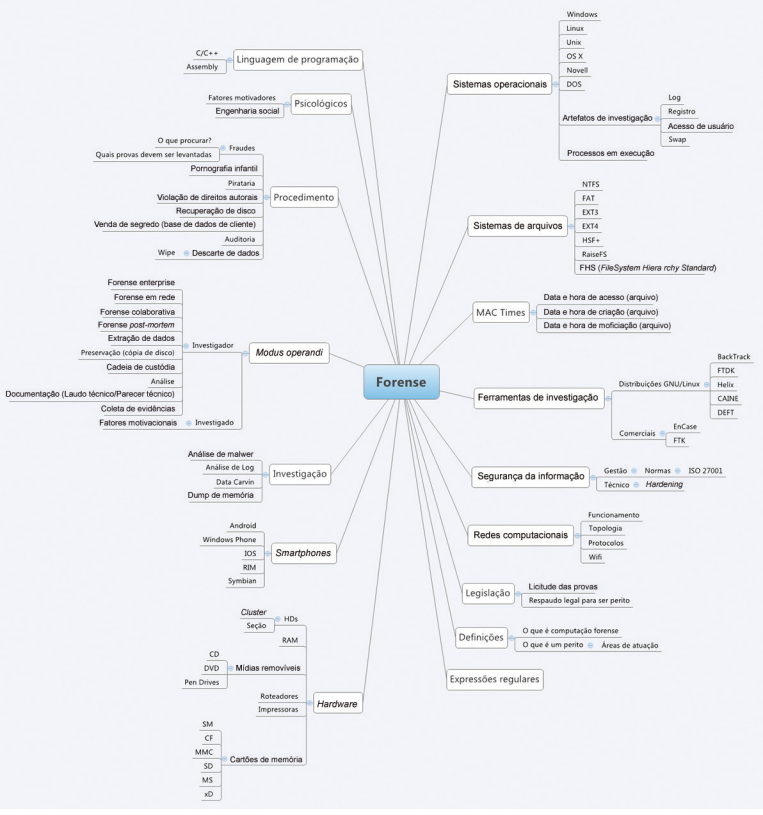

Figura 2. Mapa mental do conhecimento do perito forense computacional.
Fonte: Adaptada de Rios (2012).

3 Defesa cibernética e documentos processuais

A defesa de crimes digitais é um processo complexo pelo fato de a internet não possuir fronteiras, ou seja, qualquer conteúdo é acessado de qualquer lugar do mundo. O termo ciberespaço surge pela primeira vez no romance "Neuromancer", de William Gibson (CIBERESPAÇO, 2019). O ciberespaço (ou espaço cibernético) é uma metáfora que descreve o espaço não físico criado por diversas redes de computadores (a internet), onde as pessoas podem se comunicar de muitas formas, seja por mensagens, *e-mails*, salas de bate-papo, grupos de discussão, aplicativos de mensagens, dentre outros.

Esse espaço cibernético proporciona muitos serviços e no seu ambiente transitam informações sigilosas que estão sujeitas a muitas ameaças, devido ao seu valor e importância. Neste sentido, Nye Junior (2011) observa que nos países com a internet mais desenvolvida, além dessa gama de recursos e soluções, também existe uma forte insegurança para governos, empresas e todas as pessoas dessas nações.

Conforme Rachel (2009), Silveira (2018) e Caldeira (2011), um bom ponto a se considerar em crimes cibernéticos é a distinção entre crimes a distância e crimes plurilocais. Veja:

- nos crimes a distância, a ação e a consumação do crime ocorrem em lugares distintos, um deles fora do território nacional;
- nos crimes plurilocais, a ação e a consumação também ocorrem em lugares diversos, mas ambos no território nacional.

Qualquer medida que envolva outros países depende de acionamentos entre países para coleta, análise e validação de vestígios de crimes digitais. É o caso, por exemplo, da abertura de dados por empresas como Facebook, Instagram e WhatsApp. Existem também conflitos dentro do território nacional, geralmente relativos à competência de cada foro: o foro do local de onde partiu a ofensa, o foro de domicílio do ofendido e do infrator e ainda o foro do local onde o ofendido toma ciência da ofensa.

No Brasil, têm ocorrido evoluções no âmbito legal. A defesa de ataques cibernéticos ganhou reforço com a aprovação do Decreto nº. 10.222, de 5 de fevereiro de 2020, que estabelece a Estratégia Nacional de Segurança Cibernética.

O objetivo desse decreto é tornar o Brasil mais próspero e confiável no meio digital, aumentando a resiliência local para ameaças cibernéticas e fortalecendo a segurança do País em âmbito internacional. Veja o que o decreto diz a respeito:

> Desse modo, estes objetivos estratégicos visam a nortear as ações estratégicas do País em segurança cibernética, e representam macrodiretrizes basilares para que o setor público, o setor produtivo e a sociedade possam usufruir de um espaço cibernético resiliente, confiável, inclusivo e seguro. São os objetivos estratégicos:
> 1. Tornar o Brasil mais próspero e confiável no ambiente digital;
> 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e
> 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.
> (BRASIL, 2020, documento *on-line*).

O Decreto nº. 10.222/2020 descreve 10 ações que precisam ser implementadas (BRASIL, 2020):

1. fortalecer as ações de governança cibernética;
2. estabelecer um modelo centralizado de governança em nível nacional;
3. promover um ambiente participativo e colaborativo entre setor público e privado;
4. elevar o nível de proteção do governo;
5. elevar a proteção das infraestruturas críticas nacionais;
6. aprimorar o arcabouço legal sobre segurança cibernética;
7. incentivar a concepção de soluções inovadoras em segurança cibernética;
8. ampliar a cooperação internacional do Brasil em segurança cibernética;
9. ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade;
10. elevar o nível de maturidade da sociedade no que diz respeito à segurança cibernética.

Outra iniciativa em andamento é a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº. 13.709, de 14 de agosto de 2018. Essa lei tem como objetivo contribuir para a governança da segurança cibernética nacional por meio de normas e políticas públicas relativas à proteção de dados pessoais e à privacidade, considerando a coleta, o armazenamento, o tratamento e o compartilhamento de dados pessoais. A previsão é que a LGPD entre em vigor no Brasil no dia 16 de agosto de 2020.

Fique atento

A LGPD não substitui o Marco Civil digital, mas reúne ações complementares. O seu objetivo é atuar em um novo cenário mundial, em que os dados trafegam todos os dias dentro da imensa rede de computadores, assim como dentro de redes de grandes corporações, ou ainda por meio de redes sociais.

A LGPD tem como base a GDPR europeia: "Seguindo os passos da GDPR (General Data Protection Regulation), que vale para todos os países da União Europeia, a LGPD já engatinhava com a criação do Marco Civil da Internet em 2014" (LGPD..., 2019, documento *on-line*). A LGPD determina que o usuário tem o direito de acessar seus dados a qualquer momento, conferindo como eles são tratados e compartilhados. A lei também determina que o usuário pode atualizar ou corrigir dados incorretos, deletar dados e transferir dados para outras organizações (públicas ou privadas).

As penalizações previstas pela LGPD consideram multas, bloqueios e sanções para as empresas que descumprirem ou não se adequarem à nova lei. Além disso, a LGPD extravasa o território brasileiro. Ela pode ser aplicada a qualquer empresa, e mesmo as empresas estrangeiras que não têm sede no local estão sujeitas a sanções. A não aplicação da LGPD pode acarretar multas de até R$ 50 milhões. Por esse motivo, observa-se uma corrida das organizações desde 2018, quando a lei foi aprovada, para adaptar seus sistemas e bancos de dados ao novo cenário, o que cria muitas oportunidades para profissionais com conhecimento nesse assunto.

Referindo-se às evoluções legais, Souza Junior (2013, p. 32) ressalta o empenho dos órgãos governamentais:

> A Administração Pública Federal apresenta o real empenho e precaução na criação de um modelo de segurança cibernética para proteção do ciberespaço e dos serviços e informações nele existentes, assim se adaptando ao cenário atual de crimes cibernéticos.

É notável que os órgãos governamentais têm atuado de forma mais enfática em relação aos crimes digitais. Como você viu, tal atuação se dá por meio da criação e da aprovação de leis e decretos que suportem judicialmente direitos e deveres no universo digital. Porém, é nítido que a defesa em processos criminais cibernéticos tem um caminho longo a percorrer, seguindo a constante evolução do mundo digital.

Referências

BRASIL. *Decreto Nº 10.222, de 5 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília: Casa Civil da Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 11 abr. 2020.

BRASIL. Ministério da Justiça. *Decreto-Lei Nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília: Casa Civil da Presidência da República, [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 11 abr. 2020.

CALDEIRA, S. Qual a diferença entre crime plurilocal e crime à distância? *Sandro Caldeira*, [*S. l.*], 19 maio 2011. Disponível em: http://www.sandrocaldeira.com/plus/modulos/noticias/ler.php?cdnoticia=22&cdcategoria=1. Acesso em: 11 abr. 2020.

CIBERESPAÇO. *In*: GLOSSÁRIO da Sociedade da Informação. Lisboa: Associação para a Promoção e Desenvolvimento da Sociedade da Informação, 2019. Disponível em: https://apdsi.pt/glossario/c/ciberespaço. Acesso em: 11 abr. 2020.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. *Desvendando a computação forense*. São Paulo: Novatec, 2011. 200 p.

FERNANDES, A. Crimes virtuais e ataques cibernéticos mais do que dobram em um ano. *Correio Braziliense*, Brasília, 4 ago. 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/politica/2019/08/04/interna_politica,775357/crimes-virtuais-e-ataques-ciberneticos-mais-do-que-dobram-em-um-ano.shtml. Acesso em: 11 abr. 2020.

FREITAS, A. R. *Perícia forense aplicada à informática*. Orientador: Duval Costa. 2003. 58 f. Trabalho de Conclusão de Curso (Pós-Graduação "Lato Sensu" em Internet Security) – Instituto Brasileiro de Propriedade Intelectual, São Paulo, 2003. Disponível em: https://rl.art.br/arquivos/120158.pdf. Acesso em: 11 abr. 2020.

LGPD: O manual para compreender a lei geral de proteção de dados. *TOTVS*, São Paulo, 26 set. 2019. Disponível em: https://www.totvs.com/blog/negocios/lgpd-o-manual-para-compreender-a-lei-geral-de-protecao-de-dados/. Acesso em: 11 abr. 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Forensic File Carving Tool Specification*: Draft Version 1.0 for Public Comment. Gaithesburg: NIST, 2014. 12 p. Disponível em: https://www.nist.gov/system/files/documents/2017/05/09/fc-req-public-draft-01-of-ver-01.pdf. Acesso em: 11 abr. 2020.

NYE JUNIOR, J. S. *The future of power*. New York: PublicAffairs, 2011. 320 p.

PROCESSO de Investigação. *Forense Computacional*, [*S. l.*], [20--]. (Projeto desenvolvido por alunos da disciplina "Direito e Informática" – DIR410011, ministrada pelo professor Aires J. Rover para alunos do programa de mestrado em Ciências da Computação da Universidade Federal de Santa Catarina). Disponível em: https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao. Acesso em: 11 abr. 2020.

RACHEL, A. R. O que se entende por crime à distância? *Jusbrasil*, Salvador, 25 set. 2009. Disponível em: https://lfg.jusbrasil.com.br/noticias/1912334/o-que-se-entende-por--crime-a-distancia-andrea-russar-rachel. Acesso em: 11 abr. 2020.

REIS, F. M. *Forense computacional*: técnicas para preservação de evidências em coleta e análise de artefatos. Orientadora: Ana Cristina Azevedo Pontes de Carvalho. 2013. Monografia (Aperfeiçoamento/Especialização em Computação Forense) – Universidade Presbiteriana Mackenzie, São Paulo, 2013. Disponível em: https://monografias.brasilescola.uol.com.br/computacao/forense-computacional-tecnicas-para-preservacao--evidencias-coleta-analise-artefatos.htm. Acesso em: 11 abr. 2020.

RIOS, A. Brainstorming para Estudos Forenses. *Estudos Forenses – Site de Estudo de Computação Forense*, [*S. l.*], 7 maio 2012. Disponível em: https://4en6br.wordpress.com/2012/05/07/brainstorming-para-estudos-forenses/. Acesso em: 11 abr. 2020.

SILVEIRA, W. P. Como se define o local do crime nos crimes plurilocais e nos crimes à distância? *Jusbrasil*, Salvador, 16 abr. 2018. Disponível em: https://wesl.jusbrasil.com.br/artigos/566936270/como-se-define-o-local-do-crime-nos-crimes-plurilocais-e-nos--crimes-a-distancia. Acesso em: 11 abr. 2020.

SOUSA, A. G. Etapas do processo de computação forense: uma revisão. *Acta de Ciências e Saúde*, Taguatinga, v. 5, n. 2, p. 99–111, 2016. Disponível em: http://www2.ls.edu.br/actacs/index.php/ACTA/article/view/138. Acesso em: 11 abr. 2020.

SOUZA JUNIOR, A. F. *Segurança Cibernética*: Política Brasileira e a Experiência Internacional. Orientador: Rosalvo Ermes Streit. 2013. 120 f. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2013. Disponível em: https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1417/1/Alcyon%20Ferreira%20de%20Souza%20Junior.pdf. Acesso em: 11 abr. 2020.

TOMÁS, E. M. C. *Crimes informáticos*: legislação brasileira e técnicas de forense computacional aplicadas à essa modalidade de crime. Orientador: Mauro Cesar Sobrinho. 2009. 42 f. Monografia (Especialização em Gestão e segurança em redes de computadores) – Centro Universitário Euro-Americano, Brasília, 2009. Disponível em: https://artigos.etc.br/crimes-informaticos-legislacao-brasileira-e-tecnicas-de-forense-computacional--aplicadas-a-essa-modalidade-de-crime.html. Acesso em: 11 abr. 2020.

Leituras recomendadas

LOPES, P. A. Forense Digital – Perícia Forense Computacional. *Pentest e Forense Digital/Computação Forense*, Caxias do Sul, 11 jun. 2016. Disponível em: https://periciacomputacional.com/pericia-forense-computacional-2/. Acesso em: 11 abr. 2020.

SILVA, H. B. *Perícia forense computacional em dispositivos móveis*. Orientador: Fábio Eder Cardoso. 2015. 80 f. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) – Instituto Municipal de Ensino Superior de Assis, Assis, 2015. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1211321025.pdf. Acesso em: 11 abr. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Crimes digitais

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer as características de um crime digital.
- Identificar os tipos mais comuns de crimes digitais.
- Apresentar os princípios de investigação de crimes digitais.

Introdução

Os crimes digitais passaram a fazer parte do dia a dia das pessoas a partir do uso da Internet pela população e também pelas grandes organizações. Como em todos os meios, há oportunidade de os indivíduos realizarem crimes contrariando a lei em busca de benefícios próprios.

Os crimes digitais estão ganhando volume devido ao uso massivo da rede de computadores no cotidiano das pessoas. As ações — como estelionato, um crime que existe desde o início da humanidade — se tornaram cada vez mais frequentes no ambiente digital, principalmente pelas redes sociais, ganhando volume estrondoso e gerando inúmeros prejuízos para a sociedade e também para as empresas.

Observamos também um volume crescente de crimes de calúnia, difamação e injúrias, a partir de encorajamento das pessoas nas redes sociais, novamente embasados pela falsa percepção de impunidade.

Neste capítulo, você vai ver como os crimes são caracterizados, os tipos de crimes digitais e os princípios de investigação de crimes digitais.

1 Características de um crime digital

Com o nascimento da Internet nos EUA na década de 1960, que tinha um ideal bélico criado pela Defense Advanced Research Projects Agency para inibir intervenções em suas comunicações pela extinta União Soviética, passamos a ter um sistema de informação interligado, sem localização física ou central específica.

Em 1970, foi criado o par de padrões Transfer Control Protocol/Internet Protocol (TCP/IP — Protocolo Controle de Transferência/Protocolo de Internet), permitindo a comunicação entre usuários. Na década de 1980, foi criado o conceito de Internet, por meio da ampliação do uso da rede para ações comerciais.

A partir de 1990, a rede *web* ganhou notoriedade, passando a ser um dos principais meios de comunicação. Esse novo modelo trouxe com ele um universo amplo para disponibilização de informações e um novo modelo de convivência na sociedade, no qual podemos conversar com qualquer pessoa a qualquer momento em qualquer lugar do mundo.

O uso dessa rede de computadores abriu uma importante porta para os crimes realizados na rede, chamados de crimes digitais. Na década de 1970, foi criado o termo *hacker*, que é o indivíduo capaz de promover a invasão de sistemas privados a partir de conhecimentos técnicos.

Os crimes digitais realizados pelas redes públicas, privadas ou domésticas podem atingir um ou vários indivíduos. Uma característica marcante nesse tipo de crime é a exponencialidade das ações, afinal, um *software* malicioso utilizado para o furto de dados pode obter dados de vários clientes de uma organização.

Segundo estudo da Escola de Magistrados da Justiça Federal da 3ª Região (BRASIL, 2017, p. 19):

> [...] Com a popularização do acesso à Internet nos últimos anos, os crimes digitais no Brasil alcançam números assustadores. De acordo com a SaferNet (2017), que controla a Central Nacional de Denúncias, mais de 115 mil denúncias envolvendo exclusivamente crimes contra direitos humanos foram recebidas e processadas no ano de 2016.

Com a evolução da Internet, os crimes cibernéticos passaram a ser tão comuns que foram criadas no Brasil delegacias próprias para a realização desse tipo de denúncia, assim como mudanças na legislação, criando um recente amparo legal para julgar e punir crimes dessa natureza. Para entendermos melhor os crimes digitais, é importante entender como a Internet é segmentada:

- ***Surface web*** (*web* superficial) — é aquela na qual navegamos e acessamos *sites* de empresas, bancos, redes sociais, entre outros. Utilizamos navegadores como Google Chrome e buscadores como Google, Bing, entre outros, para realizar nossas pesquisas. Apesar da percepção que

existe um volume estrondoso de dados nesse segmento da rede, há análises de volumes de acessos que afirmam que apenas 4% de toda a informação circulada está na parte da *surface web*, conforme consta na pesquisa realizada pela empresa Experian (SIRUL, 2018, documento *on-line*, tradução nossa):

> [...] Se você é como a maioria das pessoas, é aqui que você passa a maior parte do tempo — fazendo compras *on-line*, pesquisando informações e compartilhando fotos e vídeos nas mídias sociais. No entanto, isso representa apenas cerca de 4% da Internet.

- ***Deep web*** — ao contrário da *surface web*, é composta por *sites* não indexados, portanto, não é possível encontrá-los nos canais de busca, como o Google. As informações presentes lá só podem ser acessadas se você realmente procurar. Quem acessa a *deep web* utiliza redes criptografadas, que ocultam a sua identidade. Esses sistemas funcionam com navegadores tradicionais, como Chrome, Firefox, entre outros, porém sem endereço IP e dados do usuário, que dificultam a identificação de quem está navegando. Nem todas as pessoas que navegam pela *deep web* cometem atos ilegais, algumas apenas querem ficar no anonimato, muito comum no mundo corporativo de grandes organizações e também utilizada por órgãos governamentais, entretanto, não podemos descartar que essa parte da Internet é utilizada sim para cometer crimes digitais.
- ***Dark web*** — também conhecida como zona escura da Internet, a criptografia é extremamente complexa, permitindo que apenas usuários que conheçam esse tipo de criptografia cheguem até ela. A *dark web* representa uma pequena parte da *deep web*, entretanto, é nesse espaço da rede que ocorrem os crimes digitais, como troca de informações ilegais, tráfico de drogas, ações de *hackers*, pedofilia, pornografia, entre outros crimes. Esse tipo de crime ocorre já que nesse ambiente o anonimato é garantido e a polícia tem dificuldades para descobrir quem é o responsável.

Apesar de a *surface web* ser um ambiente criptografado, permitindo uma melhor investigação e punição em casos de crimes, não impede a realização de uma extensa gama de crimes. Existem muitas infrações nessa parte da rede, principalmente crimes relacionados a fraudes, estelionato, calúnia e difamação, sendo estas duas últimas muito comuns nas redes sociais. A Figura 1 faz uma analogia entre os níveis de profundidade da *web* e um *iceberg*.

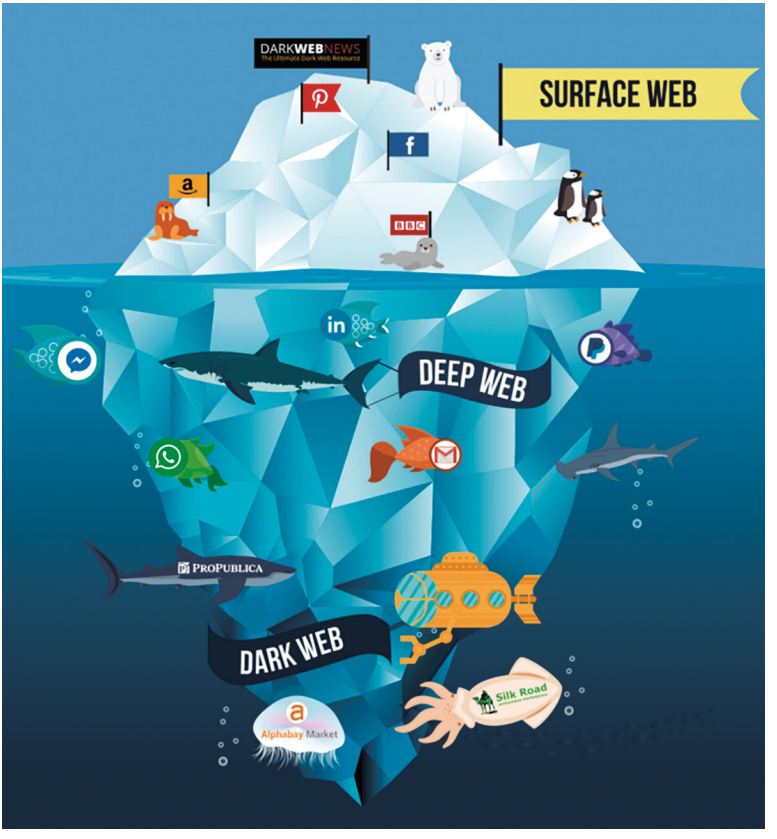

Figura 1. A *web* como um *iceberg*.
Fonte: Gogoni (2019, documento *on-line*).

A Internet é uma ferramenta-chave para as grandes organizações, permitindo a divulgação de seus produtos e aproximando o relacionamento com seus clientes. Entretanto, a Internet torna-se também uma grande preocupação em relação à segurança dos dados, tornando-se umas das maiores fontes de despesas com custos operacionais, como a compra e manutenção de ferramentas robustas para garantir a segurança das informações e a confiabilidade perante os clientes.

Nas últimas duas décadas, tivemos uma mudança cultural significativa no comportamento da sociedade a partir da criação das redes sociais. As redes sociais — pelas suas características de exposição impulsionada pelo uso de *smartphones* — trouxeram consigo um aumento nos crimes digitais a partir de uma exposição muito maior das pessoas. Outro crime que vem ganhando notoriedade com essa mudança comportamental é o aumento significativo de casos de injúrias e difamações, que estão cada vez mais comuns. Assim, o impacto que esse tipo de crime digital gera na vida das pessoas é gigantesco e desastroso.

Os usuários das redes sociais encaram suas convivências no mundo virtual como uma porta aberta para escrever o que bem entendem e realizar comentários extremamente prejudicais e ofensivos.

Saiba mais

Um estudo da Symantec, empresa do grupo Norton de segurança digital, indica que quase metade de todas as pessoas mundialmente conectadas à Internet fica feliz em contar mentiras sobre seus detalhes pessoais, incluindo nome, idade, situação financeira, estado civil, aparência e até mesmo sua nacionalidade. Além disso, um terço dos adultos já assumiu identidades falsas *on-line* — desde um nome falso até uma identidade totalmente fictícia. Os dados mostram que 33% dos adultos já utilizaram um nome falso e 45% mentiram sobre seus dados pessoais.

Os alemães são os melhores em fingir: mais da metade já adotou uma identidade falsa *on-line* ou já mentiu sobre detalhes pessoais *on-line* (53 e 51%, respectivamente). Mais da metade dos adultos chineses, brasileiros e indianos já admitiu ter mentido sobre as suas informações pessoais *on-line* (58, 56 e 55%, respectivamente).

Cerca de quatro em cada 10 italianos, brasileiros e neozelandeses já usaram identidades falsas *on-line* (41, 41 e 38%, respectivamente). As pessoas no Reino Unido sentem-se relutantes em fazer o mesmo — elas são as menos propensas a utilizar uma identidade falsa *on-line* (18%) ou mentir sobre as informações pessoais (33%).

2 Tipos mais comuns de crimes digitais

Com o crescente número de usuários na Internet, existe cada vez mais criminosos atuando na rede de computadores. Dessa forma, é muito importante entender os possíveis tipos de crimes que ocorrem na rede, ressaltando que os crimes digitais são ações que evoluem com muita velocidade. A cada novo dia, novos modelos de atividades ilícitas estão surgindo, incluindo as ações de mau comportamento dentro da rede, principalmente em redes sociais, transformando seus usuários em criminosos sujeitos a punições legais. Apresentamos a seguir alguns dos crimes virtuais mais comuns, que costumam ser praticados pela Internet:

- **Apologia ao crime** — incitar publicamente a prática de crime, fazer, publicamente (art. 287 "Apologia de fato criminoso ou de autor de crime" — Código Penal — Decreto-Lei nº. 2.848, de 7 de dezembro de 1940).
- **Aplicativos maliciosos (*malware*)** — são programas maliciosos instalados sem permissão do usuário, como vírus, para realização de furtos de dados pessoais, para fins fraudulentos.
- **Ato obsceno** — praticar ações de natureza sexual com ofensa ao pudor.
- **Calúnia** — atribuir sem provas a alguém uma ofensa que afete a sua dignidade ou acusar alguém de um crime.
- **Crimes virtuais contra mulheres** — envolvem casos de perseguições, ofensas, difamação, assédio e também a distribuição de fotos e vídeos pessoais.
- **Crimes de ódio** — são ataques racistas, de gênero, misóginos e até terroristas.
- **Difamação** — atribuir a alguém uma acusação pública que afete a sua reputação.
- **Divulgação de material confidencial** — expor publicamente dados de terceiros sem autorização (art. 153 "Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem" — Código Penal — Decreto-Lei nº. 2.848/1940).
- **Estupro virtual** — envolve coação para produção de conteúdo sexual sob ameaça de divulgação de fotos e vídeos.

- **Formulários falsos** — envio de mensagens de *e-mail* falsas para os usuários solicitando que seja preenchido um formulário, assim, os criminosos conseguem várias informações sobre os usuários, incluindo dados bancários.
- **Injúria** — atribuir a alguém uma ofensa desonrosa que afete a sua dignidade.
- **Lojas virtuais falsas** — é um golpe com a divulgação de ofertas falsas, com preços muito abaixo do preço real de produtos, no qual os usuários adquirem os produtos, realizam o pagamento, mas não recebem as mercadorias.
- **Pedofilia** — envolve armazenamento, produção, troca, publicação de vídeos e imagens contendo pornografia infantil ou do adolescente, cometido pela Internet.
- **Perfil falso** — refere-se usuários que criam identidade falsa na Internet para usar redes sociais, aplicar golpes ou realizar fraudes.
- ***Phishing*** — refere-se a conversas ou mensagens falsas com *links* fraudulentos.
- **Plágio** — é a cópia de informações veiculadas por terceiros sem a indicação da fonte.
- **Preconceito ou discriminação** — envolve utilizar *sites* da Internet ou redes sociais para opinar, de forma pejorativa e negativa, envolvendo assuntos como etnia, religião, opção sexual, raças, entre outros.
- ***Spam*** — são mensagens enviadas sem o consentimento do usuário.

Os crimes financeiros afetam inúmeros usuários da Internet, envolvendo desde ações que geram prejuízos individuais até ações que impactam ambientes corporativos, nos quais esse risco é muito maior, como o furto de dados confidenciais de seus clientes, o que poderá gerar prejuízos financeiros e à imagem da organização.

A Internet é um ambiente aberto, veloz e de fácil acesso. Vivemos em um período em que as crianças já nascem digitalizadas, assim, é nítida a velocidade na mudança dos hábitos da população em função dos usos de novas tecnologias. Por esse motivo, existe um árduo desafio na adaptação e definição de regras de boas condutas dentro do universo digital.

Assim, precisamos refletir sobre a importância da orientação e do acompanhamento dessas crianças, que não têm maturidade suficiente para se proteger de todos os perigos existentes no ambiente digital. Observamos mudanças na grade curricular do sistema de ensino, que passou a ser muito mais digitalizado, entretanto, essa digitalização ainda deixa muito espaço para crimes relacionados à pedofilia, que atinge um número imenso de crianças ao redor do mundo.

Além das redes sociais, o aplicativo WhatsApp, maior plataforma de mensagens utilizada massivamente ao redor do mundo, tem sido utilizado com muita frequência para aplicação de muitos dos crimes descritos. A Internet possibilita novas formas de interação social, sendo que esse novo modelo de relacionamento propicia golpes e o cometimento de crimes.

Uma recente pesquisa realizada pela PSafe, a desenvolvedora dos aplicativos dfndr, entre os dias 7 de maio e 22 de maio de 2019, revelou que um em cada cinco brasileiros já foi vítima de roubo de identidade na Internet, o que representa 24,2 milhões de potenciais vítimas em todo o País. As respostas à pergunta "Alguma das informações pessoais abaixo já foram usadas por alguém sem a sua permissão?" nessa pesquisa foram as seguintes (PAVÃO, 2019; PESQUISA..., 2019):

- 51,3% — número do telefone;
- 44,3% — credenciais de redes sociais;
- 37,1% — credenciais de *e-mail*;
- 26,8% — CPF;
- 19,3% — credenciais de banco ou cartão de crédito;
- 16,0% — credenciais de serviços de compra *on-line*;
- 14,9% — credenciais de serviços de *streaming*, como Netflix ou Spotify;
- 12,9% — outros.

Fique atento

No aplicativo de envio e recepção de mensagens mais popular no Brasil, o WhatsApp, as ações de punições podem ser feitas tanto em conversas individuais como em grupos. Em casos de crimes envolvendo conversas divulgadas em grupos, todos os usuários de um grupo poderão ser considerados responsáveis pelo conteúdo que outras pessoas enviam.

3 Princípios de investigação de crimes digitais

O grande volume de transações e acessos à Internet tem provocado um aumento significativo nos crimes digitais. Os usuários, apesar da sua desenvoltura para utilizar a Internet e navegar nas redes, ainda estão muito despreparados para reconhecer possíveis tentativas de fraudes e crimes digitais, sofrendo golpes que acabam gerando diversos prejuízos.

Muitos usuários não sabem de seus direitos e acabam ficando calados perante os crimes praticados. Apesar de existir uma percepção que os crimes digitais não são punidos, existem leis específicas para julgar esse tipo de crime. Além disso, existe um novo modelo de relacionamento entre países que cooperam com informações, as quais permitem a análise de casos que ultrapassam as fronteiras e as leis locais.

Localizar e identificar um criminoso digital é muito desafiador. Em crimes fora da rede, muitos criminosos são identificados por suas digitais, testemunhas ou evidências deixadas na cena do crime. No mundo digital, a busca por esses dados é feita em um enorme repositório de dados, por meio do endereço de IP do usuário da rede, podendo inclusive ter restrições de dados quanto ao conteúdo analisado.

Outro ponto em constante evolução são os julgamentos relacionados a crimes de injúria, difamação e calúnia, que ocorrem em grande volume nas redes sociais. Observamos uma evolução judiciária em relação a esses julgamentos, objetivando que os usuários examinem os conteúdos postados e evitem comentários indevidos em suas redes sociais. Esse tipo de julgamento somente acontecerá se a vítima acionar os órgãos competentes, realizando boletins de ocorrência e dando continuidade às ações judiciais. A melhor maneira de combater os crimes digitais é aplicar medidas similares ao sistema penal tradicional.

Em casos de crimes como roubo de dados, fraudes, pedofilia, entre outros, o processo de investigação não é uma tarefa fácil. Para chegar aos criminosos, é necessário descobrir muitas camadas de protocolo, quando estes são rastreáveis. Mesmo após a descoberta dos protocolos, são necessárias muitas autorizações para poder acioná-los judicialmente.

Saiba mais

O sistema judiciário brasileiro tem evoluído em relação ao julgamento de crimes cibernéticos, com a aprovação do novo Marco Civil da Internet (MCI) brasileira, sancionado em 23 de abril de 2014, pela Lei nº. 12.965, de 23 de abril de 2014, que regula o uso da Internet no Brasil, definindo direitos e deveres.

Outra lei brasileira específica para crimes digitais, Lei nº. 12.737, de 30 de novembro de 2012, é também conhecida como a **Lei Carolina Dieckmann**. A lei leva esse nome porque foi aprovada logo após o vazamento de fotos da atriz.

Conforme o art. 154-A da Lei Carolina Dieckmann (BRASIL, 2012, documento *on-line*):

> Art. 154-A 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.
> Pena — detenção, de 3 (três) meses a 1 (um) ano, e multa.

Mesmo o crime ocorrendo na *web* e caracterizado como crimes digitais poderá ser enquadrado em qualquer outra lei do Código Penal brasileiro, desde que o contexto do crime se aplique ao artigo da lei. Isso ocorre, por exemplo, em casos de calúnia e difamação. Uma barreira em todo esse processo é o enquadramento do ordenamento jurídico, considerando o sistema judiciário brasileiro, pois o local que ocorreu o crime nem sempre será o local do seu julgamento.

Grandes instituições financeiras têm impulsionado o governo para aprovação de leis contra crimes digitais. Esse interesse está embasado nos imensos prejuízos financeiros sofridos por fraudes que acontecem via rede. Uma reportagem do portal G1 cita que (ROHR, 2016, documento *on-line*):

> A Federação Brasileira dos Bancos (Febraban) afirma que instituições financeiras perderam R$ 1,8 bilhão com fraudes em 2015. Em 2011 (antes da aprovação da lei), a cifra era de R$ 1,5 bilhão. Embora a cifra não tenha crescido muito (ou nada, se for considerada a inflação), é difícil dizer se a "estagnação" dos prejuízos se deve à lei ou aos investimentos milionários dos próprios bancos em segurança.

O Quadro 1 apresenta os principais crimes digitais e suas respectivas tipificações.

Quadro 1. Alguns tipos de crimes digitais e leis utilizadas para o julgamento desses crimes

Crime	Tipificação em Lei
Furto eletrônico e estelionato (fraudes bancárias)	Arts. 155 e 171 do Código Penal — Decreto-Lei nº. 2.848, de 7 de dezembro de 1940 e alterações
Invasão de dispositivo informático e furto de dados	Art. 154-A do Código Penal
Falsificação e supressão de dados	Arts. 155, 297, 298, 299, 313-A e 313-B do Código Penal
Armazenamento: produção; troca, publicação de vídeos e imagens contendo pornografia infantil	Arts. 241 e 241-A do Estatuto da Criança ou do Adolescente (ECA) — Lei nº. 8.069, de 13 de julho de 1990
Assédio e aliciamento de crianças	Art. 241-D do ECA
Cyberbulling (veiculação de ofensas em *blogs* e comunidades virtuais)	Arts. 138, 139, 140 do Código Penal
Incitação e apologia ao crime	Arts. 286 e 287 do Código Penal
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	Art. 20 da Lei nº. 7.716, de 5 de janeiro de 1989
Crimes contra a propriedade intelectual artística e de programa de computador	Art.184 do Código Penal e Lei nº. 9.609, de 19 de fevereiro de 1998

Referências

BRASIL. Justiça Federal. Tribunal Regional Federal da 3ª. Região. Escola de Magistrados da Justiça Federal da 3ª. Região. *Investigação e prova nos crimes cibernéticos*. São Paulo: EMAG, 2017. 352 p. (Cadernos de estudos, 1). Disponível em: https://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 28 mar. 2020.

BRASIL. *Lei Nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Casa Civil da Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 28 mar. 2020.

GOGONI, R. Deep Web e Dark Web: qual a diferença? *Tecnoblog*, Americana, 18 mar. 2019. Disponível em: https://tecnoblog.net/282436/deep-web-e-dark-web-qual-a-diferenca/. Acesso em: 28 mar. 2020.

PAVÃO, S. 1 em cada 5 brasileiros já foi vítima de roubo de identidade na internet. *dfndr blog*, San Francisco, 30 out. 2019. Disponível em: https://www.psafe.com/blog/roubo-de-identidade/. Acesso em: 28 mar. 2020.

PESQUISA sobre roubo de identidade. *PSafe*, San Francisco, maio 2019. Disponível em: https://cdn.blog.psafe.com/blog/wp-content/uploads/2019/05/Pesquisa-PSafe-sobre--Roubo-de-Identidade.pdf. Acesso em: 28 mar. 2020.

ROHR, A. Quem deve investigar e punir um crime on-line: pacotão de segurança. *G1 Tecnologia*, Rio de Janeiro, 14 abr. 2016. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/quem-deve-investigar-e-punir-um-crime-line-pacotao--de-seguranca.html. Acesso em: 28 mar. 2020.

SIRUL, E. What Is the Dark Web? *Experian*, Costa Mesa, 8 abr. 2018. Disponível em: https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/. Acesso em: 28 mar. 2020.

Leituras recomendadas

ABREU, C. N.; EISENSTEIN, E.; ESTEFENON, S. G. B. (org.). *Vivendo esse mundo digital*: impactos na saúde, na educação e nos comportamentos sociais. Porto Alegre: Artmed, 2013. 336 p.

BRASIL. *Lei Nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Casa Civil da Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mar. 2020

BRASIL. Ministério da Ciência e Tecnologia. *Lei Nº 9.609, de 19 de fevereiro de 1998*. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília: Casa Civil da Presidência da República, [1998]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 28 mar. 2020.

BRASIL. Ministério da Justiça. *Decreto-Lei Nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília: Casa Civil da Presidência da República, [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 28 mar. 2020.

BRASIL. Ministério da Justiça. *Lei Nº 7.716, de 5 de janeiro de 1989*. Define os crimes resultantes de preconceito de raça ou de cor. Brasília: Casa Civil da Presidência da República, [1989]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 28 mar. 2020.

BRASIL. Ministério Público Federal. 2ª. Câmara de Coordenação e Revisão. *Crimes cibernéticos*. Brasília: MPF, 2018. 275 p. (Coletânea de artigos, 3). Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 28 mar. 2020.

OLIVEIRA, R. Cinco tipos de crimes digitais devem dominar a internet brasileira em 2019. *Jornal Opção*, Goiânia, 29 set. 2019. https://www.jornalopcao.com.br/reportagens/cinco-tipos-de-crimes-digitais-devem-dominar-a-internet-brasileira-em-2019-212858/. Acesso em: 28 mar. 2020.

POZZEBOM, R. Quais são os crimes virtuais mais comuns? *Oficina da Net*, Santa Cruz do Sul, 30 abr. 2015. Disponível em: https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em: 28 mar. 2020.

SURFACE Web vs Deep Web vs Dark Web vs Shadow Web vs Marianas Web. *Techdracula*, [*S. l.*], 22 dez. 2017. Disponível em: https://techdracula.com/surface-vs-deep-vs-dark-vs-vs-shadow-vs-marianas-web/. Acesso em: 28 mar. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

1 Proteção de dados internacional

O RGPD já está em vigor na UE desde 2018. No Brasil, a Lei Geral de Proteção de Dados (LGPD) já foi aprovada, porém ainda não está vigorando. Essas duas leis se unem a diversas legislações existentes no globo que também visam à proteção de dados dos cidadãos. Afinal, em um mercado cada vez mais digital e sem fronteiras, são necessárias algumas regulações para preservar as premissas básicas da individualidade das pessoas.

Cada país busca identificar as suas particularidades e características ao criar uma lei, porém é normal avaliar as iniciativas em andamento no resto do mundo para identificar o que deu certo e o que deu errado. Atualmente, o RGPD inspira os demais países, pois a não adequação às normas do mercado europeu se reflete no distrato comercial. Esse regulamento exige diversos cuidados, podendo inviabilizar acordos e até mesmo gerar multas aos envolvidos. Ou seja, os países que não se adequarem ao RGPD terão dificuldades para negociar com o bloco europeu.

A seguir, você vai ver como alguns países tratam a proteção de dados em seus territórios (GONZÁLEZ, 2020).

Alemanha

A Alemanha é um dos países pioneiros na regulamentação relativa à privacidade e à proteção de dados. A sua Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz* — BDSG), de 2017, segue os preceitos do RGPD. A BDSG trata dos direitos e deveres de órgãos públicos e privados para as atividades de coleta e processamento de dados. Além disso, há diretrizes específicas que determinam como as empresas devem e podem tratar os dados de seus funcionários.

Austrália

Na Austrália, a lei máxima sobre segurança e proteção de dados é a Lei de Privacidade, de 1988, que governa tanto as instituições do setor público quanto as do setor privado. A lei foi construída com base nos 13 Princípios Australianos de Privacidade (*Australian Privacy Principles* — APPs), que discorrem sobre temas como:

- uso e divulgação de dados;
- direitos do titular dos dados;
- manutenção da qualidade dos dados;
- transparência e anonimidade.

A lei é complementada pelas regulamentações estaduais de privacidade e pelas leis de proteção de dados voltadas para setores específicos.

China

A mais recente regulamentação chinesa sobre privacidade é a lei Tecnologia da Informação: Especificação Sobre Segurança de Informações Pessoais. Conhecida também apenas como "O Padrão", a regulamentação traz diretrizes sobre transparência, direitos do titular e consentimento. Antes de essa lei entrar em vigor, em 2017, o conjunto de regras chinesas sobre o tema era formado por diferentes regulamentações, como:

- Lei Civil da República Popular da China, de 2017;
- Lei de Cibersegurança, de 2017;
- Lei Criminal, de 2015;
- Decisão de Fortalecer a Proteção das Redes de Informações, de 2012;
- Padrão Nacional de Segurança da Tecnologia da Informação, de 2013;
- Lei de Proteção ao Consumidor, de 2014.

Dinamarca

Na Dinamarca, as principais regras sobre o tema estão na Lei Dinamarquesa de Proteção de Dados, de 2018. Anteriormente, a questão era regida pela Lei Dinamarquesa de Processamento de Dados Pessoais, estabelecida em 2000. A lei mais recente serve como complemento e reforço ao RGPD. Dessa forma, a lei dinamarquesa trata de processamento de dados, divulgação de informações pessoais, consentimento, transferência de dados, etc., além de estabelecer multas para casos de violação.

Filipinas

Em 2016, o país implementou a Lei nº 10.173, também conhecida como "Lei de Privacidade de Dados". Redigida quatro anos antes, em 2012, essa é a principal legislação sobre o tema nas Filipinas. A lei determina que, para que possa ser feita a coleta dos dados de um indivíduo, ele tem o direito de saber quem a realiza, com que propósito e com que finalidade. Ele também tem o direito de saber como e por quem os dados serão processados e quem terá acesso a eles.

Finlândia

A Finlândia substituiu sua Lei de Dados Pessoais, de 1999, pela Lei de Proteção de Dados, de 2018, visando a alcançar um maior alinhamento com o RGPD. Contudo, o país ainda tem outras regulamentações sobre proteção de dados específicas para setores do mercado e da indústria, como a Lei de Proteção da Privacidade dos Trabalhadores (Lei nº 759/2004) e o Código de Sociedade da Informação (Lei nº 917/2014), voltado para a confidencialidade de mensagens, *cookies* e telecomunicações.

França

A França é outro exemplo de país da UE que atualizou suas normas de proteção de dados para seguir mais explicitamente o RGPD. O país trocou sua Lei de Proteção de Dados pela Lei 2 de Proteção de Dados. A nova regulamentação estabelece as regras para os agentes de tratamento, determinando também que quaisquer tratamentos de dados devem ser feitos para fins específicos e que apenas os dados fundamentais para tais propósitos podem ser coletados. Além disso, a segunda versão da lei firma o direito do titular de saber quem é o agente de tratamento e qual é o propósito da coleta e do tratamento.

Grécia

A Grécia encontra-se em processo de elaboração de uma nova lei de proteção de dados, que já nascerá alinhada com o RGPD. Enquanto isso, a regulamentação vigente é a Lei nº 2.472/97, que traz regras para controladores e operadores e visa a garantir os princípios da transparência, do tratamento de dados com propósito e da responsabilização dos agentes. O país conta também com duas regulamentações adicionais sobre o tema: o Diretivo de Privacidade Eletrônica (Lei nº 3.471/2006), com normas complementares à lei principal, e o Diretivo de Retenção de Dados (Lei nº 3.917/2011), que trata do armazenamento de dados.

Índia

A Índia ainda não tem uma única lei central sobre proteção e privacidade de dados, e sim diversas leis e normativas que se complementam. Porém, o país publicou a Lei de Proteção de Dados Pessoais em dezembro de 2019, em análise por uma comissão parlamentar até a data da escrita deste capítulo. Enquanto

isso, as normativas mais importantes são a Lei de Tecnologia da Informação (Lei nº 21/2000) e a lista de Regras de Tecnologia da Informação, de 2011. Ambas trazem regras específicas sobre como proteger dados pessoais e outros requerimentos para garantir a privacidade de dados. Há, ainda, conjuntos de regras voltados especificamente para a coleta e o tratamento de dados pessoais nos setores bancário e de saúde.

Indonésia

O conjunto de regras sobre proteção de dados na Indonésia se constitui pela Lei de Informação e Transações Eletrônicas (Lei nº 11/2018) e sua respectiva emenda, pela Lei nº 19/2016 e pelas Regulações nº 82/2012 e nº 20/2016 (Regulação MOCI). Assim como a Índia, a Indonésia também vem trabalhando em uma lei que unifique suas regras sobre o tema: a Lei de Proteção à Privacidade de Dados Pessoais, baseada em grande parte no RGPD. O objetivo é que o texto da lei foque em consentimento, notificação de vazamentos de dados e exclusão de dados, entre outros pontos relacionados.

Islândia

Em 2018, a Islândia substituiu sua antiga Lei de Processamento de Dados Pessoais (Lei nº 77/2000) pela Lei de Proteção de Dados e Processamento de Dados Pessoais (Lei nº 90/2018) — também com o objetivo de adequar suas regras às do RGPD. A lei de 2018 traz diretrizes sobre como obter consentimento do titular, quando e como informar o titular sobre tratamentos realizados com seus dados, como armazenar dados devidamente e como fazer transferências internacionais de dados.

Japão

Desde 2003, a privacidade de dados era regida pela Lei de Proteção de Informações Pessoais (Lei nº 57/2003). Contudo, em 2017, o Japão colocou em prática a Emenda APPI, que traz preceitos básicos para a proteção de dados pessoais. A Emenda APPI traz regras sobre compartilhamento de dados com terceiros, manutenção de informações em bancos de dados e anonimização de dados e vazamentos, estabelecendo diretrizes para proteger os titulares. Devido à nova legislação, o Japão foi incluído na "lista branca" da UE, que reúne países com leis adequadas de proteção de dados.

Malásia

Em 2010, a Malásia colocou em vigor a sua primeira legislação sobre o tema, a Lei de Proteção de Dados Pessoais (Lei nº 709). Ela é construída sobre sete princípios: generalidade, notificação e escolha, divulgação, segurança, retenção, integridade de dados e acesso. Essa lei estabelece que, para que um tratamento de dados seja legítimo e legal, o titular deve receber informações por escrito sobre o propósito da coleta e do tratamento, sobre os seus direitos enquanto titular dos dados e sobre quem terá acesso a esses dados.

Nova Zelândia

A Nova Zelândia controla a privacidade de dados por meio dos 12 Princípios da Privacidade de Informação, estabelecidos em 1993 na Lei de Privacidade do país. Os princípios são focados principalmente em questões como propósito da coleta de dados, formas de armazenamento e acesso, limitações do tratamento e divulgação de dados pessoais. O país também tem legislações de privacidade voltadas para setores específicos, incluindo crédito, saúde e telecomunicações.

Saiba mais

Até a data da escrita deste capítulo, circulava pelo governo neozelandês a Lei de Privacidade de 2018 — que, quando aprovada, substituirá a legislação anterior. As mudanças mais significativas incluem reporte mandatório sobre vazamentos, notificações de *compliance* e fortalecimento de transferências internacionais de dados. Outra diretriz importante da nova legislação é o direito do titular de fazer uma reclamação sobre a legitimidade de uma coleta ou de um tratamento de dados, que subsequentemente será investigada.

Algumas considerações

Como você viu, a questão da privacidade de dados não é novidade. Afinal, diversos países já possuem legislações a respeito desse tema. O que fica cada vez mais claro é que o RGPD é a espinha dorsal das legislações que têm surgido. Ele indica o mínimo necessário para que haja cuidado com os dados individuais durante as transações comerciais (PINHEIRO, 2018).

A seguir, veja alguns aspectos comuns às diferentes leis nacionais (PINHEIRO, 2018):

- o cuidado que as empresas precisam ter com os dados dos cidadãos;
- a penalidade a que as empresas estão expostas caso haja algum tipo de vazamento;
- a noção de que o usuário é o dono dos seus dados, de modo que precisa saber o pode ser feito com o dado que disponibiliza durante determinada transação.

Na Figura 1, veja o grau de aderência dos países às leis de proteção de dados. Como você pode notar, a Argentina e o Uruguai são os países sul-americanos mais aderentes às leis de proteção de dados. Destaca-se também a Guiana Francesa, país que está sujeito às leis francesas e, por consequência, adere totalmente à legislação europeia (SERPRO, 2020).

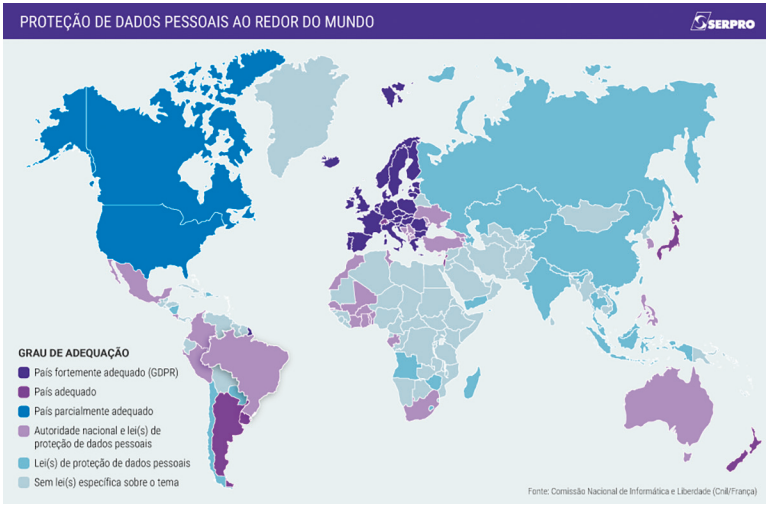

Figura 1. Adequação dos países à proteção de dados.

Fonte: Serpro (2020, documento *on-line*).

2 RGPD

No dia 27 de abril de 2016, foi consolidado o RGPD. Ele discorre sobre a proteção das pessoas físicas no que diz respeito ao correto tratamento dos dados pessoais e à utilização desses dados pelos mercados, o que implica considerar o livre fluxo de dados (*free data flow*).

Ficou acordado que a lei entraria efetivamente em vigor após dois anos, quando seriam colocadas em prática as penalidades pertinentes. Até então, as penalidades não seriam aplicadas, pois o momento seria de transição e adequação de todas as partes interessadas. Conforme Pinheiro (2018), a implementação do RGPD gerou um efeito dominó, tendo em vista que todos os países que não pertencem à UE enfrentariam algumas barreiras e até mesmo sofreriam impactos financeiros caso não aderissem à legislação da zona do euro. Em um mundo cada vez mais competitivo, os países tiveram de se adaptar às novas exigências para fazer negócios com esse mercado tão importante.

O objetivo do RGPD (UNIÃO EUROPEIA, 2016) é contribuir para a obtenção de um espaço de liberdade, segurança e justiça. Além disso, o RGPD visa à união econômica para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e o bem-estar das pessoas físicas. Esse regulamento ainda tem o intuito de assegurar um nível coerente de proteção das pessoas físicas no âmbito da UE e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno. A ideia é garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo.

Fique atento

São impostas obrigações e responsabilidades iguais aos controladores e processadores. O RGPD busca assegurar um controle coerente do tratamento dos dados pessoais, possibilitando a cooperação efetiva entre as autoridades de controle dos diferentes Estados-membros.

Vale a pena destacar que, apesar de essa lei reforçar a importância fundamental das informações dos cidadãos, ela acaba apenas complementando diversas outras leis nacionais existentes no bloco europeu, como a Carta dos Direitos Fundamentais da UE e o Tratado sobre o Funcionamento da UE. Nesse sentido, é possível fazer um paralelo com o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), ambos do Brasil (PINHEIRO, 2018).

No entanto, essa regulamentação se faz necessária no sentido de esclarecer conceitos ambíguos e não factíveis. Foi nesse ponto que o RGPD inovou em relação às demais leis, buscando também padronizar as normas relativas aos atributos qualitativos cobrados e penalizados.

No Quadro 1, a seguir, veja como o RGPD põe em prática os itens de conformidade relativos à proteção de dados. Note que esse regulamento busca esclarecer a necessidade do cuidado com os dados e exemplificar os procedimentos adequados, indicando como os dados devem ser tratados, protegidos e disponibilizados.

Quadro 1. Itens de conformidade em relação ao regime europeu

Item de conformidade	Regime europeu (RGPD)
Definição e distinção do que são dados pessoais e dados sensíveis. Tal conceituação busca delimitar os direitos e as informações protegidas pelo ordenamento jurídico.	Define que dado pessoal é qualquer informação que identifique ou torne identificável a pessoa natural. Já dados sensíveis são dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações a organizações quaisquer. O RGPD também faz considerações acerca dos dados genéticos, biométricos e relativos à saúde.
Obrigatoriedade do consentimento do usuário para a coleta de informações e limitação do tratamento do dado conforme finalidade.	Prevê a necessidade de uso do dado conforme a finalidade apontada. Traz exceções de tratamento por motivo de interesse público, segurança e saúde.

(Continua)

(Continuação)

Quadro 1. Itens de conformidade em relação ao regime europeu

Item de conformidade	Regime europeu (RGPD)
Distinção entre titularidade e responsabilidade sobre os dados, assim como delimitação das funções e responsabilidades assumidas no tratamento de dados.	Titular é a pessoa natural a quem se referem os dados que são objeto de tratamento; por outro lado, o responsável é a pessoa física ou jurídica, de direito público ou privado, que realiza decisões sobre o tratamento de dados. O controlador é quem realiza as decisões acerca do tratamento de dados; o processador, quem efetua o tratamento dos dados. Ambos são responsáveis pelo tratamento dos dados.
Indicação de um encarregado pela comunicação entre os agentes, titulares e órgãos competentes.	Aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados (DPO).
Aplicação de mecanismos e práticas pautadas no livre acesso à informação e na transparência entre os usuários e as organizações.	Os titulares têm direito a informações claras e acessíveis do início ao fim do tratamento do dado, podendo revogar o consentimento a qualquer momento.
Aplicação de medidas de segurança e dever de reportar.	As empresas devem criar medidas — como pseudonimização e encriptação de dados — para garantir a segurança de forma preventiva. No caso de qualquer incidente, a notificação às autoridades deve ser imediata.
Possibilidade de alteração e exclusão do dado pessoal.	Os titulares dos dados podem alterar ou excluir seus dados.
Aplicação de sanções no caso de descumprimento das regras.	Prevê a aplicação de sanções gradativas e multas administrativas, que podem chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa.
Criação de um órgão competente para fiscalizar e zelar pela proteção de dados pessoais e pela privacidade.	Possui um órgão de controle e fiscalização de proteção de dados pessoais por Estado (28) e aplica o princípio do balcão único.

Fonte: Adaptado de Pinheiro (2018).

3 Leis de proteção de dados nas Américas

Nas Américas, conforme Lemos *et al*. (2018), a legislação de proteção dos dados vem ganhando maturidade e mais protagonismo. Isso ocorre tanto devido a escândalos de vazamento de dados (como no caso do Banco Inter, que na época perdeu seu certificado digital) quanto pelo uso de informações para eleições (como no caso da Cambridge Analytica e do Facebook nas eleições dos Estados Unidos em 2016). A seguir, você vai ver como alguns países da América tratam a proteção de dados em seus territórios (GONZÁLEZ, 2020).

Argentina

A Lei de Proteção de Dados da Argentina (Lei nº 25.326) estabelece que a coleta de dados só pode ser feita mediante o consentimento do usuário. A lei, que se aplica a qualquer pessoa ou entidade que lida com dados pessoais no país, diz ainda que o titular dos dados (o indivíduo a quem as informações se referem) tem o direito de acessar, corrigir, deletar e solicitar a exclusão de seus dados. Porém, para deixar as regras de proteção de dados do país mais alinhadas às tendências mundiais estabelecidas pelo RGPD, a Argentina vem trabalhando em uma nova lei sobre o tema, que terá a legislação atual como base e irá ainda mais além — determinando, por exemplo, uma abordagem mais completa e obrigações mais rígidas.

Brasil

No Brasil, há a LGPD — que foi aprovada, porém, até a data de escrita deste capítulo, ainda não estava em vigor, mas já vem promovendo mudanças significativas na forma como as empresas coletam e tratam dados. O direito à privacidade já havia sido estabelecido pelo art. 5 da Constituição Federal de 1988 e pelo Código de Proteção ao Consumidor, instituído em 1990. Outra importante legislação sobre o tema no País é o Marco Civil da Internet, sancionado em 2014. Voltado inteiramente para o uso da internet no País, o Marco Civil traz princípios, garantias, direitos e deveres dos usuários da rede, além de diretrizes sobre como o Estado deve atuar. Ao lado da privacidade, alguns dos outros principais temas abordados são:

- neutralidade da rede;
- retenção de dados e funções sociais da internet, como liberdade de expressão;
- transmissão de conhecimento e responsabilidade civil.

Canadá

O país conta com um total de 28 regulamentações — entre leis provinciais e federais — que tratam das questões de privacidade e proteção de dados. A legislação nacional referente a isso é a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (*Personal Information Protection and Electronic Documents Act* — Pipeda). Válida para todas as províncias do Canadá, a Pipeda apresenta diretrizes referentes à coleta, ao tratamento e à divulgação de dados pessoais coletados por empresas durante o exercício de suas atividades comerciais. Além disso, discorre sobre as transferências internacionais e inter-regionais de dados pessoais. Como complemento a ela, há legislações similares aplicáveis em Alberta, Colúmbia Britânica e Quebec. Estabelecida em 2000, a Pipeda opera com base em 10 princípios de boas práticas a serem seguidos pelas empresas (bastante similares às bases da LGPD brasileira). São elas:

1. as empresas são responsáveis pelos dados pessoais que coletaram e que usam;
2. é preciso identificar claramente os propósitos por trás de uma coleta de dados;
3. é preciso ter o consentimento do titular para coleta, uso e compartilhamento de seus dados, salvo exceções previstas por lei;
4. podem ser coletados somente os dados necessários dentro do propósito informado;
5. os dados solicitados podem ser usados, divulgados e mantidos pela empresa apenas da maneira informada e enquanto cumprirem os propósitos;
6. as informações pessoais devem ser verídicas e mantidas atualizadas;
7. os dados devem ser protegidos por medidas adequadas, de acordo com a sensibilidade das informações;
8. a organização precisa fornecer amplamente informações claras e detalhadas sobre suas políticas e práticas de segurança e proteção de dados;
9. o titular dos dados tem o direito de receber informações sobre a existência de tratamentos de suas informações, assim como de questionar se seus dados são verídicos e estão completos;
10. o titular dos dados tem o direito de questionar as organizações que tratam e coletam suas informações pessoais, dentro dos nove princípios anteriores.

Colômbia

Na Colômbia, a questão da privacidade e da proteção de dados é regida por quatro regulamentações: o Decreto nº 1.377/2013, a Lei nº 1.581/2012, a Lei nº 1.273/2009 e a Lei nº 1.266/2008. O Decreto nº 1.377/2013 aborda o consentimento do titular, as transferências internacionais de dados e as políticas de processamento de dados pessoais. Enquanto isso, a Lei nº 1.581/2012 estabelece o direito de cada indivíduo de determinar como seus dados serão coletados, armazenados, usados, processados e transferidos — além de regulamentar os direitos à privacidade na coleta e no processamento de dados pessoais. A Lei nº 1.273/2009, por sua vez, traz diretrizes sobre crimes cibernéticos e estabelece que roubar, vender ou comprar dados pessoais é uma atividade criminosa. Finalmente, a Lei nº 1.266/2008 discorre sobre a privacidade de dados no que tange a dados comerciais e financeiros.

Estados Unidos

Os Estados Unidos não têm apenas uma lei que governe a privacidade de dados, e sim diversas legislações específicas para diferentes setores ou vigentes em determinados estados. Há cerca de 20 leis voltadas para um único setor ou indústria em âmbito nacional, além de outras cem legislações estaduais de privacidade — o estado da Califórnia é o "lar" de 25 delas. A principal lei californiana de privacidade é a Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act* — CCPA), que garante aos consumidores quatro direitos básicos sobre seus dados pessoais: de serem notificados, de terem acesso, de poderem optar (ou não) por uma coleta de dados e de terem acesso igualitário a serviços.

Todas as empresas que coletam e/ou tratam dados de cidadãos californianos precisam seguir a CCPA, e não apenas aquelas com sede no estado. Nacionalmente falando, as mais importantes regulamentações são a Lei de Privacidade, de 1974, a Lei de Proteção à Privacidade, de 1980, a Lei Gramm–Leach–Bliley, de 1999, a Lei de Portabilidade e Responsabilidade dos Seguros de Saúde, de 1999, e a Lei de Relatório de Crédito Justo, de 2018. Além disso, os Estados Unidos têm alguns acordos especiais de proteção à privacidade com a UE e a Suíça.

México

A questão da privacidade de dados no México é regida pela Lei Federal de Proteção de Dados Pessoais em Poder de Particulares — ou seja, estão em jogo dados coletados e tratados por empresas privadas. A lei foi estabelecida em 2010. Essas organizações também são governadas pelas diretrizes da lista de Regulamentações da Lei Federal de Proteção de Dados Pessoais em Poder de Particulares, instituída em 2011, pelas Orientações de Notificações de Privacidade, de 2013, e pelos Parâmetros de Autorregulamentação, de 2014. Para gerenciar todas essas regras, garantir a devida implementação e administrar penalidades, o México conta com o Instituto Federal de Acesso à Informação e Proteção de Dados (Ifai).

Algumas considerações

Da mesma forma que os demais países, conforme Pinheiro (2018), aqueles localizados no continente americano têm reforçado o cuidado com os dados dos cidadãos. Além disso, têm buscado aplicar a devida penalidade quando as empresas expõem informações de maneira indevida. Ademais, nos países americanos, também é consenso que os usuários têm o direito de saber o que será feito com as suas informações.

Como você viu ao longo deste capítulo, a proteção dos dados pessoais é essencial em um ambiente comercial cada vez mais complexo e dinâmico, em que as fronteiras entre o certo e o errado precisam ser claras para viabilizar uma sociedade melhor.

Referências

GONZÁLEZ, M. *Conheça o cenário das leis de proteção de dados ao redor do mundo*. 2020. Disponível em: https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/. Acesso em: 13 abr. 2020.

LEMOS, R. *et al. GDPR*: a nova legislação de proteção de dados pessoais da Europa. 2018. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/gdpr-dados-pessoais-europa-25052018. Acesso em: 16 abr. 2020.

PINHEIRO, P. P. *Proteção de dados pessoais*: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018.

SERPRO. *Em que "estágio" estamos?* Confira o mapa da proteção de dados pessoais no mundo. 2020. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 13 abr. 2020.

UNIÃO EUROPEIA. *Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.* Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: https://eur-lex. europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POR&toc=OJ:L: 2016:119:FULL. Acesso em: 13 abr. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Marco civil da internet

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Reconhecer os aspectos que gerenciam o marco civil da internet no Brasil.
- Analisar os princípios de neutralidade, privacidade na internet e registro de acessos.
- Relacionar a liberdade de expressão dos usuários com a responsabilidade dos provedores de serviços *web*.

Introdução

Neste capítulo, você vai estudar os principais elementos propostos pelo marco civil da internet. Assim que o marco civil da internet foi instituído, em 23 de abril de 2014, por meio da Lei nº. 12.965, foram estabelecidas as diretrizes para o uso da internet no Brasil, considerando os princípios, as garantias, os direitos e os deveres das partes.

O marco civil da internet é muito importante, tanto que é considerado a "constituição da internet" no Brasil. Como você vai ver, muitos elementos de interesse de toda a comunidade da internet foram considerados nele, como: neutralidade, privacidade e liberdade de expressão.

1 Trajetória do marco civil da internet

O marco civil da internet foi desenvolvido de forma inédita para o Brasil. Afinal, ele contou com a efetiva participação da sociedade civil por meio de cerca de 2 mil contribuições formais e informais. Assim, a Lei nº. 12.965/2014 foi construída de modo coletivo. A participação em massa da comunidade civil foi de grande contribuição para o projeto como um todo.

Fique atento

Em outros países, é possível observar a constante participação da sociedade civil na construção de leis, mas no Brasil isso não é comum, por isso o destaque do marco civil da internet.

No Brasil, todo projeto de lei passa por diversos trâmites para ser aprovado. Muitas vezes, tais trâmites envolvem interesses políticos, que nem sempre condizem com os interesses de quem de fato será afetado pela lei. Muitas votações e ajustes podem ocorrer tanto na Câmara dos Deputados quanto no Senado. Além disso, é claro, pode haver vetos presidenciais. Esse processo pode durar meses ou até anos, como ocorreu no caso das discussões que levaram à aprovação do marco civil da internet. No Quadro 1, a seguir, veja os principais pontos do marco civil da internet e a evolução nas discussões: do projeto de lei até a versão final.

Quadro 1. Evolução da criação do marco civil da internet

Temas	2011 (texto original)	2012 (proposta do relator)	2014 (proposta aprovada)
Internet livre (neutralidade da rede)	Os provedores de internet devem dar tratamento igualitário de acesso e velocidade a todos os *sites*, a não ser por aspectos técnicos.	A neutralidade poderá ser rompida para priorizar emergências (segurança pública, etc.). A regulamentação ocorrerá por decreto presidencial, após consulta ao Comitê Gestor da Internet (CGI).	Além do CGI, a Agência Nacional de Telecomunicações (Anatel) deverá ser consultada. A regulamentação das exceções será feita por determinação constitucional de "fiel execução da lei".

(Continua)

(Continuação)

Quadro 1. Evolução da criação do marco civil da internet

Temas	2011 (texto original)	2012 (proposta do relator)	2014 (proposta aprovada)
Privacidade	Os provedores devem guardar o registro de acesso geral à internet, mas não podem manter os registros específicos de acesso a *sites*.	Permanece igual.	*Sites* na internet com fins lucrativos, como Google e Facebook, devem manter o registro de acesso por seis meses. Não podem guardar dados pessoais que extrapolem o serviço.
Dados pessoais e comunicações na internet	Os registros de acesso à internet devem prezar pela intimidade, pela vida privada e pela honra. Poderão ser fornecidos somente após ordem judicial.	Permanece igual.	Dados pessoais e conteúdo de comunicações privadas são incluídos no texto, o que permite que autoridades tenham acesso a eles via ação judicial.
Liberdade de expressão *versus* conteúdo ilegal/ ofensivo	Provedores não são punidos por publicações de terceiros. Já *sites* e aplicações são responsabilizados se não acatarem a Justiça.	A viabilidade técnica para serviços retirarem publicações após ordem judicial conta. O conteúdo pode ser substituído pela ordem judicial sobre a retirada.	Se o conteúdo tiver imagens de nudez ou de atos sexuais do ofendido, o serviço deverá retirá-lo após notificação, sem necessidade de ação judicial.

(Continua)

(Continuação)

Quadro 1. Evolução da criação do marco civil da internet

Temas	2011 (texto original)	2012 (proposta do relator)	2014 (proposta aprovada)
Monitoramento na *web*	Não previa qualquer forma de coleta de dados pessoais na internet.	Dados dos usuários poderão ser utilizados para as finalidades que fundamentam a oferta de um serviço e seu uso deverá ser especificado. O usuário pode pedir a exclusão dos seus dados.	A utilização deverá ser explicitada já no contrato. Serão nulos os contratos que não permitam ações na Justiça brasileira. O Código do Consumidor passa a valer nessa relação.

Fonte: Adaptado de Gomes (2015).

O projeto de lei do marco civil da internet teve início em 2009, mas só entrou em pauta de votação em outubro de 2013, por conta de um pedido presidencial denominado "urgência constitucional". A partir de agora, você vai conhecer todo o trâmite realizado desde as discussões iniciais até a votação e a aprovação da lei. O CGI, em sua terceira reunião ordinária, que ocorreu em 2009, aprovou a Resolução CGI.br/RES/2009/003/P — Princípios para a Governança e Uso da Internet no Brasil, chamado de "decálogo do CGI.br". Esse foi um dos documentos inspiradores da criação do marco civil da internet (COMITE, 2009).

A Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL/MJ), em parceria com a Escola de Direito do Rio de Janeiro, da Fundação Getúlio Vargas (FGV Direito Rio), lançou o projeto para a construção colaborativa de um marco civil da internet no Brasil. Por sua vez, o Ministério da Cultura "concedeu" a sua plataforma para os debates. Durante a primeira fase, entre 29 de outubro e 17 de dezembro de 2009, foram mais de 800 contribuições entre comentários, *e-mails* e referências propositivas em *sites* (MARCO..., 2009).

A partir dos debates e das sugestões da primeira fase, criou-se a minuta do anteprojeto do marco civil, que voltou a ser discutida, em uma segunda fase, por meio de um processo de construção colaborativa com participação da sociedade. Os debates públicos dessa segunda fase foram iniciados em 8 de abril e encerrados em 30 de maio de 2010 (BRASIL, 2010). Em junho de 2010, ocorreu a primeira decisão judicial que menciona a iniciativa do marco civil. A desembargadora Letícia de Faria Sardas, da 20ª Câmara Cível do Tribunal de Justiça do Rio de Janeiro (TJRJ), no Agravo de Instrumento (AI) nº. 0013822-08.2010.8.19.0000, afirmou o seguinte: "O Marco Civil da Internet no Brasil, submetido à segunda consulta pública, estabelece os direitos dos cidadãos brasileiros na internet. [...] Ponto muito importante e positivo do Marco Civil é a forma como propõe regular os direitos e deveres relativos aos vários dados gerados pelo usuário quando navega" (RIO DE JANEIRO, 2010).

O projeto de lei do marco civil da internet — Projeto de Lei nº. 2.126, de 2011 — foi então apresentado à Câmara dos Deputados pelo Poder Executivo. Tal projeto estabeleceu "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2011b). Uma comissão especial foi reunida pela Câmara para analisar a proposta de criação do marco civil da internet em 26 de novembro de 2011. A instalação da comissão ocorreu no dia 28 de março de 2012. Os deputados João Arruda e Manoel Junior foram eleitos, respectivamente, presidente e primeiro vice-presidente do colegiado. Já o relator escolhido foi o deputado Alessandro Molon.

Por meio do portal e-Democracia, da Câmara, ocorreu um amplo debate virtual sobre princípios, garantias, direitos e deveres relativos ao uso da internet no Brasil. As contribuições desse debate auxiliaram os trabalhos dos deputados envolvidos com o tema (BRASIL, 2011a; BRASIL, 2012). No dia 20 de julho de 2012, os conselheiros presentes na reunião ordinária do CGI, por unanimidade, declararam amplo apoio ao parecer final do deputado federal Alessandro Molon e à aprovação de tal parecer na comissão especial da Câmara dos Deputados (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

O cientista britânico Tim Berners-Lee, criador da World Wide Web (WWW), declarou apoio ao projeto do marco civil e incentivou os brasileiros a pressionarem para que a votação começasse logo. Segundo ele, o Brasil estava à frente dos demais países porque a proposta partia da perspectiva de direitos humanos (MATURANA, 2013). Além disso, naquele período, ocorreu um fato de repercussão mundial quando o norte-americano Edward Snowden, um analista de sistemas que trabalhou na Central Intelligence Agency (CIA) e na National Security Agency (NSA), tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA, inclusive

detalhes de como a agência americana espionava a então presidente da República Dilma Rousseff. Além disso, foram divulgadas importantes transações milionárias envolvendo o leilão da área de exploração de petróleo do pré-sal (ENTENDA..., 2014).

O governo brasileiro precisava dar uma resposta ao mundo em relação à proteção dos dados de seus cidadãos e, principalmente, de membros do Congresso Nacional. Assim, a proposta do marco civil da internet, que estava na Câmara, passou a tramitar em regime de urgência constitucional (GONÇALVES, 2014).

Saiba mais

O presidente da República pode solicitar que projetos de lei de sua autoria tramitem em regime de urgência (art. 65 da Constituição). É a chamada "urgência constitucional". Nesse caso, a Câmara tem 45 dias para votar a matéria, e o Senado, mais 45 dias para apreciá-la. Se nesse prazo os parlamentares não concluírem a votação, o projeto passará a trancar a pauta de deliberações da casa em que estiver tramitando, ou seja, nada poderá ser votado antes que o projeto em urgência constitucional seja apreciado (AGÊNCIA BRASIL DE NOTÍCIAS, 2004).

A então presidente Dilma Rousseff defendeu, em 24 de setembro de 2013, na 68ª Assembleia Geral das Nações Unidas (ONU), o estabelecimento de um marco civil multilateral para a governança e o uso da internet, bem como medidas que garantissem a efetiva proteção dos dados. Dilma afirmou que as revelações sobre as atividades de uma rede global de espionagem eletrônica provocaram indignação e repúdio em amplos setores da opinião pública mundial. No Brasil, a situação foi ainda mais grave, pois dados pessoais de cidadãos e da própria presidente da República foram indiscriminadamente objeto de interceptação (PASSARINHO, 2013).

O relator do marco civil da internet, deputado Alessandro Molon, apresentou uma nova versão do texto final do seu parecer a pedido de Dilma. No novo texto, ele incluiu regras para tentar coibir a espionagem de dados de usuários brasileiros por empresas de internet estrangeiras. O novo texto condicionou a uma nova regulamentação, por meio de decreto do governo, a obrigação dos provedores de internet que exercem atividades no Brasil de guardarem os seus dados em *data centers* no País (BRASIL, 2011c).

O Plenário da Câmara dos Deputados aprovou o marco civil da internet no dia 25 de março de 2014. A partir de 26 de março de 2014, o projeto passou a tramitar no Senado Federal (Projeto de Lei da Câmara nº. 21, de 2014). O marco civil da internet foi apreciado simultaneamente pelas comissões de ciência, tecnologia, inovação, comunicação e informática; de meio ambiente, defesa do consumidor e fiscalização e controle; e de constituição, justiça e cidadania. Ele pôde receber emendas somente nas comissões de ciência, tecnologia, inovação, comunicação e informática, pelo prazo único de cinco dias úteis (BRASIL, 2014b).

O projeto que regulamenta a internet brasileira recebeu 41 emendas de senadores. Acabado o prazo para a apresentação de emendas, os relatores do projeto nas comissões estudaram o assunto e emitiram os seus votos, levando em conta as sugestões dos colegas. O projeto entrou em votação no Senado e foi finalmente aprovado como Lei nº. 12.965 em 23 de abril de 2014. A aprovação ocorreu na véspera de um importante evento sobre internet, o NETmundial — Encontro Multissetorial Global Sobre o Futuro da Governança da Internet, que aconteceu nos dias 23 e 24 de abril de 2014, em São Paulo. Esse evento teve como foco a elaboração de princípios de governança da internet e a proposta de um roteiro para a evolução futura desse ecossistema.

O marco civil da internet foi apresentado aos participantes durante o encontro. Embora não tenha agradado inteiramente a todos os representantes das dezenas de países participantes — e esteja longe de ser um documento perfeito, como reconheceu o presidente do comitê executivo do encontro, o brasileiro Virgílio Almeida —, o texto final apresentado no NETmundial resume as contribuições de diferentes regiões e de diferentes interessados na rede mundial de computadores. Sobretudo, tal texto reafirma importantes princípios para a gestão e o uso da rede mundial de computadores (A GESTÃO..., 2014).

Na ocasião, Vint Cerf, inventor do protocolo TCP/IP e considerado o "pai da internet", opinou sobre o marco civil. Veja o que ele disse: "o grande teste será agora, após a aprovação. Quão efetiva será essa legislação? Como ela será implementada? Muitos especialistas, entre os quais me incluo, querem saber como e se o Marco Civil vai realmente funcionar como esperado" (HONORATO, 2014).

O marco civil da internet sinalizou que o acesso à internet é um instrumento essencial ao exercício da cidadania e da liberdade de expressão, elevando-o ao patamar de garantia constitucional. O marco civil da internet foi publicado na edição de 24 de abril de 2014 do Diário Oficial da União (BRASIL, 2014a).

2 Neutralidade, privacidade e registro de acessos

A neutralidade de rede está prevista no art. 9º da Lei nº. 12.965/2014. A neutralidade, nesse contexto, diz respeito sobretudo ao acesso igualitário à internet, como expressa o dispositivo: "O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação" (BRASIL, 2014a).

Para garantir a igualdade na rede, a lei buscou proibir que os provedores de conexão restrinjam o acesso dos internautas a determinadas aplicações. Para tanto, definiu uma imposição legal: os provedores/operadoras não podem estabelecer pacotes de preços diferenciados para o acesso exclusivo a determinados *sites*. Seria o caso, por exemplo, de planos que só acessam redes sociais (MACHADO, 2014). Ademais, os usuários, ao contratarem um plano de internet, devem pagar apenas pela velocidade contratada, não podendo haver limitação de acesso a determinados *sites* ou mesmo serviços.

A lei foi taxativa ao proibir atos que violem o princípio da neutralidade de rede, como o estímulo ao acesso a determinadas aplicações. Porém, a própria lei prevê as possíveis exceções à regra, que serão regulamentadas por meio de decreto e somente após consulta prévia ao CGI e à Anatel. Tais exceções dizem respeito apenas aos "requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações" e à priorização dos serviços de emergência, nos termos do art. 9º, § 1º, da Lei nº. 12.965/2014. Veja (BRASIL, 2014a):

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
> I — requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
> II — priorização de serviços de emergência.

Outra questão prevista na lei se refere à proibição de os provedores utilizarem comercialmente dados pessoais de seus usuários, exceto se estes consentirem expressamente. Assim, se anteriormente os dados dos internautas eram negociados livremente pelos provedores, depois da aprovação do marco civil, foi proibida a utilização do histórico de navegação para fins comerciais. Isso é importante especialmente para limitar as enxurradas de anúncios publicitários personalizados e com temáticas de assuntos pesquisados anteriormente em *sites* de busca (MACHADO, 2014).

Dessa forma, conforme previsão do art. 7º, VII e X, do marco civil da internet, para que os provedores possam utilizar os dados pessoais de um internauta, este deve consentir "livre, expresso e informado". Ademais, tal autorização pode ser revogada a qualquer momento pelo usuário dos serviços de internet, exigindo-se a "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet", ressalvando apenas as guardas obrigatórias previstas na lei.

Em relação às previsões legais acerca da obrigatoriedade de armazenamento e disponibilização dos registros de conexão e de acesso a aplicações de internet, além dos dados pessoais e comunicações privadas, os provedores não podem se abster da preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (art. 10 da Lei nº. 12.965/2014). As empresas só estarão obrigadas a fornecer tais informações dos usuários a partir de determinação judicial.

No entanto, o art. 10, § 3º, do marco civil possibilita que as autoridades administrativas requisitem dados cadastrais que informem a qualificação pessoal, a filiação e o endereço de determinado usuário. Ora, tal regulamentação deixa uma cláusula aberta ao mencionar apenas a "autoridade administrativa", sem especificá-la. Assim, há insegurança quanto ao real sigilo das informações pessoais dos usuários. Veja o que a lei afirma (BRASIL, 2014a):

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. [...]
> § 3º O disposto no *caput* não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

Além disso, o marco civil da internet estabeleceu que todos os provedores de internet devem manter os registros de conexão por um ano (art. 13). Já os registros de acesso a aplicações devem ser mantidos por seis meses (art. 15). Tal regra vale inclusive para empresas estrangeiras que operam no Brasil. Assim, no caso de descumprimento, incidirão sanções que podem ser aplicadas isolada ou cumulativamente. Entre tais sanções, você pode considerar: advertência; multa de até 10% do faturamento do grupo econômico no Brasil; suspensão temporária ou proibição do exercício das atividades (MACHADO, 2014).

Contudo, alguns pontos devem ser observados quanto a essa regulamentação. Primeiramente, o fato de os provedores de internet terem de armazenar por um período de tempo considerável os registros de conexão e de acesso a aplicações desencadeia um custo extra às empresas. Estas, por conseguinte, poderão repassar essa despesa aos consumidores. Além disso, outro ponto que merece cuidado se refere ao efetivo sigilo e à inviolabilidade das informações pessoais dos internautas. Afinal, são corriqueiras as notícias relativas a *sites* públicos e privados invadidos que têm seus dados furtados.

Saiba mais

A TV Senado exibiu um documentário sobre o marco civil da internet. O vídeo está disponível no YouTube e no *site* do Observatório do Marco Civil da Internet. Faça uma busca *on-line* e confira!

3 A liberdade de expressão dos usuários e a responsabilidade dos provedores

A liberdade de expressão é um ponto muito importante contemplado pelo marco civil da internet. Como você sabe, a internet oferece um espaço eclético para qualquer tipo de manifestação. Além disso, por meio dela, os usuários podem expressar a sua opinião sobre qualquer tema. Contudo, nem todas as manifestações são realizadas de forma positiva (CRUZ, 2019).

Com o marco civil da internet, o direito dos usuários de se expressarem livremente continua garantido. No entanto, assim como acontece no mundo físico, agora os indivíduos podem ser responsabilizados por suas ações na internet. Ao contrário do que muitos ainda podem imaginar, a internet não

é uma terra sem lei, em que você pode ofender quem quer que seja ou tecer comentários preconceituosos sem que lhe seja imposta nenhuma punição (CRUZ, 2019).

O marco civil da internet considera a responsabilidade civil dos provedores. A fim de assegurar a liberdade de expressão e impedir a censura, a Lei nº. 12.965/2014 estabelece, em seu art. 19, que os provedores de aplicações de internet só poderão ser responsabilizados civilmente por danos decorrentes de conteúdos gerados por terceiros na hipótese de que, mesmo após determinação judicial, não tomem as medidas pertinentes. Ou seja, os provedores só serão obrigados a retirar determinado conteúdo publicado na rede mediante ordem judicial; se não o fizerem no prazo assinalado, eles poderão ser responsabilizados (BRASIL, 2014a).

Em consonância com o que já vinha sendo julgado nos tribunais, o art. 18 da lei normatiza o entendimento de que as empresas de conexão de internet não serão responsabilizadas civilmente por danos gerados por conteúdos produzidos por terceiros. Isso se mostra prudente, visto a ingerência das empresas frente ao teor das publicações.

A partir do marco civil da internet, a retirada de conteúdos da rede necessariamente passa pelo crivo judicial. Porém, a lei não se omitiu quanto aos meios de facilitação de tal medida, conforme o art. 19, § 4º. Tal dispositivo prevê a possibilidade de se antecipar, total ou parcialmente, os efeitos da tutela pretendida. Isso pode ser feito desde que haja prova inequívoca do fato, verossimilhança da alegação do autor, receio fundado de dano irreparável ou de difícil reparação e, o que é inovador, desde que seja observado o "interesse da coletividade na disponibilização do conteúdo na internet" (BRASIL, 2014a).

Entende-se que "interesse da coletividade na disponibilização do conteúdo na internet" na verdade foi a forma encontrada pelo legislador para garantir que o magistrado somente conceda a medida antecipatória caso observe que a sua concessão não causará prejuízos ao interesse da coletividade na informação (MACHADO, 2014).

No entanto, a lei é clara ao ressalvar que, em casos de nudez e sexo, os provedores são obrigados a retirar o conteúdo ofensivo após mero pedido extrajudicial da vítima, não sendo necessária intervenção judicial (art. 21). Isso se mostra plausível diante da velocidade com que esse tipo de conteúdo se espalha, de modo que é necessária máxima urgência na sua retirada da rede, a fim de evitar o agravamento do dano. Como você deve imaginar, o Judiciário não conseguiria propiciar a celeridade exigível para esses casos.

Além disso, considere o que afirma o art. 19, § 3º (BRASIL, 2014a):

> § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

Com isso, garante-se às vítimas todas as peculiaridades inerentes aos juizados, como a desnecessidade de patrocínio de advogado para o ingresso com a ação, a isenção de custas em primeiro grau, além da celeridade e da informalidade do rito. Mas, é claro, em ações cumuladas com reparação de danos, os valores pretendidos com a reparação não podem ultrapassar o limite de alçada dos juizados, inclusive no que tange à necessidade do patrocínio de advogado (MACHADO, 2014).

Como você viu, muitos esforços foram feitos para que o marco civil da internet pudesse garantir a liberdade de expressão dos usuários, bem como a responsabilidade dos provedores de serviços *web*. O marco civil da internet trouxe uma série de direitos e deveres para todos os envolvidos com o uso da internet, tanto usuários quanto provedores. Por isso, é fundamental que todo profissional de Tecnologia da Informação (TI) conheça os pontos previstos na lei, a fim de garantir que as empresas adotem mecanismos, regras e técnicas para cumpri-los.

Saiba mais

Você sabia que a constituição da Islândia foi elaborada de forma colaborativa por meio da internet? Nas redes sociais e no *site* oficial do conselho criado para a redação do documento, os cidadãos sugeriram itens e opinaram a respeito de mudanças. Para saber mais sobre essa experiência, faça uma pesquisa na internet (SALES, 2013).

Referências

A GESTÃO da Internet. *O Estado de S.Paulo*, São Paulo, 26 abr. 2014. Disponível em: https://opiniao.estadao.com.br/noticias/geral,a-gestao-da-internet-imp-,1158813. Acesso em: 21 abr. 2020.

AGÊNCIA BRASIL DE NOTÍCIAS. Urgência constitucional. *Câmara dos Deputados*, Brasília, 20 abr. 2004. Disponível em: https://www.camara.leg.br/noticias/47245-urgencia-constitucional/. Acesso em: 21 abr. 2020.

BRASIL. Câmara dos Deputados. *Conheça a última versão do Relatório do Marco Civil (11-7)*. 25 jul. 2012. Disponível em: http://edemocracia.camara.gov.br/web/marco-civil-da-internet/andamento-do-projeto/-/blogs/conheca-a-ultima-versao-do-relatorio-do-marco-civil-11-7. Acesso em: 21 abr. 2020.

BRASIL. Câmara dos Deputados. Marco Civil da Internet: Guia de discussão. *e-Democracia*, Brasília, 2011a. Disponível em: http://arquivo.edemocracia.camara.leg.br/web/marco-civil-da-internet/inicio#.XnJqMC3Oq-s. Acesso em: 21 abr. 2020.

BRASIL. Câmara dos Deputados. *PL 2126/2011: Projeto de Lei*, apresentado em 24 de agosto de 2011. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos Deputados, 2011b. Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255. Acesso em: 21 abr. 2020.

BRASIL. Congresso Nacional. *Minuta de anteprojeto de lei para debate colaborativo*. Estabelece o Marco Civil da Internet no Brasil. Brasília: Congresso Nacional, 2010. Disponível em: http://culturadigital.br/marcocivil/files/2010/04/MINUTA-DE-ANTEPROJETO-DE-MARCO-CIVIL-DA-INTERNET-PARA-DEBATE-COLABORATIVO.pdf. Acesso em: 21 abr. 2020.

BRASIL. Congresso Nacional. *Substitutivo ao projeto de lei nº. 2.126, de 2011*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos Deputados, 2011c. Disponível em: http://www.camara.gov.br/internet/agencia/pdf/Relatorio_final_Molon.doc. Acesso em: 21 abr. 2020.

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*: seção 1. Brasília, ano 151, n. 77, p. 1–3, 24 abr. 2014a. Disponível em: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=24/04/2014. Acesso em: 21 abr. 2020.

BRASIL. Senado Federal. *Projeto de Lei da Câmara n°. 21, de 2014*. Marco Civil da Internet. Brasília: Senado Federal, 2014b. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/116682. Acesso em: 21 abr. 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL. *Resolução CGI.br/RES/2009/003/P*. Princípios para a governança e uso da Internet no Brasil. São Paulo: CGI.br, 2009. Disponível em: http://cgi.br/resolucoes/documento/2009/003. Acesso em: 21 abr. 2020.

COMITÊ GESTOR DA INTERNET NO BRASIL. *Resolução CGI.br/RES/2012/010/P*. Posicionamento do CGI.br em relação ao parecer final do Deputado Alessandro Molon ao Marco Civil da Internet no Brasil. São Paulo: CGI.br, 2012. Disponível em: http://www.cgi.br/resolucoes/documento/2012/010. Acesso em: 21 abr. 2020.

CRUZ, C. H. Marco Civil da Internet: o que é e o que muda para o seu negócio. *CHC Advocacia*, Fortaleza, 27 fev. 2019. Disponível em: https://chcadvocacia.adv.br/blog/marco-civil-da-internet/. Acesso em: 21 abr. 2020.

ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. *G1*, São Paulo, 2 jul. 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 21 abr. 2020.

GOMES, H. S. Marco Civil da Internet não deve barrar serviços tipo 'WhatsApp grátis'. *G1*, São Paulo, 1 set. 2015. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/09/marco-civil-da-internet-deve-liberar-servicos-tipo-whatsapp-gratis.html. Acesso em: 21 abr. 2020.

GONÇALVES, C. Governo faz acordo sobre regulamento da neutralidade para aprovar marco civil. *Empresa Brasil de Comunicação*, Brasília, 19 mar. 2014. Disponível em: http://www.ebc.com.br/noticias/politica/2014/03/governo-faz-acordo-sobre-regulamento-da-neutralidade-para-aprovar-marco. Acesso em: 21 abr. 2020.

HONORATO, R. "É preciso avaliar a eficácia do Marco Civil", diz 'pai' da internet. *Veja*, São Paulo, 23 abr. 2014. Disponível em: https://veja.abril.com.br/tecnologia/e-preciso-avaliar-a-eficacia-do-marco-civil-diz-pai-da-internet/. Acesso em: 21 abr. 2020.

MACHADO, R. C. Marco civil da internet - Análise dos pontos relevantes da Lei nº 12.965/2014. *Jus*, Teresina, 23 jul. 2014. Disponível em: https://jus.com.br/artigos/30162/marco-civil-da-internet-analise-dos-pontos-relevantes-da-lei-n-12-965-2014. Acesso em: 21 abr. 2020.

MARCO Civil da Internet: seus direitos e deveres em discussão. *Cultura Digital*, [*S. l.*], 29 out. 2009. Disponível em: http://culturadigital.br/marcocivil/page/31. Acesso em: 21 abr. 2020.

MATURANA, M. Aos 20 anos da web, Brasil discute marco legal. *Senado Notícias*, Brasília, 28 maio 2013. Disponível em: http://www12.senado.gov.br/noticias/materias/2013/05/28/aos-20-anos-da-web-brasil-discute-marco-legal. Acesso em: 21 abr. 2020.

PASSARINHO, N. Dilma diz na ONU que espionagem fere soberania e direito internacional. *G1*, São Paulo, 24 set. 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/09/dilma-diz-na-onu-que-espionagem-fere-soberania-e-direito-internacional.html. Acesso em: 21 abr. 2020.

RIO DE JANEIRO (Estado). Tribunal de Justiça do Rio de Janeiro. *Agravo de Instrumento 0013822-08.2010.8.19.0000*. 2010. Disponível em: http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=0003CE5019F3DCD994E204507450C838B5FC2CC402471F29. Acesso em: 21 abr. 2020.

SALVES, D. Constituição colaborativa da Islândia serve de exemplo ao Brasil. *Terra*, Porto Alegre, 23 maio 2013. Disponível em: https://www.terra.com.br/noticias/tecnologia/internet/constituicao-colaborativa-da-islandia-serve-de-exemplo-ao-brasil,f9f3a0b2993de310VgnVCM3000009acceb0aRCRD.html. Acesso em: 21 abr. 2020.

Leituras recomendadas

BRASIL. Câmara dos Deputados. *Projeto de Lei nº. 2.126 de 2011*: Emenda Aglutinativa 1. Brasília: Câmara dos Deputados, 2014. Disponível em: http://www.camara.gov.br/internet/agencia/pdf/Emenda_aglutinativa_N_1.pdf. Acesso em: 21 abr. 2020.

BRASIL. Câmara dos Deputados. *Sessão: 359.3.54.O*. Debate do Marco Civil da Internet. Brasília: Câmara dos Deputados, 2013. Disponível em: http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=3&nuSessao=359.3.54.O&nuQuarto=3&nuOrador=3&nuInsercao=0&dtHorarioQuarto=09:21&sgFaseSessao=CG. Acesso em: 21 abr. 2020.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Proteção de dados pessoais

Karoline Freire

OBJETIVOS DE APRENDIZAGEM

- Apresentar os fundamentos teóricos e históricos da proteção de dados pessoais
- Analisar conceitos, princípios e institutos da Lei Geral de Proteção de Dados (LGPD).
- Definir o uso da LGPD nas áreas de educação, saúde e relações trabalhistas

Introdução

O aperfeiçoamento das discussões relativas aos dados pessoais nas últimas décadas representa a ênfase de sua relevância como direito fundamental autônomo para a tutela dos cidadãos. Com a rapidez dos avanços tecnológicos e a difusão em larga escala do acesso ao ambiente virtual, o manejo das informações sobre si próprio se tornou expressão essencial do indivíduo. Logo, torna-se impossível cogitar a integral proteção da liberdade, da privacidade e do desenvolvimento da pessoa natural sem que lhe seja garantida a eficiente defesa e o controle dos próprios dados, ou seja, a expressão da autodeterminação informativa.

Diante dos requerimentos sociais de uma nova instituição legislativa especializada na proteção dados, nasceu a denominada Lei Geral de Proteção de Dados (LGPD), a Lei nº 13.709 de 2018 (BRASIL, [2019]), que passou a dispor sobre o tratamento de dados pessoais, inclusive no ciberespaço, por pessoa natural ou jurídica, de direito público ou privado, com o intuito de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme dispõe o artigo inaugural do documento

legal. Assim, os mais diferentes âmbitos sociais, como saúde, educação e relações de trabalho, passam a ter a necessidade de se adequar à LGPD, para um melhor desenvolvimento da sociedade e da proteção à dignidade da pessoa humana e dos preceitos trazidos na Constituição de 1988 (BRASIL, [2016]).

Neste capítulo, você vai conhecer os fundamentos teóricos e históricos da proteção de dados pessoais. Além disso, vai ver conceitos, princípios e institutos da LGPD, com destaque ao tratamento de dados e ao consentimento. Por fim, vai estudar a LGPD nas áreas da educação, saúde e relações trabalhistas.

Proteção de dados pessoais: fundamentos teóricos e históricos

Inaugurando a redação da LGPD, o artigo 1º define o alcance da proteção de dados pessoais, os quais estão vinculados tanto para o ambiente físico quanto para o digital, certificando como sujeito de direitos unicamente a pessoa natural identificada ou identificável (BRASIL, [2019]). O documento legal indica que o objetivo requerido é a proteção dos direitos fundamentais da liberdade e privacidade, além do livre desenvolvimento da pessoa natural. Finalmente, dirige-se para pessoa física ou jurídica, de direito público ou privado, que trabalhe com dados da pessoa natural (BRASIL, [2019]).

O desenvolvimento de regulações específicas à proteção de dados também ganhou, ao longo dos anos, respaldo teórico, com atenção para preceitos advindos da Carta Maior (BRASIL, [2016]), entre eles a privacidade. O descontrole e a incerteza sobre aquele que tem o direito ao acesso aos dados pessoais perpassa o poder de escolha que delimita e define a esfera pessoal de cada ser humano. A necessidade de tutela jurídica aos que confiam seus dados pessoais às entidades públicas ou privadas se tornou evidente à medida que esses dados têm valor econômico e são usados para fins comerciais (PEZZI, 2007).

Nesse contexto, antes da edição da lei de proteção de dados, havia um debate teórico relacionado aos limites da privacidade, uma vez que os bancos de dados armazenavam — e continuam armazenando — milhões de dados pessoais, o que, na verificação da doutrina, parecia ultrapassar os direitos das pessoas em relação à gestão de seus dados. Assim, os bancos de dados se tornaram um instrumento perfeito para dilacerar os limites da privacidade. Os bancos de dados permitiam que fossem criados perfis específicos de acordo com os interesses dos titulares dos dados pessoais, e o acesso a esses bancos tomou uma dimensão ainda mais expressiva pela facilidade de transmissão

e circulação de dados. Assim, diante das relações de consumo, a criação de perfis era perfeita para a fácil e rápida transmissão de dados por meio dessas plataformas de informações pessoais. Um curso de pós-graduação, por exemplo, poderia utilizar um banco de dados de uma editora de livros especializada no segmento do curso para promover as atividades de ensino. Uma empresa de seguro de saúde poderia utilizar o banco de dados de uma loja esportiva para identificar as pessoas que, potencialmente, precisariam de serviços médicos. Uma financeira, apropriando-se de um banco de dados de uma loja de departamentos, poderia oferecer cartões de crédito a quem lhe interessasse o histórico de quitação de pagamentos para concessão da vantagem creditícia (PEZZI, 2007).

> A proporção dos reflexos possíveis com cruzamentos [de dados] se dimensiona de tal forma quando órgãos do próprio Estado tomam iniciativas para disponibilizar informações pessoais de seus cidadãos. Os jornais passam a estampar o debate sobre a possibilidade de empresas terceirizadas administrarem e comercializarem o cadastro de segurança pública do Estado de São Paulo, em troca da modernização do banco de dados. [Permitia-se ainda que] os planos de saúde [acessassem] dados sigilosos do paciente. Mesmo sendo criada para nortear o intercâmbio de dados entre os planos e os prestadores de serviço, melhorar a qualidade de gestação e coletar informações epidemiológicas necessárias para o planejamento de políticas de saúde, a medida [chocava-se] com o sigilo médico-paciente e [fornecia] um manancial de informações para o setor privado das seguradoras de saúde, [que eram capazes] de restringir [o] acesso a possíveis segurados (PEZZI, 2007, p. 11–12).

Logo, as relações de consumo, que já colocam o consumidor como figura vulnerável, passaram a ficar ainda mais instáveis por força do impacto da utilização dos bancos de dados e cadastros de consumidores sem que existisse qualquer regulamentação com embasamento específico para legislar a respeito da proteção de dados.

Foi apenas com o advento da publicação da LGPD que uma lacuna no ordenamento jurídico pátrio foi preenchida, no sentido da proteção de dados pessoais, mas normas anteriores foram precursoras desse propósito. O reconhecimento da proteção de dados como direito autônomo e fundamental advém de considerações dos riscos que o tratamento automatizado traz para a proteção da personalidade em relação às garantias constitucionais de igualdade, liberdade e dignidade da pessoa humana, com destaque, ainda, para a proteção da intimidade e da vida privada. A proteção de dados pessoais no ordenamento jurídico brasileiro, embora hoje desfrute de legislação específica, ganhou respaldo em outros documentos legais (DONEDA, 2011). A Constituição Brasileira contempla a questão da informação por meio das

garantias à liberdade de expressão e do direito à informação, além de fundamentar a proteção da personalidade e o direito à privacidade (BRASIL, [2016]).

Além disso, o Código de Defesa do Consumidor (CDC) de 1990, documento legal que traz, em sua Seção VI, os Bancos de Dados e Cadastros dos Consumidores, garante o direito às informações existentes em relação ao consumidor (BRASIL, 1990). Nesse documento legal, destaca-se o conteúdo do artigo 43, o qual estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em bancos de dados e cadastros, "[...] implementando uma sistemática baseada nos *fair information principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro" (DONEDA, 2011, p. 103). Assim:

> [Parecia] existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e [...] abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; a respeito da característica sigilosa ou não de determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem considerar os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais (DONEDA, 2011, p. 104).

Outro documento jurídico especialmente importante à proteção de dados no Brasil é o Marco Civil da Internet, Lei nº 12.965 de 2014 (BRASIL, 2014), o qual assegura aos usuários da rede mundial de computadores a inviolabilidade da intimidade e da vida privada, com destaque para o artigo 7º, incisos I a XIII, que tratam sobre direitos e garantias dos usuários, assegurando o direito às informações de forma clara e completa sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais. Além disso, o artigo 7º informa o direito do usuário ao consentimento expresso sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais e a garantia da exclusão definitiva dos dados pessoais fornecidos a determinada aplicação de internet, a requerimento do usuário, ao término das relações entre as partes (BRASIL, 2014).

Assim, é possível perceber que, anteriormente à edição e publicação da LGPD, outros documentos legais já dissertavam, ainda que de forma discreta, sobre a necessidade da proteção de dados. Eles foram impulsionados, por exemplo, pelas revelações sobre as iniciativas de espionagem antiéticas e ilegais do governo norte-americano, como é o caso do Marco Civil da Internet (CARVALHO; OLIVEIRA, 2019).

Porém, essas iniciativas não surgiram apenas de uma preocupação do legislador brasileiro em garantir efetivas responsabilidades e sanções para entidades públicas e privadas quanto ao cuidado com o tratamento de dados. Diversos países no mundo foram impulsionados a criar legislações específicas em matéria de proteção de dados, pois escândalos de vazamento de dados passaram a influenciar processos democráticos importantes, como as eleições presidenciais estadunidenses de 2016 e o plebiscito sobre a saída do Reino Unido da União Europeia (BREXIT), também em 2016.

Um acontecimento notório e de grande repercussão foi o caso envolvendo a empresa Cambridge Analytica, sob a qual se especulava a relação de vendas e o uso indevido de dados na campanha eleitoral de Donald Trump em 2016. O caso veio a público pela primeira vez em dezembro de 2015 e chegou até a corte americana no início de 2018. A rede social Facebook foi responsabilizada pelo caso e penalizada ao pagamento de 5 bilhões de dólares (BISSO *et al*., 2020).

Outros exemplos práticos do vazamento de dados que foram importantes à articulação de autoridades em diversas partes do mundo para tratar os dados pessoais ocorreu com a companhia hoteleira Marriott, que foi multada em 100 milhões de libras esterlinas pelo vazamento de 339 milhões de dados de clientes. Entre esses dados, havia números de cartões de crédito e dados de passaporte. A falha foi decorrente de um sistema adotado pela empresa após a compra de outra rede de hotéis, a Starwood, que já havia sido notificada sobre problemas de segurança em seus sistemas em 2014. Outro caso ocorreu com a companhia aérea British Airways, vítima de um ataque de *hackers*, que afetou mais de 500 mil clientes em 2018. Os dados roubados incluíam o histórico de compra de passagens, informações de pagamentos e informações pessoais de seus usuários, como nome e endereço. A empresa foi responsabilizada ao pagamento de 183 milhões de libras esterlinas pelo acontecimento (BISSO *et al*., 2020).

O indiscriminado vazamento e compartilhamento de dados de forma ilegal em inúmeros casos passou a gerar impactos socioeconômicos expressivos. Segundo informações publicadas em 2018, o custo envolvendo o vazamento de dados, somente nos Estados Unidos, somou 654 bilhões de dólares e expôs 2,4 bilhões de dados de usuários (BISSO *et al*., 2020).

Diante desse cenário, governos passaram a tomar medidas para que empresas aumentassem os investimentos com a segurança dos dados dos usuários. A União Europeia criou, em 2016, uma nova regulamentação para proteção de dados pessoais: a General Data Protection Regulation 2016/679 (GDPR) (UNIÃO EUROPEIA, 2016). Tal instrumento legal foi um importante marco para proteção e privacidade de dados dos cidadãos da União Europeia e do

Espaço Econômico Europeu. Por meio dele, a proteção de dados pessoais passou a ser tratada como direito fundamental (BISSO *et al*., 2020).

Os Estados Unidos, por outro lado, embora inúmeras sanções sejam impostas e notadamente difundidas em relação à proteção de dados, carece de uma legislação federal que regule a matéria de forma específica. Contudo, diferente do que acontece na União Europeia com a GDPR e no Brasil com a LGPD, as leis de segurança e privacidade de dados nos Estados Unidos são específicas, regulamentando, por exemplo, o uso de determinados tipos de dados no setor de saúde, finanças e telecomunicações. Assim, objetivando tratar sobre matérias não legisladas no nível federal, algumas regulações específicas para proteção de dados estaduais são expressivamente importantes, como é o caso do estado da Califórnia, onde a matéria é regulada por meio da California Consumer Privacy Act (CCPA), e do estado de Nova York, com a New York Stop Hacks and Improve Eletronic Data Security Act (NY SHIELD) (BISSO *et al*., 2020).

A legislação sobre proteção de dados brasileira foi notadamente inspirada no regulamento da União Europeia, a GDPR, que entrou em vigor em 2018 e trouxe importantes impactos para empresas e consumidores. Com isso, o Brasil, com o advento da LGPD, que entrou em vigor em 18 de setembro de 2020, passou a compor um grupo de países que contam com legislação específica para a proteção de dados de seus cidadãos. Assim, diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras passaram a garantir a privacidade dos titulares dos dados pessoais, além de passar a evitar entraves comerciais com outros países (MOTA; TENA, 2020).

Saiba mais

Stefano Rodotà (2008), no livro *A vida na sociedade da vigilância*, afirma que:

> [...] não se faz mais possível considerar os problemas de privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem (RODOTÀ, 2008, p. 25).

Conceitos, princípios e institutos da LGPD

A LGPD foi sancionada pensando que todo dado pessoal tem relevância e valor. Por tal razão, o conceito de dado pessoal ganhou amplitude, assim como na GDPR, no sentido de que os dados pessoais são equivalentes a informações relativas à pessoa singular identificada ou identificável, conforme preceitua o artigo 5º, I da LGPD (BRASIL, [2019]). Assim, mesmo que determinados dados pareçam não ter relevância em dado momento ou que não façam a direta referência a uma determinada pessoa, quando são transferidos, cruzados ou organizados, têm a possibilidade de resultar em dados específicos em relação a uma determinada pessoa. Eles podem carregar informações de caráter sensível sobre ela, como foi observado pelo Tribunal Constitucional Alemão no julgamento sobre a Lei do Censo em 1983 (MARTINS, 2016).

Assim, pela cautela de tratamento da matéria, a regra estabelecida pela LGPD, em seu artigo 1º, é a de que qualquer pessoa que trate de dados, seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada por meios eletrônicos, deverá ter um arquétipo legal para fundamentar os tratamentos de dados pessoais que realizar (BRASIL, [2019]). Portanto, não haverá necessidade de identificação de uma base legal específica apenas nos casos enquadrados nas hipóteses de exclusão da aplicação da LGPD, conforme o disposto no artigo 4º (BRASIL, [2019]). Contudo, da mesma forma, o tratamento de dados pessoais (previsto no artigo 4º, III), ou seja, aqueles para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, "[...] será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observando o devido processo legal, os princípios gerais de proteção e os direitos do titular" (BRASIL, [2019], documento *on-line*). Assim, foi estabelecida, junto à Câmara dos Deputados, uma comissão de especialistas judiciais responsáveis pela elaboração de um anteprojeto de lei em relação à matéria. Logo, quando não cabe possibilidade de exclusão, o tratamento deverá ser adaptado e realizado em pelo menos uma das hipóteses legais, para que ele seja considerado legítimo e lícito. Tais bases foram determinadas de forma genérica, e as adequações devem ser realizadas por meio da Autoridade Nacional de Proteção de Dados (ANPD), pelo Poder Judiciário e pelo Poder Legislativo (TEFFÉ; VIOLA, 2020).

É fundamental ressaltar que a LGPD no Brasil disciplina os dados por meio de fundamentos que se balizam no respeito à privacidade, na autodeterminação informativa, na liberdade de expressão, informação, de comunicação

e de opinião, na inviolabilidade da honra, da intimidade e da imagem, no desenvolvimento econômico e tecnológico, na livre iniciativa e na livre concorrência e a partir da defesa do consumidor e, de acordo com os direitos humanos, do livre desenvolvimento da personalidade e pela igualdade e exercício da cidadania pelas pessoas naturais, conforme a extração do artigo 2º, incisos I a VII, da LGPD (BRASIL, [2019]).

Vale observar que, com o advento da LGPG, uma série de conceitos foi delineada de maneira expressa, como o que acontece na definição de dados pessoais e dados sensíveis, os quais, por previsão legais, recebem tratamentos diferentes e têm determinações legislativas particulares. O artigo 5º, I, conceitua **dado pessoal** como a informação relacionada a pessoa natural identificada ou identificável, enquanto os **dados sensíveis** são aqueles relacionados a dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além dos dados referentes à saúde ou à vida sexual, dado genético ou biométrico (quando vinculado a uma pessoa natural, disposição prevista no artigo 5º, II (BRASIL, [2019]). A lei ainda traz considerações a respeito do conceito de:

> [...] dado anonimizado [...]; banco de dados [...]; titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, [2019], documento *on-line*).

A base da LGPD é desenvolvida a partir da concepção de princípios e da observância da boa-fé, que regem as atividades de tratamento de dados pessoais. Por meio dos princípios que norteiam a base legal da proteção de dados, é possível compreender as condições e circunstâncias pelas quais ela vai ser aplicada, especialmente pelo fato de que os princípios funcionam como uma bússola que norteará as interpretações dos tribunais nos casos em que questões sejam aludidas e não possuam respaldo expresso no dispositivo de lei. Nesse sentido, "[...] princípio é toda norma jurídica considerada determinante de outra ou outras que lhe são subordinadas que a pressupõe, desenvolvendo e especificando o preceito em direções mais particulares" (VAINZOF, 2019, p. 136).

Assim, os princípios gerais da proteção de dados foram elaborados e expressamente previstos em lei, devendo ser interpretados em benefício do titular de dados.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas 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 difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, [2019], documento *on-line*).

Logo, por meio do **princípio da finalidade**, o titular pode garantir a legalidade do seu processamento de dados (por meio das informações obtidas previamente, limitando a finalidade do processamento) e de terceiros, podendo ou não acessar os dado e, reduzindo, assim, o risco do uso secundário dos dados sem o consentimento do titular (VAINZOF, 2019).

O **princípio da adequação** prevê que o tratamento de dados pessoais "[...] somente pode ser realizado quando houver compatibilidade com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (VAINZOF, 2019, p. 142).

A **necessidade**, como princípio previsto da LGPD, determina "[...] a limitação do tratamento aos dados pertinentes, proporcionais e não excessivos em relação à finalidade do tratamento" (LOUZADA, 2019, p. 96).

Por meio do **princípio do livre acesso**, permite-se que o titular do dado acompanhe o fluxo informacional do dado, tendo o direito de descarte em

casos de dados incorretos, desatualizados, fora de contexto ou de caráter ilícito (MACHADO; MARCONI, 2020).

O **princípio da qualidade** funciona como um instrumento de impedimento de injustiças, pois estabelece a necessidade de exatidão, clareza, relevância e atualização dos dados (LOUZADA, 2019).

O **princípio da transparência** é entendível como fonte essencial para se atingir o objetivo do instrumento legal de proteção de dados: proteger a privacidade e o livre desenvolvimento da personalidade. Sem o simples acesso às informações de forma clara e precisa em relação ao tratamento dos dados, não há como garantir ao titular a tutela da transparência (VAINZOF, 2019).

Sabidamente, o **princípio da segurança** "[...] tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade" (BRASIL, 2020, p. 52). Logo, a centralidade desse princípio está na manutenção dos dados da pessoa física em ambiente seguro.

O **princípio da prevenção** deve estar calcado no conceito de *privacy by design*, o qual vem sendo reconhecido mundialmente "[...] como valioso auxílio para o cumprimento de exigências legais sobre privacidade de dados, considerando que são diretrizes gerais que devem nortear o processo de adequação específica de cada empresa" (VAINZOF, 2019, p. 158).

O tratamento de dados não pode ser realizado para **fins discriminatórios** ilícitos ou abusivos.

> Não se pode ter exclusão de titulares de dados pessoais no momento de seu tratamento de dados pessoais por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, saúde ou orientação sexual (MACHADO; MARCONI, 2020, p. 2611).

Finalmente, por meio do **princípio da responsabilização e prestação**, a LGPD demonstrou aos controladores e aos operadores de dados que eles são responsáveis por todas as medidas que forem adotadas com o objetivo de atender a exigências legais e de princípios estabelecidos em lei (VAINZOF, 2019).

Os princípios previstos na LGPD, ainda que fracionados, condensados ou adaptados, formam a centralidade de diversas leis, tratados, convenções ou acordos de proteção de dados pessoais. Juntos, formam o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais (DONEDA, 2011).

Outra questão de extrema importância extraída da LGPD é o tratamento dos dados pessoais e dos dados sensíveis, expressamente previstos na lei de proteção de dados brasileira. Compreende-se que, tanto o rol do artigo 7º, que prevê o tratamento dos dados pessoais, quanto o do artigo 11, que

dispõe sobre o tratamento de dados sensíveis (BRASIL, [2019]), são taxativos, embora sejam dotados de hipóteses mais abertas e com relativo grau de subjetividade, como o legítimo interesse (TEFFÉ; VIOLA, 2020).

> De forma a se evitar abusos no tratamento de dados e garantir os direitos do titular, ele poderá revogar o seu consentimento, [...] ou pleitear o direito à oposição, que significa que o titular poderá se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (Art. 18, §2º). Além disso, encontra-se positivado o direito à explicação (Art. 20), que dispõe que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (TEFFÉ; VIOLA, 2020, p. 4-5).

O sistema legal que foi desenvolvido para o tratamento de dados confere ao titular instrumento de controle em relação as suas informações pessoais e de garantia de direitos, com especial destaque para o consentimento e o legítimo interesse. O consentimento simboliza "[...] instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular" (TEFFÉ; VIOLA, 2020, p. 7). É por meio do consentimento que se realiza a promoção da personalidade, representando uma modalidade para a edificação e determinação da esfera privada. Ele vincula-se, então, à autodeterminação existencial e informacional do ser humano, se apresentando como fundamental para a proteção do titular dos dados e, da mesma forma, para o fluxo de informações (DONEDA, 2011).

A LGPD, na disposição do artigo 5º, XII, prevê o consentimento como a "[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, [2019], documento *on-line*). Com relação ao consentimento requerido e ao consentimento necessário, Teffé e Viola (2020, p. 10) afirmam:

> Na hipótese em que o consentimento é requerido, ele será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Quando o consentimento for necessário, havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações.

Assim, a LGPD procura, seja pelo consentimento, seja pelo tratamento de dados ou por tantos outros instrumentos dispostos expressamente na

legislação, implementar mecanismos para a proteção e garantia da dignidade humana. Assim, a lei de proteção de dados, além de facilitar o controle dos dados tratados, impõe responsabilidades aos agentes de tratamento e oportuniza segurança para que as informações sejam transmitidas. A lei objetiva avançar os riscos de violação à privacidade e impede intervenções abusivas de informações e vazamento de dados (TEFFÉ; VIOLA, 2020).

Saiba mais

O estudo "Direito fundamental à liberdade de pesquisa genética e à proteção de dados pessoais: os princípios da prevenção e da precaução como garantia do direito à vida privada", de Regina Linden Ruaro (2015), analisou os direitos fundamentais de liberdade de pesquisa e da proteção de dados pessoais no âmbito da genética humana e propôs a aplicação dos princípios de precaução e da prevenção. A partir desse trabalho, foi realizada uma avaliação da legislação brasileira como medida de garantia à privacidade dos dados pessoais e das informações colhidas na investigação científica. O estudo queria elucidar a limitação de direitos fundamentais a partir da concepção de que eles não são absolutos. Foi proposta, ainda, a aplicação dos princípios da precaução e da prevenção no ciberespaço.

LGPD nas áreas de educação, saúde e relações trabalhistas

O artigo 5º, inciso II, da LGPD, traz importantes e sensíveis desdobramentos dos dados pessoais (BRASIL, [2019]). Entre eles, estão os dados vinculados com saúde, também denominados de dados clínicos ou informações médicas. Por seu elevado potencial discriminatório e lesivo, os dados que contêm informações de saúde impulsionam a imprescindibilidade de preservação e proteção, para que sejam garantidos os direitos à dignidade, ao sigilo e à vida privada dos titulares (BRASIL, [2019]).

Pelo elevado grau de lesividade dos dados sensíveis (por revelarem informações de caráter personalíssimo, embutidas no âmbito da proteção do direito de personalidade), sua coleta, processamento e tratamento devem acontecer apenas após o consentimento expresso do titular, uma vez que a inobservância da anuência viola a legislação de proteção de dados, com destaque para os dados confidenciais e as reservas do ser (SIQUEIRA; HOCH, 2019).

Há construção teórica e legislativa, no plano internacional, que fomenta a utilização do referencial de "direitos humanos dos pacientes" (DHP), previstos em documentos elaborados e adotados no âmbito de organizações e sistemas internacionais, como

Ataques internos

São brechas de segurança ocasionadas por um indivíduo que faz parte de uma organização, que controla os bens que devem ser protegidos, como, por exemplo, o usuário de um sistema, que deve proteger as informações contidas nele. Veja alguns exemplos de ataques internos:

- **Entradas clandestinas:** uma entrada clandestina envolve introduzir deliberadamente uma vulnerabilidade em um *software*, como, por exemplo, o *overflow*, que consiste em o invasor explorar *bugs* de implementação nos quais o controle da memória temporária para armazenamento dos dados não tenha sido feito adequadamente. Quando o profissional conhece essa falha, de forma maliciosa, pode explorá-la para obter privilégios elevados. Entretanto, nem sempre as entradas clandestinas se dão de forma maliciosa. Imagine a seguinte situação: um sistema de identificação biométrica de um banco pode conter uma entrada clandestina inserida por um programador no desenvolvimento do sistema; se essa entrada clandestina for mantida como ativa, ela poderá fornecer mecanismos de entrada em caso de algum problema imprevisto.
- ***Easter eggs*:** um *software* pode incluir características escondidas que podem ser processadas de forma similar às entradas clandestinas.

Saiba mais

No sistema operacional Windows, há um *easter egg* no jogo paciência que permite que o usuário vença apenas pressionando as teclas shift + alt + 2.

- **Bombas lógicas:** programa que realiza ação maliciosa como resultado de alguma condição lógica do sistema que está tentando danificar. Para ser considerada uma bomba lógica, deve haver intenção maliciosa por parte do programador.

Exemplo

Um exemplo de bomba lógica é o desenvolvedor de um sistema implementar um código que programe esse sistema para ter determinadas falhas após um tempo de uso pelo cliente. Nesse caso, o usuário do sistema se obrigaria a contatar o desenvolvedor para ajustar o problema — portanto, esse tipo de bomba lógica é uma forma de extorsão.

Fique atento

Em 31 de julho de 1996, uma bomba lógica elaborada pelo programador Tim Lloyd foi disparada no servidor das operações de fabricação da Omega Engineering e custou milhões de dólares em danos à empresa, levando-a a demitir muitos empregados. Descobriu-se que, a partir dessa bomba, arquivos do servidor haviam sido destruídos e que o programador em questão era o administrador do servidor.

Vírus de computador

É um *software* ou código de computador que pode replicar-se pela modificação de outros arquivos e programas para inserir código capaz de replicação posterior. Segundo Levine e Young (2013), vírus de computador são programas que passam entre computadores, da mesma forma que um vírus biológico passa entre pessoas — como, por exemplo, a gripe.

Seu principal objetivo é a danificação de um computador, corrompendo arquivos do sistema, utilizando recursos da máquina, destruindo dados ou deixando pastas ocultas.

- **Vírus de macro:** é ativado quando um documento é aberto, momento em que o vírus pode procurar outros documentos para infectar.

Saiba mais

Sality é um vírus de arquivo executável. Quando executado, desabilita programas antivírus e infecta outros arquivos executáveis. Ele disfarça sua presença em um arquivo executável (.exe) por meio da modificação de seu ponto de entrada. Caso o computador em que esteja alocado possua conexão com a internet, ele se conectará a sites de *malware* e fará download de outros *softwares* maliciosos, os *malwares.*

- **Vírus de setor de carga (*boot sector*):** é um tipo de vírus que infecta o código no setor de carga de uma unidade, que é executado sempre que o computador é ligado ou reiniciado. É o primeiro programa que o computador executa.
- **Vírus mutantes ou polimórficos:** possuem a capacidade de gerar réplicas de si, utilizando chaves de encriptação diversas e fazendo com que suas cópias possuam formas diferentes.
- **Vírus encriptados:** são vírus que, por estarem codificados, acabam dificultando a ação de *softwares* antivírus.

Vírus de computador são um tipo de *malware*. Um *malware* é um ataque interno que se refere a um furo de segurança criado em um *software* por um de seus programadores. Esse tipo de ataque é perigoso, pois é iniciado por alguém considerado de confiança dentro de uma organização e que tem, portanto, acesso ao sistema. O *malware* embutido pode iniciar a escalação de privilégios, causando danos por algum evento do sistema ou instalando um segundo *malware*.

Outros tipos de *softwares* que atacam um computador são:

- ***Ransomware* corporativo:** é um *malware* que tem como principal função criptografar todos os dados visíveis para o usuário. A intenção é, a partir do *Ransomware*, solicitar resgate às informações bloqueadas. Caso o usuário tente quebrar a segurança do *malware* por meio de alguma técnica de força bruta, parte dos dados (ou todos os dados) pode ser deletada.
- **Cavalo de Troia:** é um *malware* que finge ser um *software* legítimo ou vem integrado a um. Ele engana o usuário, estimulando-o a "abrir portas" e instalar outros *malwares* a fim de infectar uma máquina.

- ***Spyware*:** é um *malware* projetado para espionar usuários, salvar suas senhas, informações pessoais e enviar esses dados a um destino.
- ***Adware*:** é um *malware* que importuna vítimas com anúncios indesejados e abre pontos de segurança vulneráveis para outros *malwares*.
- ***Rootkit*:** é um *malware* que altera utilitários do sistema em uso ou do sistema operacional. Muitas vezes, esconde arquivos do disco. *Rootkits* são, frequentemente, utilizados para esconder ações maliciosas ou outros tipos de *malware*, como Cavalos de Troia.

Fique atento

Em 2005, um dos *rootkits* mais famosos foi incluído no *software* de proteção de cópia em alguns CDs distribuídos pela Sony BMG. Esse *malware* podia instalar-se em um computador quando um usuário inserisse o CD na sua mídia ótica. Ele tinha como objetivo reforçar a proteção de cópia do conteúdo de músicas dos CDs infectados. O *rootkit* não pretendia ser malicioso, mas, visto que podia ocultar qualquer processo com um nome iniciado por certa String, alguns profissionais maldosos da área de TI resolveram usá-lo.

- **Ataques de dia zero:** é um ataque que explora uma vulnerabilidade previamente desconhecida, mesmo pelos projetistas e desenvolvedores de *software* que criaram o sistema contendo essa vulnerabilidade. Esse nome vem pelo fato de que, se um *malware* explora uma vulnerabilidade que os desenvolvedores desconhecem, diz-se que esse ataque aconteceu no "dia zero" a partir do seu conhecimento.
- ***Distributed Denial of Service* (DDoS):** é uma das principais técnicas utilizadas para impedir o acesso a páginas e serviços web. É conhecido como ataques de negação de serviço distribuído e consiste no uso de várias máquinas zumbis para a distribuição de múltiplos pacotes e requisições para um único servidor. Dessa forma, é possível dificultar e/ou invia-bilizar completamente a visualização de aplicativos e sites hospedados em um determinado IP.

Saiba mais

Uma declaração feita em 2007, realizada pelo ex-oficial de segurança da informação do governo norte-americano, Paul Strassman, apontou a existência de cerca de 750 mil máquinas zumbis somente na China.

Técnicas de invasão voltadas para equipamentos da Internet das Coisas

A Internet das Coisas traz inúmeros benefícios, como, por exemplo, os dispositivos que se conectam a redes e *softwares* por meio de conexões sem fio e que nos auxiliam na automatização de processos no ambiente corporativo, na otimização de rotinas e na redução de custos. Porém, o uso dessa tecnologia torna os equipamentos utilizados vulneráveis ao acesso de hackers, que buscam formas de capturar dados privados, além de permitir sua integração a redes de *bots*.

Vulnerabilidades causadas pela incorporação do BYOD (*Bring Your Own Device* ou Traga o Seu Próprio Dispositivo) no ambiente corporativo

BYOD (*Bring Your Own Device* ou Traga o Seu Próprio Dispositivo) é uma política administrativa em que empresas incentivam os seus profissionais a utilizarem os próprios equipamentos. Essa política tem como objetivos a redução de custos operacionais, a melhoria do ambiente interno e a atualização mais ágil dos dispositivos internos. Porém, se não houver um cuidado de segurança, a vulnerabilidade interna aumenta, ampliando as chances de alguma ameaça atingir a empresa.

- **Ataques pelo *browser*:** criminosos virtuais se utilizam de engenharia social e de diferentes técnicas de *phishing* a fim de encontrar uma brecha. Alguns exemplos são as URLs suspeitas, links que enviam o usuário para outro domínio que facilita a invasão, sites clonados que pedem informações pessoais, *pop-ups* com anúncios enganosos.

- **Ataques evasivos:** hackers criam estratégias que podem modificar *softwares* maliciosos e/ou evitar a detecção por *firewalls*. Essa técnica é usada pelos criminosos para explorar vulnerabilidades e confundir os dispositivos de rede a fim de encobrir a existência do *malware*.
- **Ataques SSL (*Secure Socket Layers*) e TLS (*Transport Layer Security*):** é um padrão que diz respeito à criptografia virtual. Nesse caso, os hackers se escondem no tráfego criptografado, pois sabem que muitas empresas não utilizam ferramentas adequadas para inspecioná-los. Já o TLS foi desenvolvido depois do SSL, é mais frequente nos programas de e-mails e usa mecanismos de criptografia mais fortes.

Saiba mais

Existem várias formas de ataques aos protocolos SSL/TLS, como a *Compression Ratio Info-Leak Mass Exploitation*, conhecida como 'CRIME' em sua forma abreviada. Esse tipo de ataque possibilita que o invasor consiga acesso aos conteúdos guardados em *cookies* da internet quando é utilizado TLS. Com esse tipo de ataque, é possível que o invasor "sequestre" uma sessão web, expondo as informações e comprometendo a integridade do acesso do usuário.

- **Ataques de força bruta:** é a maneira mais famosa que existe para se quebrar senhas. Consiste em tentar todas as combinações possíveis até que o *password* seja encontrado.

Formas de monitoramento de ataques

Por meio da identificação de vulnerabilidades na infraestrutura de TI, é possível prevenir possíveis ataques, trabalhando em soluções que possam corrigir as falhas encontradas.

Sistemas de monitoramento podem vasculhar o ambiente de TI de uma empresa para fazer varredura de vulnerabilidades, informações em *logs*, indicadores e falhas encontradas. Também é possível analisar os pontos críticos dos sistemas e possíveis falhas que venham a acontecer por excesso de demanda.

Ações de monitoramento incluem:

- monitorar os eventos em tempo real ou com o máximo de proximidade;

- inventariar, obter e armazenar dados acerca de *softwares*, redes e demais dispositivos em uso na empresa;
- executar varreduras constantes em busca de vulnerabilidades ou eventos suspeitos;
- análise e revisão periódica de informações sobre eventos críticos;
- criar indicadores e relatórios personalizados e claros para demonstrar os resultados do monitoramento;
- efetuar correções sobre as vulnerabilidades e falhas encontradas durante o processo.

Uma das ferramentas mais utilizadas na área de segurança é o *firewall*, que funciona como uma barreira a conteúdos maliciosos, enquanto permite que informações sejam recebidas e enviadas por meio da internet. Apenas passam na barreira dados que obedecem a certas regras, garantindo a integridade da rede. Existem, basicamente, duas maneiras de se implementar soluções de *firewall*: por meio de aplicativos, ou seja, *software*, e por meio de *hardware*, uma solução mais robusta, também conhecida como *appliance*.

Fique atento

No mercado, há uma evolução do *firewall* chamada Next Generation. Essa nova solução é mais moderna e pode realizar bloqueios não somente de portas e protocolos, mas, também, de funcionalidades especificas dentro de uma URL.

Outra ferramenta de *firewall* existente é o UTM (*Unified Theat Mangement*), um *firewall* multifuncional que incorpora, em uma única solução, IPS, Gateway Antivírus, Web Filter, Antispam VPN, entre outros sistemas de segurança.

Existe, também, a segurança *endpoint*, que protege cada nó de extremidade de uma rede corporativa contra ataques e invasões. Qualquer dispositivo que se conecte internamente na rede pode ser considerado uma porta de ameaça que venha a prejudicar a infraestrutura da empresa.

Para ser bom, um programa de monitoramento deve realizar a coleta e a análise de dados a partir dos quais indicadores de ataque e de comprometimento podem ser extraídos de várias fontes, tais como: padrões de navegação, registros de DNS, tráfego *netflow*, serviços e processos em execução em servidores e estações de trabalho.

Veja alguns *softwares* que podem auxiliar no monitoramento de ataques:

- Cacti: *software open source*, com agilidade na análise de dados. O objetivo é recolher informações sobre o estado da rede e exibir os resultados com gráficos para o usuário. Além disso, também analisa a largura de banda utilizada e o desempenho da CPU.
- Nagios: ferramenta *open source* que monitora, além dos serviços, os *hosts*. Por meio dessa ferramenta, é possível ter acesso ao momento em que o problema foi solucionado. Ele monitora serviços de rede, os recursos necessários para que ela funcione e também permite a criação de *plugins*, de forma que os usuários possam criar seus próprios modelos de monitoramento.
- Inciga: *open source*, avisa o usuário sobre erros e quando eles são solucionados, gera relatórios de desempenho para o administrador. A partir dele, o monitoramento pode ser feito remotamente, ou seja, por *smartphones* e *tablets*, por exemplo.
- Nedi: sua principal vantagem é o sistema de rastreamento de dispositivos pela rede, mantendo controle sobre cada um deles. O Nedi também mostra a localização de cada máquina conectada à rede.
- Zabbix: *open source*, é uma solução que pode ser utilizada 100% on--line; permite o envio de dados por e-mail e SMS sobre problemas e suas resoluções.
- Observium: oferece suporte para diversos sistemas, sendo uma plataforma *open source* desenvolvida em PHP/MySQL. Quando instalado na versão profissional, faz um rastreamento geográfico de todas as máquinas da rede, podendo encontrar aparelhos roubados.

Em relação a ataques internos, podemos ter defesas como:

- Evitar pontos simples de falha, não deixando apenas uma pessoa criar *backups* ou gerenciar recursos críticos.
- Usar inspeções de códigos (no caso de ter programadores próprios na organização), fazendo com que cada programador saiba o que está ocorrendo em relação a erros com o código do colega e, dessa forma, conseguindo auxiliar na sua solução. Assim, um programador raramente conseguirá implementar uma bomba lógica.
- Limitar autoridade e permissão, fazendo com que se estabeleça que cada programa ou usuário do sistema receba privilégios adequados a seu uso.

- Limitar o comportamento dos empregados, especialmente se usuários máster e programadores estiverem com algum descontentamento.
- Limitar instalações de *softwares* nas máquinas de uma empresa.

Existem várias formas de monitorar um ataque, mas é preciso saber a real necessidade de cada empresa para que seja escolhida a maneira mais adequada de proteção.

Ataques autenticados e não autenticados

Primeiramente, devemos ter em mente que o ataque não autenticado é uma forma de descobrir e explorar falhas de segurança a partir do acesso a uma conta de usuário comum em uma empresa, bem como tentando comprometer uma máquina não muito crítica, como, por exemplo, um *desktop* ou *notebook*.

O ataque autenticado ou "escala de privilégios", por outro lado, será realizado com a tentativa de obter a conta do administrador da máquina invadida, conseguindo acesso à sua conta. Nesse tipo de ataque, o invasor tentará projetar-se para servidores até conseguir hackear toda a rede da empresa. A partir desse ataque, o hacker terá como acessar o sistema de forma remota a partir de seus *backdoors*. Usualmente, os mecanismos de autenticação incluem:

- **Autenticação baseada em conhecimento**: utiliza uma informação que o usuário conhece para identificá-lo. Um exemplo é quando se inclui login e senha e, para lembrança futura do usuário, caso esqueça, solicita-se "perguntas-respostas".
- **Autenticação baseada em *token***: utiliza um dispositivo específico, como, por exemplo, cartões de memória, chaves, crachás, *smart cards*, etc., para identificação do usuário.
- **Autenticação baseada em biometria**: utiliza informações estáticas, como impressão digital, reconhecimento de retina, etc., para autenticação.

A funcionalidade de autenticação em um sistema está sujeita a muitas falhas, o que inclui a funcionalidade de login e também as de registro de usuário, mudança de senha e recuperação de conta. Podemos citar, dentre as falhas de projeto e implementação em mecanismos de autenticação: senhas fracas, força bruta de login, mensagens de erro detalhadas, transmissão vulnerável de credenciais, funcionalidade de alterar a senha, funcionalidade "lembre-me" da

senha, funcionalidade "mantenha-me conectado", funcionalidade representação de usuário, validação incompleta de credenciais, nomes de usuários não exclusivos, nomes de usuários previsíveis, senhas iniciais previsíveis, distribuição insegura de credenciais. Formas de quebra de sessão de usuários são:

- **Engenharia social**: muitos usuários são facilmente enganados por aquilo que veem na internet; por isso, um atacante pode conseguir do próprio usuário as credenciais de acesso, como, por exemplo, por meio de um e-mail, que solicita seus dados de login e senha.
- ***Bruteforce***: por vezes, os usuários utilizam-se de senhas fracas em suas contas. Se a aplicação não tem nenhum método que impeça que ataques de *bruteforce* aconteçam, esse ataque pode acabar identificando a senha de um usuário (se o mesmo já for conhecido previamente) por meio de sua data de nascimento, seu nome, apelido, etc.
- **Transição limpa de troca de credenciais**: cenário em que as credenciais de uma autenticação são capturadas em trânsito, e a requisição (nesse caso) poderá ser alterada para a obtenção de um resultado (entrar numa conta sem permissão).

Veja os ataques e as ameaças contra autenticação baseada em senhas:

- **Ataque por dicionário**: obtém uma lista de palavras e testa todas as palavras possíveis contra o sistema.
- **Ataque por combinação exaustiva**: caso o invasor conheça a quantidade máxima de caracteres que a senha possa ter e os limites de combinação, o usuário testa todas as possibilidades possíveis.
- **Ataque por senha popular**: utiliza senhas fáceis, como, por exemplo, abc123, 123456, etc. Assim, há grande possibilidade de que um ou mais usuários utilizem o mesmo tipo de senha.
- **Ataque por informação conhecida**: esse ataque utiliza dados do usuário para prever a senha, como, por exemplo, data de aniversário, número de telefone, nome do pai, nome da mãe, etc. É uma técnica utilizada para sistemas que exigem validação de perguntas para recuperação de senhas.

Para evitar a "adivinhação" de senhas, é possível "setar" uma série de ações relacionadas a bloqueio de contas, depois de um certo número de tentativas de acesso, configuração do nível de segurança das senhas, para que cumpram requisitos de segurança da organização, uso de auditoria e *event log.*

A seguir, confira ataques e ameaças contra autenticação baseada em *tokens* e contra sistemas:

- ***Token***: esse tipo de ataque envolve o roubo ou empréstimo do elemento utilizado como *token* para parceiros. Nesse caso, é necessário adotar políticas de uso que proíbam empréstimo do *token* e uso por parte de terceiros, adoção de tecnologias redundantes, como câmeras, para monitorar qual pessoa está utilizando o recurso, e mecanismos para cancelamento de um determinado *token*, se o usuário o perdeu ou foi furtado.
- **Sistema**: nesse caso, deve-se reduzir a quantidade de usuários que podem ter acesso diretamente ao sistema e aplicar políticas em relação a usuários, que, por exemplo, deixem a organização.

É preciso saber como usar a tecnologia de autenticação; portanto, a seguir, confira algumas dicas:

a) Definir os tipos de usuários e seus respectivos níveis de acesso vinculados a cada tipo.
b) Ao cadastrar um novo usuário, ele deve ser vinculado ao nível de acesso conveniente.
c) Se o usuário acessar um sistema publicamente, ferramentas de maior segurança deverão ser utilizadas.
d) Caso o usuário acesse um sistema disponível localmente, diferentes níveis de autenticação deverão ser utilizados. Recursos críticos deverão ter sistemas de autenticação mais exigentes, enquanto recursos não críticos deverão ter níveis menos exigentes.
e) Obrigar a troca periódica do recurso usado para autenticação.

Referências

GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de Computadores*. Porto Alegre: Bookman, 2013.

LEVINE, J. R.; YOUNG, M. L. *Internet para leigos*. Rio de Janeiro: Alta Books, 2013.

Leituras recomendadas

AMTI. *Ataques que todo setor de TI deve conhecer*. 16 maio 2017. Disponível em: <https://www.amti.com.br/blog/seguranca-da-informacao-4-ataques-que-todo-setor-de-ti-deve-conhecer>. Acesso em: 11 dez. 2018.

CARNEIRO, L. D. *Infrações Penais e a Informática:* a tecnologia como meio para o cometimento de crimes. 2016. Disponível em: <https://jus.com.br/artigos/52698/infracoes-penais-e-a-informatica-a-tecnologia-como-meio-para-o-cometimento-de-crimes>. Acesso em: 11 dez. 2018.

OLIVEIRA, W. J. *Dossiê Hacker*. São Paulo: Digerati Books, 2007.

REVISTABW. Segurança de Computadores e da Informação: métodos de autenticação de usuário. *Revista Brasileira de Web: Tecnologia*, 2016. Disponível em: <http://www.revistabw.com.br/revistabw/seguranca-autenticacao-de-usuario/>. Acesso em: 11 dez. 2018.

STRONG SECURITY BRASIL. *5 Ferramentas de segurança da informação que você precisa investir*. 04 jan. 2018. Disponível em: <https://www.strongsecurity.com.br/5-ferramentas-de-seguranca-da-informacao-que-voce-precisa-investir/>. Acesso em: 11 dez. 2018.

SZYMANSKI, T. *Os 4 ataques Hackers mais comuns da web*. 20 fev. 2012. Disponível em> <https://www.tecmundo.com.br/ataque-hacker/19600-os-4-ataques-hackers-mais-comuns-da-web.htm>. Acesso em: 11 dez. 2018.

Criptografia

Thiago Nascimento Rodrigues

OBJETIVOS DE APRENDIZAGEM

- Conceituar criptografia.
- Identificar as bases teóricas da criptografia.
- Descrever aplicações de criptografia.

Introdução

A necessidade de ocultar informações ou garantir o sigilo de mensagens trocadas entre duas partes remonta aos períodos mais antigos da história. Seja pela simples garantia da privacidade de um canal de comunicação, seja por razões estratégicas de natureza financeira ou militar, a demanda por confidencialidade veio crescendo ao longo dos anos. Em razão disso, novas tecnologias seguem sendo desenvolvidas para atender um nível de segurança cada vez mais crítico. Especialmente com o advento da internet, essa necessidade ganhou uma relevância sem precedentes.

Nesse cenário, a criptografia se consolidou como uma ciência que subsidia todo o desenvolvimento e implementação de mecanismos de segurança. Com o rápido aumento do poder computacional a cada ano, mais fundamentos matemáticos vem sendo incorporados a pesquisas e estudos em criptografia para garantir o projeto de algoritmos mais robustos e complexos de serem violados.

Neste capítulo, você vai estudar esse campo de estudo que está no cerne de toda a segurança digital moderna. Além disso, vai conhecer as principais estratégias de criptografia e as respectivas fundamentações matemáticas. Por fim, vai ver exemplos práticos, o que proporciona uma visão mais aplicada das técnicas de criptografia.

Introdução à criptografia

A palavra criptografia tem sua origem em duas palavras gregas que significam "[...] escrita secreta" (CRIPTOGRAFIA, c2021, documento *on-line*) e é a arte e a ciência de ocultar o significado. A criptografia parece estar intimamente ligada à comunicação eletrônica moderna. No entanto, a criptografia é uma arte/ciência muito antiga, e os primeiros exemplos são de cerca de 2000 a.C., quando hieróglifos "secretos" não padronizados eram usados no antigo Egito. Desde aquele tempo, a criptografia tem sido usada em muitas — ou na maioria — das culturas que desenvolveram a linguagem escrita. Por exemplo, há casos documentados de escrita secreta na Grécia e na Roma antigas (PAAR; PELZL, 2010).

Saiba mais

Os egípcios eram capazes de se comunicar por mensagens escritas com hieróglifos. Esse código era o segredo de uma categoria selecionada de pessoas: os escribas. Os escribas costumavam transmitir o segredo de escrever hieróglifos de pai para filho, até que a sociedade entrou em colapso. Vários milênios depois, em 1822, esse código secreto foi quebrado pelo egiptólogo francês Jean-François Champollion (VAUDENAY, 2006).

Outro exemplo de proteção de escrita ou uso de criptografia primitiva na antiguidade foi empregado pelos guerreiros espartanos, que costumavam criptografar mensagens usando cítalas (Figura 1). As cítalas eram cilindros em torno dos quais eles envolviam um cinto de couro. A criptografia era realizada escrevendo a mensagem nesse cinto de couro ao longo do eixo do cilindro e desembrulhando o cinto. A operação inversa, ou "descriptografia", era feita envolvendo o cinto em torno de um cilindro de mesmo diâmetro e fazendo a leitura da mensagem ao longo do eixo (VAUDENAY, 2006).

Figura 1. Cítala espartana.
Fonte: Medeiros (2015, documento *on-line*).

Historicamente, os maiores consumidores de criptografia eram as organizações militares e os governos. Veja a seguir para o que essa comunicação com códigos secretos era comumente necessária.

- Para a diplomacia: governos precisavam se comunicar com suas embaixadas remotas em ambientes suspeitos.
- Durante a guerra: quando um quartel-general do exército precisava se comunicar em ambientes hostis.
- Para privacidade individual ou corporativa: pessoas queriam ser protegidas de sua vizinhança (cônjuges ciumentos, ditaduras etc.) e empresas queriam proteger seus ativos de concorrentes.

A maioria desses cenários, no entanto, usava a criptografia de maneira trivial. Além disso, a maioria dos códigos secretos tinha uma segurança baseada na obscuridade: os códigos secretos eram dedicados a aplicações específicas, e as pessoas que queriam se comunicar com segurança tinham que escolher seu próprio código secreto. Assim, todos os usuários envolvidos na comunicação deveriam ser capazes de manipular a técnica de criptografia relacionada. A história da criptografia moderna começou com a tecnologia de comunicação elétrica, para a qual esse modelo se mostrou claramente inadequado.

Até o final do século XX, a criptografia era em grande parte uma arte. Construir bons códigos ou quebrar os existentes dependia da criatividade e de um senso desenvolvido de como os códigos funcionam. Havia pouca teoria em que se apoiar e, por muito tempo, nenhuma definição funcional do que constitui um bom código. Nas décadas de 1970 e 1980, esse quadro da criptografia mudou radicalmente. Uma rica teoria começou a emergir, permitindo

o estudo rigoroso da criptografia como ciência e disciplina matemática. Essa perspectiva, por sua vez, influenciou como os pesquisadores pensam sobre o campo mais amplo da segurança de computadores (KATZ; LINDELL, 2015).

Em suma, a criptografia passou de um conjunto heurístico de ferramentas preocupadas em garantir a comunicação secreta dos militares para uma ciência que ajuda a proteger sistemas para pessoas comuns em todo o mundo. Isso também significa que a criptografia se tornou um tópico mais central na ciência da computação.

Encriptação

A encriptação é a principal aplicação da criptografia. Ela torna os dados incompreensíveis para garantir a sua confidencialidade (segurança de que determinada informação não possa ser acessada por pessoas não autorizadas). O processo de encriptação usa um algoritmo denominado cifra e um valor secreto chamado de chave de forma. Se alguém não conhecer essa chave secreta, não será capaz de decriptar nem de aprender qualquer informação sobre a mensagem encriptada.

Quando uma mensagem é encriptada (ou criptografada), o texto limpo se refere à mensagem não criptografada e o texto cifrado, à mensagem criptografada. Uma cifra é, portanto, composta de duas funções: a criptografia que transforma um texto limpo em um texto cifrado e a descriptografia que transforma um texto cifrado em um texto simples. Contudo, em geral, o termo cifra é empregado de forma intercambiável com o termo criptografia. Por exemplo, a Figura 2 mostra uma cifra (E) representada como uma caixa que toma como entrada um texto limpo (P) e uma chave (K) e produz um texto cifrado (C) como saída. Essa relação é comumente denotada por C = E(K, P). Da mesma forma, quando a cifra está em modo de descriptografia, a relação é expressa como D(K, C).

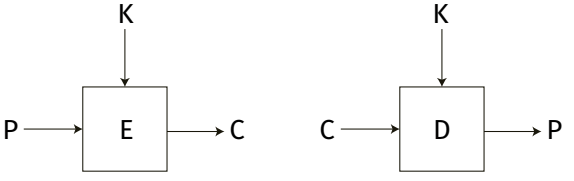

Figura 2. Encriptação e decriptação básicas.
Fonte: Aumasson (2018, p. 25).

Fique atento

Para algumas cifras, o texto cifrado tem o mesmo tamanho que o texto limpo. Para outras, o texto cifrado é um pouco mais longo. No entanto, os textos criptografados nunca podem ser mais curtos que os textos limpos (AUMASSON, 2018).

Fundamentos de criptografia

Conforme visto, criptografia é definida como a arte de escrever ou resolver códigos. Embora essa definição seja historicamente precisa, ela não captura a amplitude atual do campo ou seus fundamentos científicos atuais. A definição se concentra exclusivamente nos códigos que foram usados por séculos para permitir a comunicação secreta. Contudo, atualmente, a criptografia abrange muito mais do que isso. Ela trata de mecanismos de garantia de integridade, técnicas de troca de chaves secretas, protocolos de autenticação de usuários, leilões e eleições eletrônicas, dinheiro digital etc. Apesar de não ser uma tentativa de fornecer uma caracterização completa, é possível afirmar que a criptografia moderna envolve o estudo de técnicas matemáticas para proteger informações digitais, sistemas e computações distribuídas contra ataques adversários.

Hoje, a criptografia está em toda parte. Qualquer pessoa que já tenha se autenticado digitando uma senha, comprado algo com cartão de crédito pela internet ou baixado uma atualização verificada para seu sistema operacional, usou criptografia. Cada vez mais, programadores com relativamente pouca experiência estão sendo solicitados a proteger os sistemas que escrevem incorporando mecanismos criptográficos.

Uma primeira observação em relação ao estudo da criptografia é o reconhecimento de que ela é parte integrante de uma teoria de abrangência ainda maior. A Figura 3 apresenta um diagrama de como essa teoria está organizada sob um conceito mais geral denominado **criptologia**. Essa área de estudo é dividida em dois grandes ramos; veja a seguir.

- Criptografia: é a ciência da escrita secreta, com o objetivo de ocultar o significado de uma mensagem.
- Criptoanálise: é a ciência e, às vezes, a arte de quebrar criptossistemas. Um equívoco comum é considerar que a quebra de códigos é para a comunidade de inteligência ou talvez para o crime organizado e, por isso, não deveria ser incluída em uma classificação séria de uma

disciplina científica. No entanto, a maior parte da criptoanálise é feita por pesquisadores respeitáveis. A criptoanálise é muito importante para os criptossistemas modernos. Sem pessoas que tentem quebrar os conhecidos métodos de criptografia, jamais seria possível saber se eles são realmente seguros ou não.

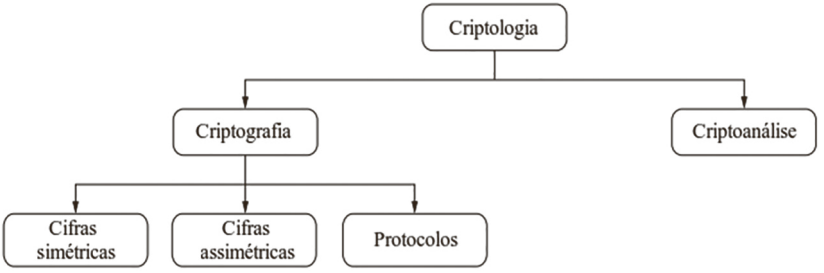

Figura 3. Visão geral do campo da criptologia.
Fonte: Adaptada de Paar e Pelzl (2010).

Ainda em relação ao conceito de criptologia esquematizado na Figura 3, a critptografia pode ser subdividida nos seguintes três ramos principais.

- Cifras ou algoritmos simétricos: presumem que ambas as partes envolvidas na comunicação têm um método de criptografia e descriptografia para o qual compartilham uma chave secreta. Toda a criptografia, desde os tempos antigos até 1976, foi baseada exclusivamente em métodos simétricos. Cifras simétricas ainda são amplamente utilizadas, especialmente para criptografia de dados e verificação de integridade de mensagens.
- Cifras ou algoritmos assimétricos (ou de chave pública): em 1976, esse tipo de cifra totalmente diferente foi projetado. Dentro da criptografia de chave pública, um usuário possui uma chave secreta (como na criptografia simétrica), mas também uma chave pública. Algoritmos assimétricos podem ser usados para aplicações como assinaturas digitais e troca de chaves, além da criptografia de dados clássica.

- Protocolos criptográficos: em linhas gerais, os protocolos criptográficos lidam com a aplicação de algoritmos criptográficos. Algoritmos simétricos e assimétricos podem ser vistos como blocos de construção com os quais aplicações como a comunicação segura pela internet podem ser realizadas. O esquema TLS (Transport Layer Security, ou segurança da camada de transporte, em tradução livre), usado em todos os navegadores da *web*, é um exemplo de protocolo criptográfico.

Fique atento

Segundo Bishop (2018), um criptossistema é uma quíntupla (E, D, M, K, C), onde M corresponde ao conjunto de textos limpos, K ao conjunto de chaves, C ao conjunto de cifras ou algoritmos criptográficos, E: M × K → C ao conjunto de funções de encriptação e D: C × K → M ao conjunto de funções de decriptação.

Criptografia simétrica

Os esquemas de criptografia simétrica também são chamados de chave simétrica, chave secreta e esquemas ou algoritmos de chave única. A criptografia simétrica pode ser melhor introduzida por meio de um cenário simples, como o ilustrado na Figura 4. Existem dois usuários, Alice e Bob, que desejam se comunicar por meio de um canal inseguro. O canal é apenas um termo geral para o *link* de comunicação, que pode ser a internet, o ar (no caso de telefones celulares ou comunicação LAN sem fio) ou qualquer outro meio de comunicação. O problema real começa com um terceiro indivíduo mal intencionado, Oscar, que tem acesso ao canal, por exemplo, ao invadir um roteador de internet ou ouvir os sinais de rádio de uma comunicação Wi-Fi. Ele consegue escutar clandestinamente a troca de mensagens. Naturalmente, muitas são as situações em que Alice e Bob preferem se comunicar sem que sejam escutados por Oscar. Por exemplo, se Alice e Bob representam dois escritórios de um fabricante de automóveis e estão transmitindo documentos com a estratégia de negócios para a introdução de novos modelos de automóveis nos próximos anos, esses documentos não devem chegar às mãos de seus concorrentes ou de agências de inteligência estrangeiras que têm interesse no projeto.

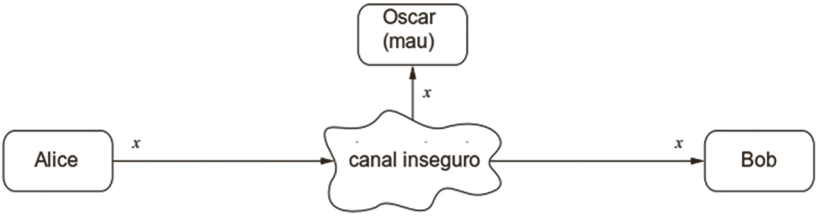

Figura 4. Comunicação por meio de um canal inseguro.
Fonte: Adaptada de Paar e Pelzl (2010).

Nessa situação, a criptografia simétrica oferece uma solução poderosa. Alice criptografa sua mensagem *x* usando um algoritmo simétrico, gerando o texto cifrado *y*. Bob recebe o texto cifrado e descriptografa a mensagem. A descriptografia é, portanto, o processo inverso de criptografia. Todo esse processo é ilustrado na Figura 5. A principal vantagem desse criptossistema está no uso de um algoritmo de criptografia forte. Nesse caso, o texto cifrado parecerá bits aleatórios para Oscar e não conterá qualquer informação útil para ele. Os elementos *x*, *y* e *k* na Figura 5 correspondem ao texto limpo, ao texto cifrado e à chave, respectivamente. O sistema precisa de um canal seguro para a distribuição da chave entre Alice e Bob. O canal seguro mostrado nessa figura poderia ser, por exemplo, uma pessoa que está transportando a chave em uma carteira entre Alice e Bob. Um exemplo prático em que esse método funciona é o das chaves pré-compartilhadas, usadas na criptografia de acesso protegido por Wi-Fi em redes sem fio. Em qualquer caso, a chave só precisa ser transmitida uma vez entre Alice e Bob e então pode ser usada para proteger qualquer comunicação subsequente.

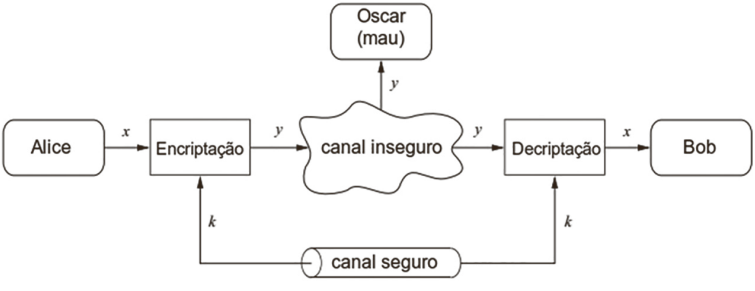

Figura 5. Criptossistema de chave simétrica.
Fonte: Adaptada de Paar e Pelzl (2010).

Um fato importante nesse esquema criptográfico é que os algoritmos de encriptação e decriptação são conhecidos publicamente. Aparentemente, manter o segredo do algoritmo de criptografia deveria tornar todo o sistema mais difícil de ser quebrado. No entanto, algoritmos mantidos em sigilo também significam algoritmos que não são testados. De fato, a única maneira de encontrar e verificar se um método de criptografia é forte, ou seja, que não pode ser quebrado por um determinado atacante, é torná-lo público e deixá-lo ser analisado por outros criptógrafos.

As cifras simétricas datam de períodos anteriores aos computadores e, portanto, funcionam sobre letras em vez de bits. Existem várias dessas cifras, mas as mais famosas são a cifra de deslocamento ou de César, a cifra Afim e a cifra de Vigenère. A cifra de César recebeu esse nome porque o historiador romano Suetônio relatou que Júlio César fez uso dela. Ele criptografava uma mensagem substituindo cada uma das letras pela corresponde a três posições atrás no alfabeto. Por exemplo, a palavra SAGAH seria criptografada como VDJDK, e FHVDU seria descriptografada como CESAR. A cifra de deslocamento também pode ser elegantemente descrita usando aritmética modular. Para a representação matemática da cifra, as letras do alfabeto são codificadas como números, como apresentado no Quadro 1.

Quadro 1. Codificação de letras usadas pela cifra de César

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

A funções de encriptação e decriptação da cifra são expressas como:

$$\text{Encriptação: } Ek(x) = y \equiv x + k \bmod 26$$
$$\text{Decriptação: } Dk(y) = x \equiv y - k \bmod 26$$

Como exemplo, pense que seja $k = 7$ a chave da cifra de deslocamento e o seguinte texto limpo:

$$\text{ATAQUE} = x_1, x_2, \ldots, x_6 = 0, 19, 0, 16, 20, 4$$

Nesse caso, o texto cifrado é dado como:

$$y_1, y_2, \ldots, y_6 = 7, 0, 7, 23, 1, 11 = \text{HAHXBL}$$

Fique atento

Operação módulo: sejam a, r e m números inteiros e $m > 0$. A operação $a \equiv r \bmod m$ é válida se m divide $a - r$. Além disso, m é o módulo e r, o resto. Por exemplo, seja $a = 42$ e $m = 9$. Então, $42 = 4 \cdot 9 + 6$ e, portanto, $42 \equiv 6 \bmod 9$.

Como observado, a cifra de deslocamento é simples de ser quebrada: para descriptografar um determinado texto cifrado, simplesmente desloque as letras *k* (a chave) de posições de volta para recuperar o texto original (texto limpo). Demorou cerca de 1.500 anos para que uma melhoria significativa na cifra de César fosse proposta na forma da cifra de Vigenère. Criada por Giovan Battista Bellaso, o nome dessa cifra vem do francês Blaise de Vigenère, que inventou uma cifra diferente no século XVI, mas devido à má atribuição histórica, foi o nome de Vigenère que permaneceu. No entanto, a cifra de Vigenère se tornou popular e foi mais tarde usada durante a Guerra Civil Americana pelas forças confederadas e durante a Primeira Guerra Mundial pelo exército suíço, entre outros casos (AUMASSON, 2018).

A cifra de Vigenère é semelhante à cifra de César, com a diferença que as letras não são deslocadas de um número fixo de posições, mas sim por valores definidos por uma chave, uma coleção de letras que representam números com base em sua posição no alfabeto. Por exemplo, se a chave é DUH, as letras do texto limpo são alteradas usando os valores 3, 20 e 7, pois D é a terceira letra depois de A, U é a vigésima letra depois de A e H é a sétima letra após A. O padrão 3, 20, 7 se repete até criptografar todo o texto simples. Por exemplo, a palavra CRYPTO seria criptografada como FLFSNV, usando DUH como a chave: C é deslocado três posições para F, R é deslocado 20 posições para L e assim por diante. A Figura 6 ilustra esse princípio ao criptografar a palavra VULNERABILIDADE.

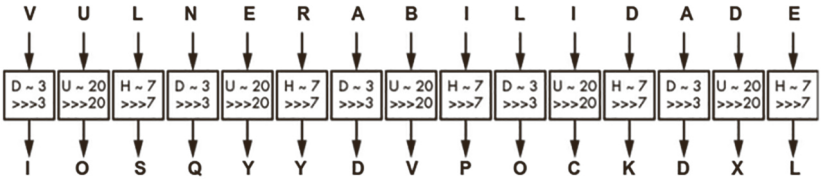

Figura 6. A cifra de Vigenère.
Fonte: Aumasson (2018, p. 27).

O terceiro exemplo de cifra simétrica, a cifra Afim, corresponde a mais uma melhoria da cifra de deslocamento, feita por meio da generalização da função de criptografia. Cabe lembrar que a criptografia real da cifra de deslocamento envolvia a adição da chave, ou seja, $y_i = x_i + k \bmod 26$. A cifra Afim realiza a criptografia multiplicando o texto limpo por uma parte da chave, seguida pela adição de outra parte da chave. A representação matemática dessa cifra é:

$$\text{Encriptação: } E_k(x) = y \equiv a \cdot x + b \bmod 26$$
$$\text{Decriptação: } D_k(y) = x \equiv a^{-1} \cdot (y - b) \bmod 26$$

onde x, y, a e b são números inteiros pertencentes ao intervalo $[-26, 26]$ e $k = (a, b)$ corresponde à chave de criptografia com a restrição de que o máximo divisor comum entre a e 26 deve ser 1, ou seja, MDC$(a, 26) = 1$. Para exemplificar, seja a chave $k = (a, b) = (9, 13)$ e o seguinte texto limpo:

$$\text{ATAQUE} = x_1, x_2, \ldots, x_6 = 0, 19, 0, 16, 20, 4$$

Neste caso, o inverso a^{-1} de a existe e é dado por $a^{-1} = 3$. Assim, o texto cifrado é computado como:

$$y_1, y_2, \ldots, y_6 = 13, 2, 13, 1, 11, 23 = \text{NCNBLX}$$

Fique atento

Na cifra Afim, a restrição de MDC$(a, 26) = 1$ decorre do fato de que o elemento a da chave precisa a ser invertido para fins de descriptografia. Para que o inverso de a exista, é preciso que a seja primo relativo com o módulo. Assim, a deve pertencer ao conjunto:

$$a \in \{1,3,5,7,9,11,15,17,19,21,23,25\}$$

Além disso, para que a^{-1} seja encontrado, uma estratégia de tentativa e erro pode ser empregada. Isso significa que, para um dado a, basta testar todos os valores possíveis de a^{-1} até que a seguinte relação seja válida: $a \cdot a^{-1} \equiv 1 \bmod 26$. Por exemplo, se $a = 3$, então $a^{-1} = 9$, uma vez que $3 \cdot 9 = 27 \equiv 1 \bmod 26$. Vale observar que a^{-1} também satisfaz à condição de que $\text{MDC}(a^{-1}, 26) = 1$.

Um aspecto que deve ser considerado a respeito da cifra Afim é a sua segurança. O seu espaço de chaves é apenas um pouco maior do que no caso da cifra de deslocamento:

$$\text{Espaço de chaves} = (\#\text{valores para } a) \cdot (\#\text{valores para } b) = 12 \cdot 26 = 312$$

Um espaço de chaves com 312 elementos pode, naturalmente, ser explorado exaustivamente por meio de um ataque de força bruta. Esse processo demandaria uma fração de segundo usando simples computadores domésticos. Além disso, a cifra Afim tem a mesma fraqueza que a cifra de deslocamento: o mapeamento entre as letras do texto limpo e as letras de texto cifrado é fixo. Portanto, pode facilmente ser quebrado com a análise de frequência de letras.

Criptografia assimétrica

A introdução da criptografia assimétrica ou chave pública marcou uma revolução na criptografia. Até então, os criptógrafos confiavam exclusivamente em chaves secretas e compartilhadas para conseguir uma comunicação privada. No entanto, esquemas de chave simétrica apresentavam as seguintes deficiências intrínsecas (PAAR; PELZL, 2010).

- Problema de distribuição de chaves: a chave deve ser estabelecida entre Alice e Bob usando um canal seguro. Porém, o canal de comunicação da mensagem não é seguro. Assim, enviar a chave diretamente pelo canal — o que seria a mais maneira conveniente de transportá-la — não é viável.
- Número de chaves: mesmo se o problema de distribuição de chaves fosse resolvido, haveria, ainda assim, um número potencialmente grande de chaves para serem manipuladas. De fato, se cada par de usuários precisar de um par de chaves em uma rede com n usuários, haveria $\frac{n \cdot (n-1)}{2}$ pares de chaves, e cada usuário deveria armazenar

$n - 1$ chaves com segurança. Mesmo para redes de médio porte, como uma empresa com 2.000 pessoas, isso requer mais de 4 milhões de chaves pares, que devem ser geradas e transportadas por meio de canais seguros.

Para superar essas desvantagens, uma ideia revolucionária foi proposta: não é necessário que a pessoa (Alice, seguindo o exemplo) que deseja criptografar uma mensagem possua uma chave secreta. A parte crucial é que Bob, o receptor, só pode descriptografar usando uma chave secreta. Para viabilizar um sistema assim, Alice deve ter acesso à chave de criptografia pública de Bob que é conhecida por todos. Bob também tem uma chave secreta correspondente, usada para descriptografar. Assim, a chave k de Bob consiste em duas partes: uma pública, pk, e uma privada, sk. A Figura 7 apresenta uma visão esquemática dessa comunicação.

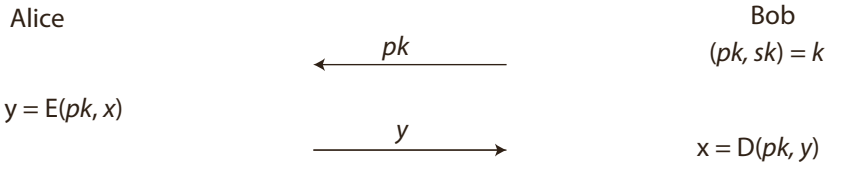

Figura 7. Funcionamento básico da criptografia de chave pública.
Fonte: Adaptada de Paar e Pelzl (2010).

Como o objetivo é evitar a necessidade de duas partes se encontrarem com antecedência para chegar a um acordo sobre qualquer informação, uma questão permanece em relação a como o remetente (Alice) tem acesso à chave pk de Bob. Em um nível abstrato, isso poderia ocorrer de duas maneiras. Na primeira abordagem, quando Bob descobre que Alice deseja se comunicar com ele, ele pode, nesse ponto, gerar o seu par de chaves (pk, sk) — assumindo que ele ainda não o tenha feito — e, em seguida, enviar sua chave pública pk para Alice. Alice então pode usar a chave pk para criptografar sua mensagem. Cabe enfatizar que o canal entre Alice e Bob pode ser público. Porém, presume-se que esse canal seja autenticado, ou seja, um outro indivíduo não pode modificar a chave pública enviada por Bob para Alice nem pode substitui-la por sua própria chave (KATZ; LINDELL, 2015).

Fique atento

Na criptografia assimétrica, a chave *pk* é inerentemente pública e, portanto, pode ser facilmente capturada por um indivíduo mal intencionado. Para isso, ele pode escutar a comunicação entre as partes envolvidas e obter a *pk* diretamente. Outra maneira de conseguir a chave é o invasor procurá-la por conta própria. Dessa forma, fica evidente que a segurança da criptografia de chave pública não pode depender do sigilo da *pk*, mas sim do sigilo da chave privada *sk* correspondente. Portanto, é crucial que o receptor não revele sua chave privada a ninguém, o que inclui o próprio remetente.

Uma abordagem alternativa é Bob gerar suas chaves (*pk*, *sk*) com antecedência, independentemente de qualquer remetente em particular. Na verdade, no momento da geração da chave, Bob não precisa nem mesmo estar ciente de que Alice deseja falar com ele, ou mesmo que Alice existe. Bob então pode divulgar amplamente sua chave pública *pk* publicando essa chave em sua página na *web* ou colocando em seus cartões de visita ou em um diretório público, por exemplo. Agora, qualquer pessoa que desejar se comunicar em particular com Bob pode procurar sua chave pública e proceder como descrito. Vale ressaltar que vários remetentes podem se comunicar várias vezes com Bob usando a mesma chave pública *pk* para criptografar todas as suas comunicações.

A ideia de um criptossistema de chave pública foi apresentada por Diffie e Hellman, dois criptógrafos norte-americanos, em 1976. Então, em 1977, Rivest, Shamir e Adleman inventaram o conhecido algoritmo RSA. Vários sistemas de chave pública foram propostos, cuja segurança depende de diferentes problemas computacionais. Desses, um dos mais importantes é o RSA e as variações dele, em que a segurança é baseada na dificuldade de se fatorar números inteiros grandes (STINSON; PATERSON, 2018).

Saiba mais

Saiba mais sobre a criptografia de chave pública no trecho a seguir:

> Antes de Diffie e Hellman, a ideia de criptografia de chave pública já havia sido proposta por James Ellis em janeiro de 1970, em um artigo intitulado A Possibilidade de Criptografia não Secreta (a frase "criptografia não secreta" pode ser lida como "criptografia de chave pública"). James Ellis era membro de uma seção especial do governo britânico [...]. Esse artigo não foi publicado na literatura aberta e foi um dos cinco artigos lançados oficialmente em dezembro de 1997. Também incluído nesses cinco artigos estava um artigo de 1973 escrito por Clifford Cocks intitulado Uma Nota sobre Encriptação não Secreta, no qual um criptossistema de chave pública é descrito, e é essencialmente o mesmo que o criptossistema RSA (STINSON; PATERSON, 2018, p. 186, tradução nossa).

As funções de encriptação e decriptação RSA são apresentadas a seguir.

- Encriptação RSA: dada uma chave pública $pk = (n, e)$ e um texto limpo x, a função de encriptação é:

$$y = E(x, e) \equiv x_e \bmod n$$

onde x, y são números inteiros pertencentes ao intervalo $[-n, n]$.

- Decriptação RSA: dada uma chave privada $sk = d$ e um texto cifrado y, a função de decriptação é expressa por:

$$x = D(y, d) \equiv y_d \bmod n$$

onde x, y são números inteiros pertencentes ao intervalo $[-n, n]$.

Na prática, x, y, n e d são números muito longos, geralmente com 1.024 bits ou mais. O valor e às vezes é referenciado como expoente de criptografia ou expoente público, e a chave privada d às vezes é chamada de expoente de descriptografia ou expoente privado. Se Alice deseja enviar uma mensagem criptografada para Bob, ela precisa ter sua chave pública (n, e), e Bob descriptografa com sua chave privada d. Como exemplo, suponha que Alice queira enviar para Bob uma mensagem cujo conteúdo seja o número 88. Para isso, considerando a chave pública de Bob como $pk = (7, 187)$ e a respectiva chave privada como $d = 23$, a Figura 8 descreve como os processos de encriptação e decriptação são realizados pelo algoritmo RSA.

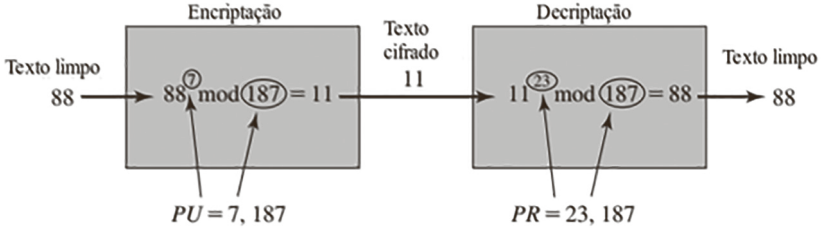

Figura 8. Exemplo do algoritmo RSA.
Fonte: Adaptada de Stallings e Brown (2015).

Uma característica distintiva de todos os esquemas de criptografia assimétrica é que há uma fase de configuração durante a qual as chaves pública e privada são calculadas. Dependendo do esquema de chave pública, a geração de chaves pode ser muito complexa. O algoritmo a seguir descreve as etapas envolvidas no cálculo da chave pública e privada para um criptossistema RSA. No passo 4, a condição de que MDC(e, $\varphi(n)$) = 1 garante que o inverso de e exista no módulo $\varphi(n)$, de modo que sempre haja uma chave privada d.

Saída: chave pública $pk = (n, e)$ e chave privada $sk = d$

1. Escolha dois números primos p e q suficientemente grandes.
2. Compute $n = p \cdot q$.
3. Compute $\varphi(n) = (p - 1)(q - 1)$.
4. Selecione um expoente público e pertencente a $\{1, 2, ..., \varphi(n - 1)\}$ tal que MDC(e, $\varphi(n)$) = 1.
5. Compute a chave privada d tal que $d \cdot e \equiv \text{mod } \varphi(n)$.

Como novo exemplo, suponha que Alice deseja enviar uma mensagem criptografada para Bob. A princípio, Bob calcula seus parâmetros RSA usando os passos de 1 a 5 do algoritmo. Ele então envia para Alice sua chave pública. Alice criptografa a mensagem ($x = 4$) e envia o texto cifrado y para Bob, que o descriptografa usando sua chave privada. A Figura 9 detalha o passo a passo para que essa comunicação aconteça de forma segura com o suporte do algoritmo RSA. Vale observar que os expoentes privado e público cumprem a condição $e \cdot d = 3 \cdot 7 \equiv 1 \text{ mod } \varphi(n)$.

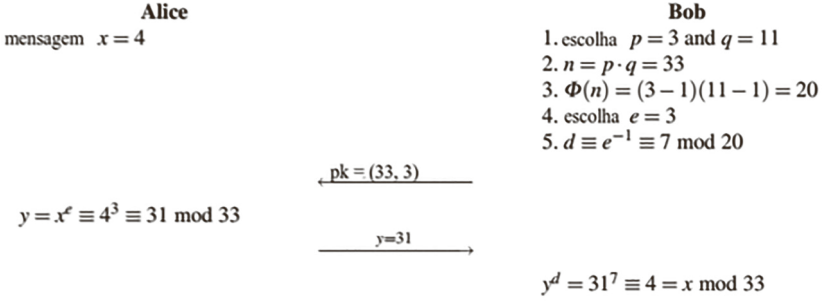

Figura 9. Exemplo de geração de chaves e criptografia RSA.
Fonte: Adaptada de Paar e Pelzl (2010).

Criptografia e aplicações

Os fundamentos matemáticos e os algoritmos computacionais baseados em conceitos criptográficos podem ser encontrados nas mais variadas aplicações. Por se tratar de uma estratégia de criptografia com mais tempo de uso, a criptografia simétrica pertence à realidade de praticamente todas as aplicações digitais nos mais diversos setores (ARAMPATZIS, 2019).

Setor bancário. Devido ao melhor desempenho e à velocidade mais rápida da criptografia simétrica, ela é normalmente usada para criptografia em massa de grandes quantidades de dados. As aplicações de criptografia simétrica no setor bancário incluem as seguintes (ARAMPATZIS, 2019, documento *on-line*, tradução nossa).

- Aplicativos de pagamento, como transações de cartão em que PII (Personal Identfying Information, ou Informações de Identificação Pessoal, em tradução livre) precisam ser protegidos para evitar roubo de identidade ou cobranças fraudulentas sem grandes custos de recursos. Isso ajuda a reduzir o risco envolvido em lidar com transações de pagamento diariamente.
- Validações para confirmar se o remetente de uma mensagem é quem afirma ser.

Dados em repouso. Os dados em repouso são os que não estão se movendo ativamente de um dispositivo para outro ou de rede para rede, como dados armazenados em um disco rígido, *laptop*, unidade *flash* ou arquivados/armazenados de alguma outra forma. Os dados em repouso são considerados menos vulneráveis que os em trânsito. Contudo, invasores costumam considerá-los um alvo mais valioso. Para proteger os dados em repouso, as empresas podem criptografar arquivos confidenciais antes de armazená-los ou criptografar a própria unidade de armazenamento (ARAMPATZIS, 2019).

De acordo com Arampatzis (2019, documento *on-line*, tradução nossa), a melhor forma de criptografar dados em repouso é:

> [...] por meio da criptografia do disco inteiro. A criptografia de disco completo tem vários benefícios em comparação à criptografia regular de arquivos, pastas ou cofres criptografados. Quase tudo, incluindo o espaço de troca e os arquivos temporários, é criptografado. Criptografar esses arquivos é importante, pois eles podem revelar dados confidenciais importantes. No entanto, com uma implementação de *software*, o código de inicialização não pode ser criptografado. Por exemplo, a criptografia de unidade de disco conhecida como BitLocker deixa um volume

não criptografado para ser inicializado, enquanto o volume que contém o sistema operacional é totalmente criptografado. Além disso, a decisão de quais arquivos individuais criptografar não é deixada ao critério dos usuários. Isso é importante para situações em que os usuários podem não querer ou podem esquecer de criptografar arquivos confidenciais.

Em contrapartida, um típico e amplamente difundido uso da criptografia assimétrica é para o provimento de **assinaturas digitais**. Uma assinatura digital é uma forma de uma entidade demonstrar a autenticidade de uma mensagem vinculando sua identidade a essa mensagem. A propriedade de provar que determinada pessoa gerou uma mensagem também é muito importante fora do domínio digital. No mundo real (analógico), isso é conseguido por meio de assinaturas manuscritas no papel. Assim como acontece com as assinaturas manuscritas convencionais, apenas a pessoa que cria uma mensagem digital deve ser capaz de gerar uma assinatura válida. Para conseguir isso com primitivas criptográficas, é preciso aplicar a criptografia de chave pública.

A ideia básica é que a pessoa que assina a mensagem usa uma chave privada, e a parte receptora usa a chave pública correspondente. A estrutura geral é que Alice deve ser capaz de usar sua chave privada com um algoritmo de assinatura para produzir uma assinatura digital, SAlice(M), para uma mensagem M. Além disso, dada a chave pública de Alice, a mensagem M e a assinatura Salice(M) de Alice, deve ser possível para a outra parte, Bob, verificar a assinatura de Alice em M, usando apenas esses elementos (GOODRICH; TAMASSIA, 2014). A Figura 10 ilustra esse processo.

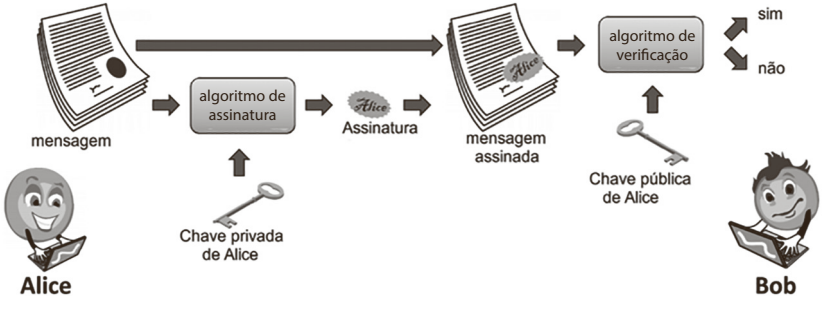

Figura 10. Processo de assinatura digital de Alice e de verificação de assinatura por Bob.
Fonte: Adaptada de Goodrich e Tamassia (2014).

Um esquema de assinatura digital comumente utilizado atualmente faz uso da criptografia de chave pública RSA. Ao usar esse criptossistema, Alice deve criar uma chave pública, (e, n), para que outras partes possam criptografar uma mensagem M como $C_e \bmod n$. No esquema de assinatura RSA, Alice criptografa uma mensagem M usando sua chave secreta d da seguinte forma:

$$S = Md \bmod n$$

Qualquer terceiro pode verificar essa assinatura testando a seguinte condição:

$$\text{É verdadeiro que } M = S^e \bmod n?$$

O método de verificação segue do fato que $d \cdot e \equiv 1 \bmod \varphi(n)$. Além disso, a verificação do esquema de assinatura RSA envolve o mesmo algoritmo da criptografia RSA e usa a mesma chave pública, (e, n), de Alice.

Neste capítulo, os conceitos centrais de criptografia foram contextualizados, desde suas origens até as aplicações mais modernas. Na perspectiva das principais estratégias criptográficas, tanto o esquema de chave simétrica quanto o de chave assimétrica ou pública foram detalhados. Além disso, foram abordados, com exemplos práticos, os principais algoritmos e técnicas que implementam essas duas abordagens.

Referências

ARAMPATZIS, A. *What are the best use cases for symmetric vs asymmetric encryption?* 2019. Disponível em: https://www.venafi.com/blog/what-are-best-use-cases-symmetric-vs-asymmetric-encryption. Acesso em: 12 jul. 2021.

AUMASSON, J.-F. *Serious cryptography*: a practical introduction to modern encryption. San Francisco, CA: No Starch, 2018.

BISHOP, M. *Computer security*: art and science. 2nd ed. Boston, MA: Addison-Wesley, 2018.

CRIPTOGRAFIA. *In*: DICIONÁRIO Priberam da Língua Portuguesa. Lisboa: Priberam Informática, c2021. Disponível em: https://dicionario.priberam.org/criptografia. Acesso em: 11 jul. 2021.

GOODRICH, M.; TAMASSIA, R. *Introduction to computer security*. Harlow, UK: Pearson, 2014.

KATZ, J.; LINDELL, Y. *Introduction to modern cryptography*. 2nd ed. Boca Raton, FL: Taylor & Francis, 2015.

MEDEIROS, F. *Uma breve história sobre criptografia*. Crypto Id, 2015. Disponível em: https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/. Acesso em: 12 jul. 2021.

PAAR, C.; PELZL, J. *Understanding cryptography*: a textbook for students and practitioners. Berlin: Springer, 2010.

STALLINGS, W.; BROWN, L. *Computer security*: principles and practice. 3rd ed. Harlow, UK: Pearson, 2015.

STINSON, D. R.; PATERSON, M. B. *Cryptography*: theory and practice. 4th ed. Boca Raton, FL: Taylor & Francis, 2018.

VAUDENAY, S. *A classical introduction to cryptography*: applications for communications security. Berlin: Springer, 2006.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Criptografia aplicada a *blockchain*

Juliane Adelia Soares

OBJETIVOS DE APRENDIZAGEM

- Conceituar criptografia com *blockchain*.
- Integrar criptografia com *blockchain*.
- Apresentar exemplos de criptografia com *blockchain*.

Introdução

Novas tecnologias e novos dispositivos estão surgindo a todo momento para atender a demandas de diferentes áreas. Essa revolução tecnológica traz inúmeros benefícios para a sociedade, como, por exemplo, a realização de transações financeiras e compras *on-line*. No entanto, isso também gera diariamente um número considerável de dados, que ficam armazenados no ciberespaço e, assim, são mais facilmente acessados por cibercriminosos.

É, portanto, fundamental investir em sistemas seguros. Para atender a essa necessidade, tem-se mostrado uma alternativa bastante relevante a *blockchain*, um sistema de banco de dados descentralizado que armazena dados de transações. Estas, então, são efetuadas de forma rápida e mantidas em segurança com o uso da criptografia.

Neste capítulo, você vai conhecer os principais aspectos da criptografia no contexto de *blockchain* e compreender como essas duas tecnologias funcionam de maneira integrada. Por fim, vamos exemplificar a aplicação da criptografia na tecnologia *blockchain*.

Criptografia no contexto de *blockchain*

Com o crescente número de dispositivos e sistemas tecnológicos, a segurança digital tem se tornado um fator de preocupação, pois os ataques de cibercriminosos estão a cada dia mais sofisticados. Isso também ocorre com a *blockchain*.

Segundo Bashir (2017), a *blockchain* pode ser definida de diferentes formas, a depender da maneira como ela é analisada. Algumas das definições existentes são as seguintes:

- mecanismo de consenso descentralizado, em que todos os pares eventualmente chegam a um acordo em relação ao estado de uma transação;
- livro-razão compartilhado e distribuído de transações, que são ordenadas e agrupadas em blocos; seu modelo distribuído serve como fonte única de verdade para todas as organizações que o utilizam;
- estrutura de dados, ou seja, pode ser considerado uma lista vinculada que utiliza ponteiros de *hash*, que são usados para apontar o bloco anterior.

Basicamente, a *blockchain* é um livro-razão distribuído ponto a ponto, que roda sobre a internet, criptograficamente seguro, imutável e que se atualiza apenas por consenso ou acordo entre pares. Em uma plataforma de *blockchain*, os pares podem trocar valores utilizando transações sem que seja necessário um arbitrador central confiável, o que faz com que nenhuma autoridade seja responsável pelo banco de dados (BASHIR, 2017).

O livro-razão facilita o processo de registro de transações e rastreamento de ativos (tangíveis e intangíveis) em uma rede de negócios. É grande o leque de coisas que podem ser rastreadas e negociadas em uma rede *blockchain* de modo que riscos e custos sejam reduzidos para todos os envolvidos. Como os negócios funcionam na base da informação, essa tecnologia é importante porque fornece imediatamente tais informações, que são compartilhadas, transparentes e podem ser acessadas somente por pessoas autorizadas. Na rede *blockchain*, podem-se rastrear pedidos, pagamentos, contas, produção, etc., sendo possível ver os detalhes de uma transação de ponta a ponta (GUPTA, 2017).

Como todos os participantes da rede *blockchain* têm acesso ao livro-razão distribuído e ao registro de transações (que é imutável), todas as transações são registradas uma única vez, eliminando-se duplicações. Dizer que os registros são imutáveis significa que, uma vez armazenados na *blockchain*, eles

não poderão mais ser alterados, e, em caso de erros, uma nova transação deverá ser adicionada, ficando ambas visíveis (GUPTA, 2017).

Cada uma das transações é registrada como bloco de dados, e os usuários escolhem as informações que serão registradas (quem, o quê, quando, onde, etc.). Cada um desses blocos está conectado aos anteriores e aos posteriores. Sendo assim, uma referência a um bloco anterior também é incluída ao bloco, caso não seja um bloco de origem. Geralmente, sua estrutura varia de acordo com o tipo e o *design* da *blockchain*, mas alguns atributos são essenciais para a funcionalidade do bloco, como o cabeçalho, os ponteiros para blocos anteriores, o carimbo de data e hora, o contador de transações, entre outros (BASHIR, 2017).

Garantir a segurança das informações do usuário e dos dados das transações é uma condição obrigatória em uma *blockchain*. Essa segurança pode ser obtida por meio da criptografia, que torna os dados incompreensíveis a fim de garantir sua confidencialidade. Para tanto, é usado um algoritmo, chamado de "cifra", e um valor secreto, denominado "chave". Se a chave secreta não for conhecida por quem obtiver o arquivo, não será possível descriptografá-lo, nem apreender qualquer informação sobre a mensagem criptografada (AUMASSON, 2018).

O funcionamento básico da criptografia é apresentado na Figura 1, em que se pode observar que o texto original é cifrado, sendo transformado em uma aparente pilha inútil de letras e números, e, em seguida, descriptografado, recuperando-se o texto original.

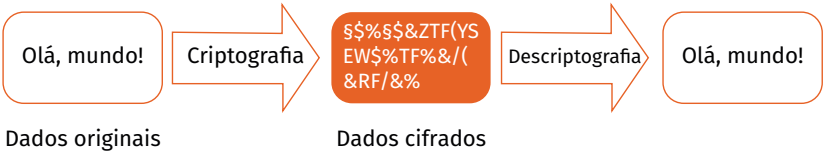

Figura 1. Esquema básico de criptografia.
Fonte: Adaptada de Drescher (2017).

Necessária para criar um meio confiável de identificação, autenticação e autorização que assegure a segurança dos dados, a criptografia pode ser classificada, de acordo com Vallim (2019), em chave simétrica e chave assimétrica.

A **chave simétrica** faz uso da mesma chave para cifragem e decifragem da mensagem, conforme ilustra a Figura 2.

Figura 2. Chave simétrica.
Fonte: Adaptada de Drescher (2017).

Dessa forma, algoritmos simétricos podem ser considerados mais simples e com processamento mais rápido se comparados a algoritmos assimétricos. Quando se trata de grandes volumes de dados, utilizar chave simétrica pode ser vantajoso. No entanto, esse método apresenta algumas vulnerabilidades no processo de comunicação de senha, justamente na parte que a torna mais eficiente, pois todos os envolvidos na transação devem conhecer a mesma chave. Assim, não é possível identificar o criador da mensagem, o que torna mais fácil que uma alteração maliciosa feita por um terceiro que conheça a chave ocorra sem ser percebida.

Já a **chave assimétrica** faz uso de duas chaves, uma utilizada para cifrar e outra para decifrar, como se pode observar na Figura 3. A parte superior da ilustração apresenta a criptografia, e a parte inferior, a descriptografia. O texto cifrado em preto só poderá ser decifrado com o texto em branco e vice-versa.

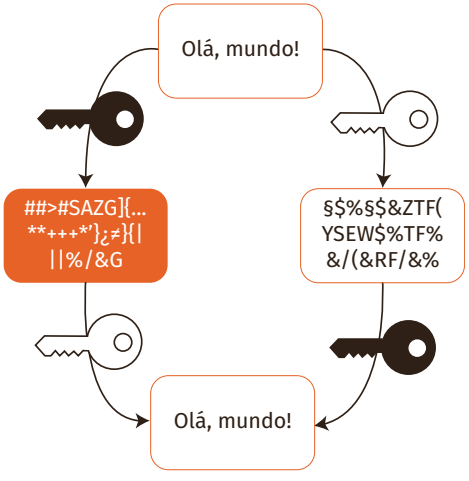

Figura 3. Chave assimétrica.
Fonte: Adaptada de Drescher (2017).

A chave utilizada para cifrar a mensagem é privada, secreta, sendo conhecida somente pelo criador da mensagem. Já a chave para decifrar a mensagem é pública, ou seja, é conhecida por todos. Entretanto, ambas as chaves são geradas de modo simultâneo por um algoritmo e são correlatas. Dessa forma, apenas o destinatário conseguirá acessar o conteúdo da mensagem, garantindo sua autoria. A desvantagem da chave assimétrica é que ela exige mais processamento que a chave simétrica, mas com a garantia de que a confidencialidade e a autenticidade das mensagens estejam protegidas.

Mas, afinal, qual é a relação entre *blockchain* e criptografia? Como a *blockchain* funciona como um modelo de rede ponto a ponto descentralizado, não existe apenas um nó. Além disso, esses nós não precisam confiar uns nos outros. Por isso, a *blockchain* deve garantir proteções adequadas para informações de transações que ocorrem em canais não seguros, enquanto mantém a integridade da transação. Assim, a criptografia é essencial para que a *blockchain* consiga, ao mesmo tempo, proteger as informações de transações e sua privacidade e assegurar a consistência dos dados.

A criptografia é utilizada em diversos lugares para fornecer segurança a uma rede *blockchain*, baseando-se em três conceitos básicos: *hashing*, chaves e assinaturas digitais. O *hash* é uma impressão digital única usada para verificar se as informações não foram alteradas, sem que seja necessário vê-las. As chaves, por sua vez, são usadas combinando-se públicas e privadas para criptografar e descriptografar as mensagens. Já a assinatura digital é um cálculo matemático utilizado para comprovar a autenticidade de uma mensagem ou de um documento digital (MOUGAYAR, 2016).

Mougayar (2016) afirma que, no contexto da *blockchain*, a criptografia é baseada na hegemonia público/privado, ou seja, há visibilidade pública, mas inspeção privada. Como analogia, você pode pensar em seu endereço residencial, que, embora possa ser publicado (isto é, tornado público), não fornece informações sobre o interior da sua residência. Sendo assim, você só poderá acessá-lo se tiver a chave privada, e, como esse endereço foi reivindicado como seu, ninguém mais poderá se apropriar dele.

A *blockchain* utiliza a criptografia de chave assimétrica, com o objetivo de identificar contas e autorizar transações, conforme define Drescher (2017).

- Identificação de contas: a *blockchain* precisa identificar usuários ou contas de usuários, com o intuito de manter o mapeamento entre proprietário e propriedade, e, para isso, utiliza uma abordagem público-privada. Como os números das contas na *blockchain* são chaves criptográficas públicas, os dados das transações fazem uso de chaves

públicas para identificar as contas que estão envolvidas na transferência de propriedade. Assim, as contas de usuários têm um endereço conhecido publicamente, e todos podem enviar mensagens para ele.

- Autorização de transações: os dados das transações devem conter uma informação que comprove que o proprietário da conta que transfere a propriedade realmente concorda com essa transação. Ou seja, o fluxo de informações implícito nesse acordo inicia com o proprietário da conta, que faz a transferência da propriedade e deve chegar a todos que realizam a inspeção dos dados da transação. Quando transfere a propriedade, o proprietário da conta cria um texto cifrado com sua chave cifrada e todos que tiverem sua chave criptográfica pública podem verificar essa prova de concordância.

O processo de criptografia envolve o uso de códigos matemáticos avançados para armazenar e transmitir valores de dados de forma segura. Com isso, é possível garantir que somente os usuários aos quais as transações ou os dados se destinam consigam obtê-los, lê-los e processá-los.

Na próxima seção, serão apresentadas as principais ferramentas utilizadas para garantir a integridade das informações na *blockchain*.

Integração entre criptografia e *blockchain*

A *blockchain* é um banco de dados distribuído, em que são permitidas transações diretas sem que seja necessária a atuação de um mediador autorizado. A criptografia *blockchain* encapsula transações na forma de blocos, de modo que esses blocos sejam vinculados por meio do *hash* criptográfico, formando uma cadeia de blocos protegidos.

A seguir, vamos apresentar, baseando-se em Gayoso Martínez, Hernández-Álvarez e Hernández Encinas (2020) e Raikwar, Gligoroski e Kralevska (2019), os principais conceitos criptográficos utilizados para que a integridade das informações seja garantida na *blockchain*.

Funções *hash*

Funções *hash* são funções capazes de transformar qualquer bloco de dados binários em outro bloco binário com tamanho fixo. O resultado dessa transformação é o chamado *hash*, ou *digest*. Observe os exemplos apresentados na Figura 4.

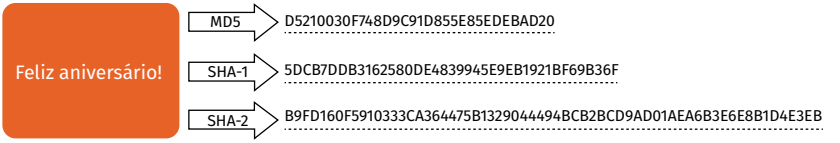

Figura 4. Exemplos de *hash*.

A Figura 4 mostra a transformação da frase "Feliz aniversário!" nas principais funções *hash*, detalhadas a seguir.

- MD5 (Message Digest 5): gera *hashes* de 128 bits e parou de ser utilizada quando foram publicadas algumas vulnerabilidades nela encontradas.
- SHA-1 (Secure Hash Algorithm-1): gera *hashes* de 160 bits e, embora apresente algumas colisões, ainda é utilizada.
- SHA-2 (Secure Hash Algorithm-2): a família de funções SHA-2 inclui funções SHA-224, SHA-256, SHA-384 e SHA-512, que fornecem *hashes* de 224, 256, 384 e 512 bits, respectivamente. As funções *hash* mais utilizadas na *blockchain* são SHA-256.

Na *blockchain*, as funções criptográficas de *hash* podem ser usadas para:

- resolver quebra-cabeças criptográficos, ou seja, a prova de trabalho (PoW, do inglês *proof of work*) em *bitcoin*;
- gerar endereços para chaves públicas e privadas;
- reduzir o tamanho de endereços públicos;
- resumir mensagens em assinaturas.

Saiba mais

A PoW serve para evitar comportamentos indesejados em uma rede, como ataques de negação de serviço (DoS, do inglês *denial of service*). Trata-se de um protocolo que funciona exigindo que o cliente execute ações, geralmente operações computacionais complexas (como o *captcha*, por exemplo). Assim que a ação é executada, ela é verificada pela rede. Se o desempenho do cliente for aprovado, os acessos solicitados por ele serão permitidos.

A Figura 5 mostra a estrutura básica de uma *blockchain*. Como ela é uma maneira de encapsular transações em forma de blocos, é por meio de *hash* criptográfico que esses blocos são vinculados, formando uma cadeia de blocos. Cada bloco tem um *hash* exclusivo, ou seja, sempre único e responsável por identificar um bloco e todo o seu conteúdo. Dessa forma, quando um bloco é criado, qualquer mudança ocorrida dentro dele fará com que o *hash* também mude.

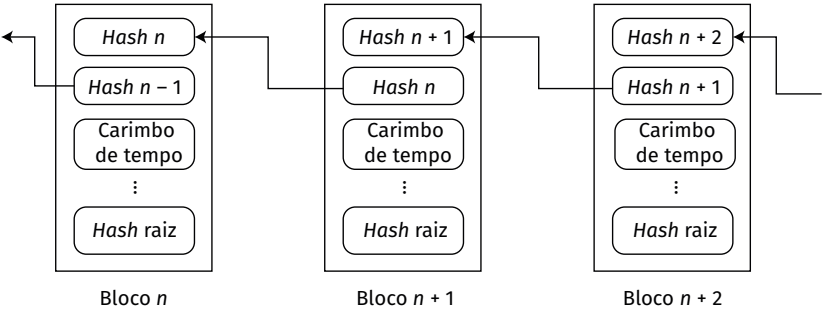

Figura 5. Estrutura básica de uma *blockchain*.
Fonte: Adaptada de Mohamed (2020).

Assinaturas digitais

Assim como a assinatura manuscrita, a assinatura digital visa a garantir a autoria de um documento a fim de evitar falsificações, podendo ser realizada mediante um certificado digital. Esse pode ser considerado o protocolo criptográfico mais utilizado atualmente.

Uma assinatura digital é um esquema matemático baseado em criptografia de chave pública, que produz códigos curtos, chamados "assinaturas de mensagens digitais", pelo uso de uma chave privada. Assim, essas assinaturas são verificáveis usando-se a chave pública correspondente.

Na *blockchain*, usa-se o esquema de assinatura para assinar transações, com o objetivo de autenticar o remetente e garantir a integridade da transação. A Figura 6 apresenta um exemplo do processo de criação de uma transação ou de um bloco assinado digitalmente por um usuário (signatário) da *blockchain*, utilizando sua chave privada.

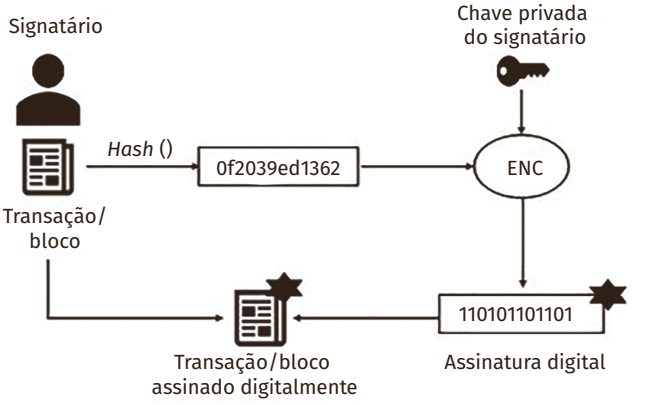

Figura 6. Processo de assinatura de transação/bloco.
Fonte: Adaptada de Raikwar, Gligoroski e Kralevska (2019).

A Figura 7 ilustra como os outros nós (verificador) da *blockchain* verificam a autenticidade da assinatura utilizando a chave pública do signatário.

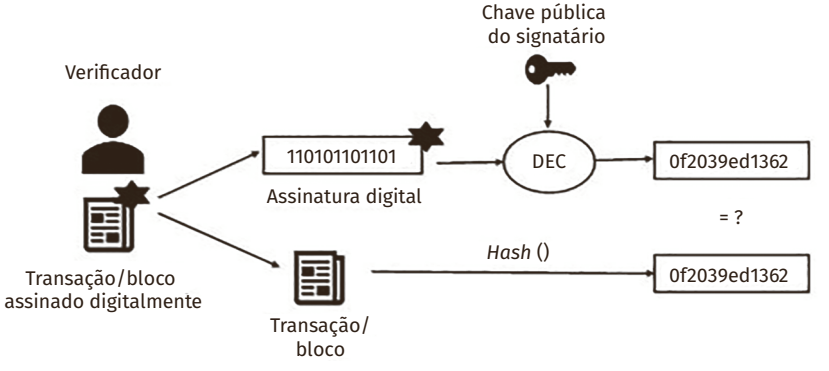

Figura 7. Verificação de assinatura da transação/bloco.
Fonte: Adaptada de Raikwar, Gligoroski e Kralevska (2019).

Conheça a seguir os diferentes métodos de assinatura utilizados na *blockchain* para adicionar recursos como privacidade, anonimato e desvinculação.

- Assinatura múltipla: uma única mensagem é assinada por um grupo de usuários.
- Assinatura cega: signatários e autores das transações são partes diferentes, fornecendo anonimato e desvinculação.
- Assinatura de anel: uma assinatura é criada por qualquer membro de um grupo, preservando a identidade do signatário individual.
- Assinatura de limite: quando *n* partes recebem uma parte da chave secreta, permitindo a criação da assinatura *t* sobre qualquer mensagem.

Na próxima seção, vamos apresentar exemplos de aplicação da criptografia em *blockchain*.

Criptografia aplicada a *blockchain*

Nas seções anteriores, você pôde compreender o que é *blockchain*, criptografia e os principais conceitos criptográficos usados nessa integração. Para facilitar o entendimento da aplicação da criptografia nesse processo, a seguir vamos exemplificar o funcionamento da *blockchain*.

As criptomoedas estão em alta, sendo hoje usadas em diversas transações. Seu próprio nome nos indica que se trata de moedas digitais protegidas por criptografia, o que torna quase impossível sua falsificação. Baseadas na tecnologia *blockchain*, as criptomoedas são sistemas que permitem a realização segura de pagamentos *on-line*, dispondo de diversos algoritmos de criptografia e técnicas criptográficas que protegem essas entradas.

Uma das criptomoedas mais populares é o *bitcoin*, que foi a primeira criptomoeda baseada em *blockchain*. Chaves assimétricas e assinaturas digitais são responsáveis por definir a propriedade de um *bitcoin*. O endereço *bitcoin* usado como receptor na transferência de propriedade é criado por uma chave pública, que é criada a partir de uma chave privada. Normalmente essas chaves são criadas por *software* específico, chamados, de forma genérica, de *wallets* (carteiras), que não dependem nem do protocolo *bitcoin*, nem da internet. Sendo assim, não é necessário que as chaves sejam armazenadas na rede, e, então, a segurança *bitcoin* depende de como os usuários protegem suas chaves privadas.

A Figura 8 mostra genericamente como um endereço *bitcoin* é gerado. Como se pode observar, primeiramente é gerada uma chave privada, que só pode ser vista pelo proprietário. A partir dela, ocorre a transformação algorítmica, gerando a chave pública. Esta, então, por meio das funções *hash*, geram o endereço do *bitcoin*, que é público, ou seja, pode ser visto por todos. Convém salientar que um *bitcoin* não armazena moedas digitais, como se pode ver, mas, sim, as chaves que permitem seu uso.

Figura 8. Endereço *bitcoin*.

Veja na Figura 9 um exemplo do funcionamento da *blockchain* e da integração com as demais tecnologias, inclusive a criptografia.

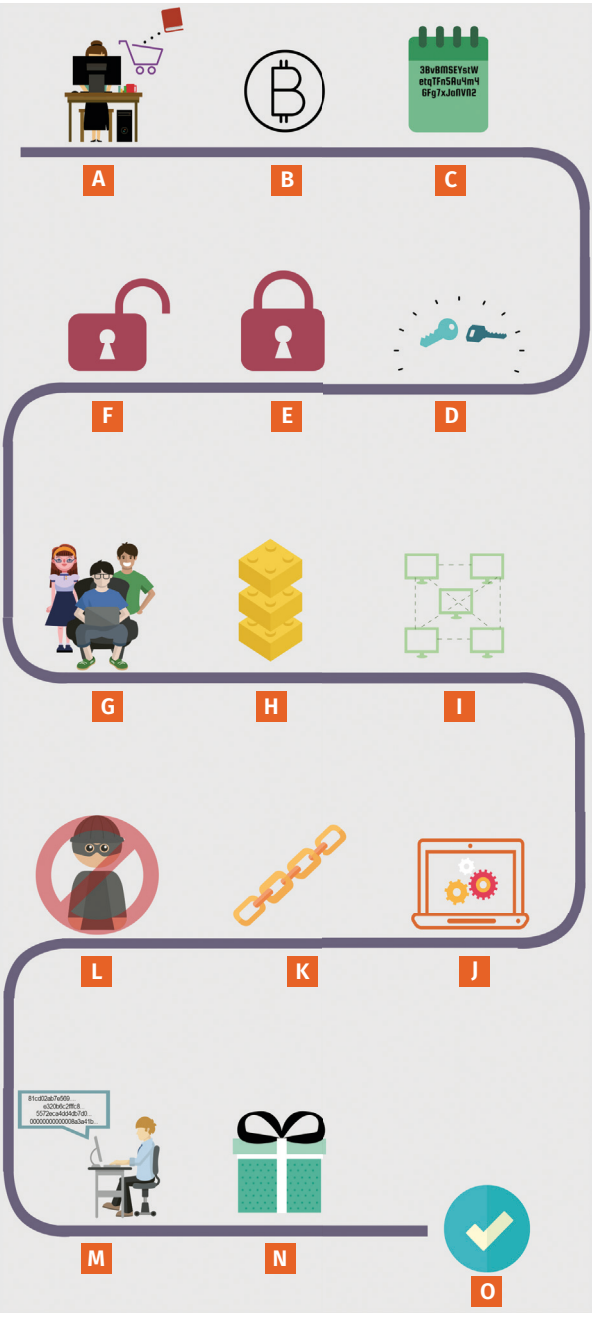

Figura 9. Exemplo de funcionamento *blockchain*.
Fonte: Adaptada de Al-Housni (2019).

A seguir são descritas as etapas de uma transação de *bitcoin*, ilustradas na Figura 9.

a) A usuária está realizando uma compra *on-line*, e a loja em questão aceita pagamento em *bitcoin*.
b) A usuária, que já tem uma carteira *bitcoin*, escolhe usar essa criptomoeda como forma de pagamento pelo produto desejado.
c) A loja envia à usuária seu endereço *bitcoin* (uma cadeia de 26 a 35 caracteres).
d) Os endereços costumam ser diferentes para cada transação, de modo a garantir a privacidade. Um endereço está vinculado a uma chave privada e a uma chave pública.
e) A usuária envia o pagamento para o endereço da loja. Ela assina a transação com a chave privada de seu próprio endereço (criada para essa determinada transação) e adiciona sua própria chave pública à transação.
f) Assim que é iniciada, a transação se propaga ponto a ponto em uma rede distribuída para todos os participantes. Com a chave pública, qualquer pessoa pode verificar a transação.
g) Os mineiros entram em jogo para garantir a autenticidade e a validação das transações, já que não existe uma autoridade central para esses fins. Assim, a transação é transmitida na forma de mensagem digital utilizando algoritmo criptográfico, e os mineiros validam as transações por meio da rede de trabalho. Essa autenticação ocorre mediante assinatura digital, que prova a propriedade do documento.
h) Após a verificação das transações, elas são registradas em blocos. A *blockchain* é a realização de um livro-razão público.
i) A *blockchain* é compartilhada em tempo real nos computadores dos mineiros e armazena o registro de todas as transações de *bitcoin* confirmadas.
j) Os computadores dos mineiros criam *hashes* criptográficos (sequências de letras e números) para armazenar uma transação na *blockchain*.
k) Todos os blocos são ligados entre si, e cada um deles contém os *hashes* dos blocos anteriores e atuais e, ainda, um "nonce" (um número aleatório).
l) A cada 10 minutos, é criado um novo bloco. Isso significa que, se um bloco gravado fosse modificado, seria necessário modificar todos os blocos seguintes, o que é quase impossível.

m) Um *hash* deve seguir um determinado parâmetro (iniciando com vários zeros). Assim, muitos *hashes* são gerados por parte dos mineiros até que seja encontrado um bem-sucedido.
n) O mineiro que encontra o *hash* correto é recompensado com *bitcoins*.
o) Por fim, a transação é concluída com sucesso e adicionada ao livro-razão. Seu saldo é atualizado na carteira *bitcoin*.

Com esse exemplo, é possível compreender todo o processo da *blockchain* e identificar onde a criptografia e as funções criptográficas se encaixam nessa questão, sendo elas indispensáveis para garantir a segurança dessa tecnologia. Cada vez mais as *blockchains* estão ganhando espaço no mercado, não apenas em moedas criptográficas, mas também em diversas outras áreas, o que se deve à segurança que esse banco de dados distribuído garante.

Referências

AL-HOUSNI, N. *An exploratory study in blockchain technology*. 2019. 88 f. Dissertação (Mestrado) — School of Computer Science, University of Manchester, Manchester, 2019.

AUMASSON, J. P. *Serious cryptography*: a practical introduction to modern encryption. San Francisco: No Starch Press, 2018.

BASHIR, I. *Mastering blockchain*: deeper insights into decentralization, cryptography, bitcoin, and popular blockchain frameworks. Birmingham: Packt Publishing, 2017.

DRESCHER, D. *Blockchain basics*: a non-technical introduction in 25 steps. Frankfurt: Apress, 2017.

GAYOSO MARTÍNEZ, V.; HERNÁNDEZ-ÁLVAREZ, L.; HERNÁNDEZ ENCINAS, L. Analysis of the cryptographic tools for blockchain and bitcoin. *Mathematics*, v. 8, n. 131, 2020.

GUPTA, M. *Blockchan for dummies*: IBM limited edition. Hoboken: John Wiley & Sons, 2017.

MOHAMED, K. S. *New frontiers in cryptography*: quantum, blockchain, lightweight, chaotic and DNA. Cham: Springer, 2020.

MOUGAYAR, W. *The business blockchain*: promise, practice, and application of the next internet technology. New Jersey: John Wiley & Sons, 2016.

RAIKWAR, M.; GLIGOROSKI, D.; KRALEVSKA, K. Sok of used cryptography in blockchain. *IEEE Access*, v. 7, p. 148550-148575, 2019.

VALLIM, A. P. A. *Forense computacional e criptografia*. São Paulo: Senac, 2019.

Métodos criptográficos

Víctor de Andrade Machado

OBJETIVOS DE APRENDIZAGEM

- Diferenciar os mecanismos PGP, PEM/RIPEM, SSH e SET.
- Explicar funcionamento dos certificados de segurança SSL/TLS.
- Descrever o papel do protocolo de autenticação Kerberos.

Introdução

A tecnologia da informação é uma ferramenta indispensável em várias áreas e, consequentemente, a segurança da informação se torna importante em todo o tipo de sistema. Visando a regular o tratamento de dados e proteger os direitos de liberdade e privacidade dos cidadãos, foi instituída a Lei nº 13.709, de 14 de agosto de 2018, a chamada Lei Geral de Proteção aos Dados (LGPD).

Uma das metodologias de proteção eficientes no armazenamento e na transmissão de dados é a criptografia. Basicamente, ela codifica os dados ou a mensagem transformando-os em uma nova sequência, que será decodificada apenas em seu destino ou em outros sistemas programados para a sua utilização. Alguns métodos focam na autenticação remota segura, como o SSH (*Secure Shell*); outros, na criptografia de dados para transmissão por *e-mail*, como o PGP (*Pretty Good Privacy*). Em ambos os casos é feita uma validação para garantir que o solicitante (cliente/emissor) é realmente quem afirma ser, além do destino, seja receptor-cliente ou um servidor para acesso remoto, *e-mail* ou *web*.

Neste capítulo, você vai conhecer alguns métodos de criptografia, seu funcionamento, algoritmo e principais aplicações. Você vai estudar como comparar

e decidir em que momento aplicar um ou outro método. Vai conhecer mecanismos como PGP e PEM, com base na privacidade e na autenticidade, de forma a implementar algoritmos e estruturas de criptografias seguras para manter a integridade das mensagens (de *e-mail*, por exemplo) transmitidas de ponta a ponta. Além disso, você vai estudar o protocolo *Kerberos*, cuja função principal é assegurar a autenticidade de quem acessa um serviço de rede e a integridade das informações trafegadas — este último em conjunto com outros protocolos, como SSL.

Mecanismos de criptografia

Cifras, códigos e outros métodos de criptografia têm sido usados ao longo da história pela maioria das civilizações de uma forma ou de outra para impedir que pessoas não autorizadas entendam as mensagens. Eles aumentaram consideravelmente em sofisticação ao longo da história e são comumente usados hoje. Enfatizando os princípios básicos da segurança informação, a criptografia é considerada uma das linhas de defesa para possíveis ataques e tentativas de roubo de informações, como o *ransomware*.

Saiba mais

O *ransomware* é um *malware* que impede ou limita o acesso dos usuários ao seu sistema bloqueando a tela do sistema ou os arquivos dos usuários até que o resgate seja pago. Famílias de *ransomware* mais modernas, coletivamente categorizadas como *criptorransomware*, criptografam certos tipos de arquivos em sistemas infectados e forçam os usuários a pagar o resgate para obter uma chave de descriptografia (CERT.BR, 2018).

Confira a seguir os quatro principais mecanismos de criptografia (TANENBAUM; WETHERALL, 2011).

- Autenticação: verificar a identidade de um usuário em um computador ou sistema.
- Confidencialidade: fazer a manutenção dos dados como um conteúdo secreto/confidencial.
- Integridade: garantir que os dados não são alterados do momento em que deixam a fonte até o momento em que chegam ao destinatário.
- Confiabilidade: permanência do funcionamento de uma rede/serviço ainda que alguma falha possa ocorrer.

A seguir, serão abordados alguns métodos criptográficos com foco na privacidade, no acesso seguro e na criptografia, bem como na integridade das mensagens transmitidas e recebidas pela rede.

PGP (*Pretty Good Privacy*)

O PGP (privacidade muito boa, em português) pretende garantir a privacidade e a autenticidade dos dados enviados ou recebidos pela rede (intranet e internet). É um sistema de criptografia usado para enviar *e-mails* criptografados e criptografar arquivos confidenciais. Desde sua invenção em 1991, o PGP se tornou o padrão para segurança de *e-mail* (FOROUZAN; MOSHARRAF, 2013).

A popularidade do PGP é baseada em dois fatores. A primeira é que o sistema estava originalmente disponível como *freeware* e, portanto, espalhou-se rapidamente entre os usuários que desejavam um nível extra de segurança para suas mensagens de *e-mail*. A segunda é que, uma vez que o PGP usa criptografia simétrica e criptografia de chave pública, ele permite que usuários que nunca se encontraram enviem mensagens criptografadas uns para os outros sem trocar chaves de criptografia privadas (FOROUZAN; MOSHARRAF, 2013).

O PGP pode ser usado para assinar ou criptografar mensagens de *e-mail* com um simples clique do mouse. Dependendo da versão do PGP, o *software* usa SHA (*Secure Hash Algorithm*) ou MD5 (*Message-Digest algorithm 5*) para calcular o *hash* da mensagem; CAST (Carlisle Adams and Stafford Tavares), Triple-DES (*Data Encryption Standard*) ou IDEA (*International Data Encryption Algorithm*) para criptografia; e RSA (Rivest-Shamir-Adleman) ou DSS/*Diffie-Hellman* (*Digital Signature Standard*) para troca de chaves e assinaturas digitais (TANENBAUM; WETHERALL, 2011). Quando o PGP é instalado pela primeira vez, o usuário deve criar um par de chaves. Uma chave (pública) pode ser anunciada e amplamente divulgada. A chave privada é protegida pelo uso de uma frase secreta. A frase-senha deve ser inserida toda vez que o usuário acessar sua chave privada (FOROUZAN; MOSHARRAF, 2013).

O PGP compartilha alguns recursos com outros sistemas de criptografia, como o Kerberos (usado para autenticar usuários de rede) e SSL (*Secure Sockets Layer* — (usado para proteger *sites*). Em um nível básico, a criptografia PGP usa uma combinação de duas formas de criptografia: de chave simétrica e de chave pública (COMER, 2016).

Vamos descrever o funcionamento do PGP. Imaginemos que um usuário *A* deseja enviar uma mensagem de texto assinada (vamos chamar a mensagem de *M*) para o usuário *B*. O usuário *A* realiza a requisição do programa PGP em seu computador, que submete a mensagem *M* a um processo *hash* utilizando MD5, por exemplo. Na sequência, o resultado é criptografado com a chave

privada em *A*. Ao receber a mensagem, *B* decodifica-a com a chave pública de *A*, verificando a corretude do *hash*.

A chave pública está ligada à identidade de uma pessoa específica, e qualquer pessoa pode usá-la para enviar uma mensagem. O remetente envia sua chave de sessão PGP criptografada ao destinatário, e ele é capaz de descriptografá-la usando sua chave privada. Com essa chave de sessão, o destinatário pode descriptografar a mensagem real.

Pode parecer um pouco estranho, afinal, por que criptografaríamos a própria chave de criptografia? A criptografia de chave pública é muito mais lenta do que a criptografia simétrica (em que o remetente e o destinatário têm a mesma chave). Usar a criptografia simétrica requer, no entanto, que um remetente compartilhe a chave de criptografia com o destinatário em texto simples, e isso não seria seguro. Portanto, ao criptografar a chave simétrica usando o sistema de chave pública (assimétrica), o PGP combina a eficiência da criptografia simétrica com a segurança da criptografia de chave pública (COMER, 2016). O esquema de codificação com chaves públicas e privadas é mostrado na Figura 1.

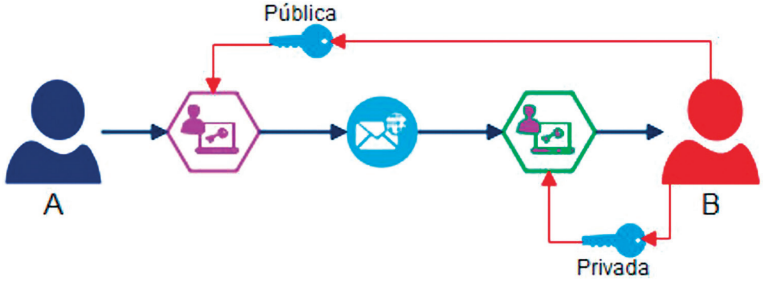

Figura 1. Funcionamento básico da troca de chaves.

A Figura 1 pode ser descrita conforme os tópicos a seguir.

1. Usuário *A* quer enviar mensagem para o *B*.
2. Usuário *B* gera chaves públicas e privadas.
3. Usuário *B* mantém sua chave privada e envia de volta sua chave pública.
4. Usuário *A* criptografa sua mensagem usando a chave pública.
5. Usuário *A* envia a mensagem privada criptografada.
6. Usuário *B* decodifica a mensagem usando a chave privada.

O formato clássico da mensagem PGP pode ser visto na Figura 2. A parte relacionada à chave tem os campos IDEA (chave em si), com o K_M, uma vez que

um usuário pode ter mais de uma chave pública. A parte da assinatura tem um cabeçalho, um campo para registro de tempo, o identificador da chave pública do transmissor, tipo de informação para identificar algoritmos utilizados e o *hash* criptografado (MD5). Já na parte de mensagens, a composição se dá por cabeçalho, nome de arquivo, registro de hora e mensagem em si.

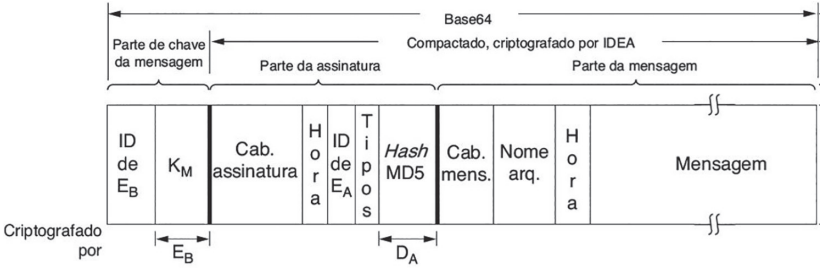

Figura 2. Formato clássico do PGP.
Fonte: Adaptada de Tanenbaum e Wetherall (2011).

PEM/RIPEM (*Privacy Enhanced Mail*/Riordan's *Internet Privacy-Enhanced Mail*)

O PEM é um padrão que define a criptografia de mensagens e alguns procedimentos para autenticação com o intuito de acrescentar privacidade na transferência de mensagens via internet, mais especificadamente serviços de *e-mail*, trabalhando em conjunto com o SMTP (LINN, 1993).

Existem pelo menos duas implementações diferentes de PEM disponíveis. Uma é a *Internet Privacy Enhanced Mail* (RIPEM), escrita por Mark Riordan. Atualmente, essa não é uma implementação completa do PEM, mas ainda é útil. A maior parte do código, exceto para as rotinas RSA que ele emprega, é de domínio público. As rotinas RSA estão na forma da biblioteca RSAREF licenciada pela RSA Data Security, Inc. (RSADSI). A outra implementação do PEM foi originalmente chamada de TIS/PEM (Trusted Information Systems, Inc., TIS). No entanto, ela foi sucedida pelo TIS/MOSS, um programa que implementa o PEM com extensões MIME adicionadas a ele.

Na RFC 1422, é definido o esquema de autenticação para PEM. Ele usa uma estrutura de autenticação compatível com X.509, que contém itens como o algoritmo de assinatura digital usado para assinar o certificado, o assunto, o nome do emissor do certificado, um período de validade, indicando as datas de início e término em que o certificado deve ser considerado válido, e a chave pública junto com o algoritmo que o acompanha. Essa estrutura de autenticação hierárquica

tem quatro entidades. A primeira é uma autoridade central, chamada **autoridade de registro de política da internet (IPRA)**, que atua como raiz da hierarquia e forma a base de toda a validação de certificado na hierarquia. É responsável por certificar e revisar as políticas das entidades no nível imediatamente inferior. As outras são as **autoridades de certificação (CAs)**, responsáveis por certificar tanto CAs subordinadas quanto usuários individuais. Os usuários individuais estão no nível mais baixo da hierarquia (FOROUZAN; MOSHARRAF, 2013). Essa hierarquia torna mais difícil falsificar um certificado, porque provavelmente poucas pessoas confiarão ou usarão certificados que tenham trilhas de certificação não rastreáveis. Para gerar um certificado falso, seria necessário subverter pelo menos uma CA e, possivelmente, a certificação do PCA e do próprio IPRA.

O envio de uma mensagem PEM é feito em quatro etapas, transparentes ao usuário.

1. Padronização: traduz a mensagem utilizada por um texto ou programa de correio eletrônico para uma representação comum entre todas as máquinas e plataformas da rede. Isso é o que chamamos de interoperabilidade. O receptor pode utilizar uma plataforma completamente diferente da do emissor, e o PEM busca garantir a leitura das mensagens, permitindo transformações de padrões comuns utilizados na internet, como no SMTP (RFC 882).
2. Autenticação e integridade: é realizado o cálculo de *hash* da mensagem, o qual informa ao receptor que a mensagem não foi modificada durante a transmissão e o tráfego na rede. O *hash* deve ser protegido, o que ocorre com as assinaturas digitais, podendo ser verificadas por qualquer receptor (até mesmo de origem desconhecida), mas não podendo ser falsificada.
3. Cifração: realizada se o tipo de mensagem do PEM for ENCRYPTED. Nesse momento, é importante o conceito de chave pública visto anteriormente. O RSA é o algoritmo usado nas especificações PEM para esse caso.
4. Codificação: não podemos confundir a cifração com a codificação. A cifração está relacionada à chave cifrada, que é apenas decifrada no lado remetente com a chave correspondente. A codificação é o mecanismo utilizado para a transmissão da mensagem, semelhante ao descrito no método do PGP.

SSH (*Secure Shell*)

SSH é um protocolo de administração remota que permite aos usuários controlarem e modificarem seus servidores remotos pela internet (TANEN-

BAUM; WETHERALL, 2011). O serviço foi criado como uma substituição segura para o Telnet não criptografado e usa técnicas criptográficas para garantir que toda a comunicação de/para o servidor remoto aconteça de maneira criptografada. Ele fornece um mecanismo para autenticar um usuário remoto, transferindo entradas do cliente para o *host* e retransmitindo a saída de volta para o cliente.

Se você estiver usando Linux ou Mac, usar SSH é muito simples. Se você usa o Windows, precisará usar um cliente SSH para abrir as conexões SSH. O cliente SSH mais popular é o PuTTY (2021), cuja interface é mostrada na Figura 3. O protocolo funciona no modelo cliente-servidor, o que significa que a conexão é estabelecida pelo cliente SSH que se conecta ao servidor SSH. O cliente SSH conduz o processo de configuração da conexão e usa criptografia de chave pública para verificar a identidade do servidor SSH.

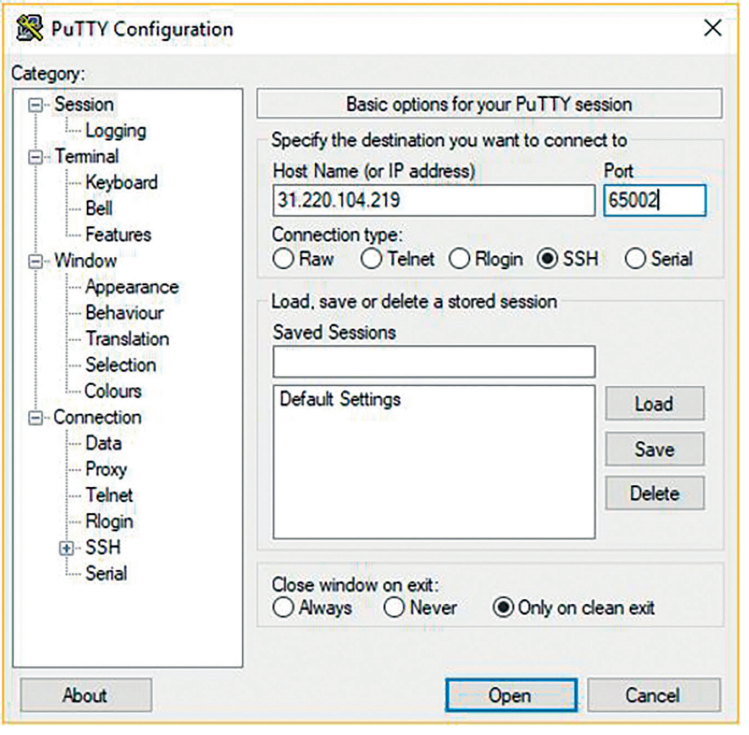

Figura 3. Interface do PuTTY.
Fonte: Rafael H. (2020, documento *on-line*).

Após a fase de configuração, o protocolo SSH usa criptografia simétrica forte e algoritmos de *hash* para garantir a privacidade e integridade dos dados trocados entre o cliente e o servidor. A Figura 4 apresenta um fluxo de configuração simplificado de uma conexão *shell* segura. O processo de solicitação para o estabelecimento de conexão é chamado de *handshaking*.

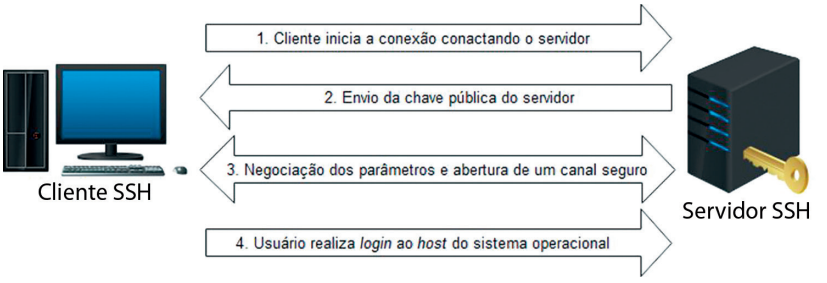

Figura 4. Fluxo básico de uma comunicação SSH.

O comando SSH instrui o sistema com o qual se deseja abrir uma conexão *secure shell* criptografada (por exemplo, acessar o usuário *root*, que é basicamente sinônimo de administrador do sistema, com direitos completos para modificar qualquer coisa). O campo *{host}* refere-se ao computador que se quer acessar. Pode ser um endereço IP (por exemplo, 244.235.23.19) ou um nome de domínio (por exemplo, www.abcdominio.com).

Assim que uma conexão for estabelecida entre o cliente SSH e o servidor, os dados transmitidos são criptografados de acordo com os parâmetros negociados na configuração. Durante a negociação, o cliente e o servidor concordam com o algoritmo de criptografia simétrica a ser usado e geram a chave de criptografia que será usada. O tráfego entre as partes que se comunicam é protegido com algoritmos de criptografia forte padrão da indústria (como AES — *Advanced Encryption Standard*), e o protocolo SSH também inclui um mecanismo que garante a integridade dos dados transmitidos usando algoritmos de *hash* padrão, como SHA-2 (TANENBAUM; WETHERALL, 2011). A etapa final antes que o usuário tenha acesso ao servidor é a autenticação de suas credenciais. Para isso, a maioria dos usuários SSH usa uma senha. O usuário é solicitado, então, a inserir o nome de usuário e a senha. Essas credenciais passam com segurança pelo túnel criptografado simetricamente, portanto não há chance de serem capturadas por terceiros (COMER, 2016).

Embora as senhas sejam criptografadas, ainda não é recomendado o uso de senhas para conexões seguras. Isso ocorre porque muitos *bots* podem

simplesmente usar força bruta fácil ou senhas-padrão e obter acesso à conta. Em vez disso, a alternativa recomendada são pares de chaves SSH. Trata-se de um conjunto de chaves assimétricas utilizadas para autenticar o usuário sem a necessidade de inserir uma senha.

Assim, uma série de protocolos e certificados vêm somar às metodologias de acesso seguro e criptografias já existentes. A seguir, vamos estudar um padrão para estabelecer uma conexão à internet de forma segura, como para acessar dados no internet banking: o SET.

SET (*Secure Electronic Transation*)

O SET (Transação Eletrônica Segura) é um sistema que garante segurança e integridade das transações eletrônicas realizadas com cartão de crédito por meio de diferentes técnicas de criptografia e *hash*. O SET não é usado para fazer pagamentos; é um protocolo de segurança aplicado a esses pagamentos. Foi apoiado por grandes organizações, como Visa, Mastercard, Microsoft (que forneceu sua STT, *Secure Transaction Technology*) e *NetScape* (que forneceu a tecnologia SSL) (TECHTARGET CONTRIBUTOR, c2021).

O protocolo SET restringe a revelação das informações do cartão de crédito aos comerciantes, protegendo-as de *hackers* e ladrões. Inclui autoridades de certificação para usar certificados digitais padrões, como o X.509 (COMER, 2016). Além disso, mantém a credibilidade dos comerciantes em suas transações criptografando dados (como número de cartão), ajuda na proteção com a assinatura digital e é usado em todas as fases da transação, garantindo confiabilidade em todo processo (ALISHIRVANI; MORTAZAVI, 2016). A Figura 5 mostra o funcionamento do protocolo SET.

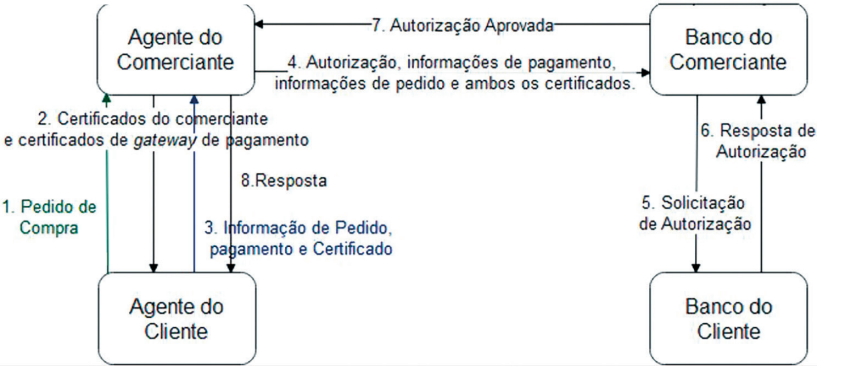

Figura 5. Funcionamento padrão do SET.
Fonte: Adaptada de Tiwari *et al*. (2007).

Os passos enumerados na Figura 5 indicam processos, tarefas e transações de um pedido cujo pagamento será realizado via cartão de crédito. Observe a sequência a seguir.

1. O pedido de compra é realizado pelo cliente (via navegador, por exemplo).
2. São verificados os certificados do comerciante, *gateway*, dados de pagamento do comerciante.
3. As informações de pedido, pagamento e certificado são passadas do cliente ao comerciante.
4. Uma requisição para autorização do pagamento com suas informações e as informações de pedido e certificados são enviadas.
5. É realizada a solicitação de autorização de compra ao banco/bandeira do cartão do cliente.
6. A autorização é concedida (ou negada).
7. Para o pedido prosseguir, a autorização é aprovada.
8. Finalmente, a resposta é dada ao cliente, dizendo que a transação foi autorizada.

Com alguns protocolos para transação, com base na integridade e na confidencialidade dos dados transitados, existem certificados que permitem a conexão com internet segura para proteção dos dados a serem enviados entre dois sistemas. A seguir, vamos estudar o certificado SSL/TLS, encarregado de manter a conexão segura para atender aos princípios da segurança da informação.

Certificado SSL/TLS

SSL significa *Secure Sockets Layer* e, em suma, é a tecnologia padrão para manter uma conexão de internet segura e proteger todos os dados sensíveis que estão sendo enviados entre dois sistemas, evitando que criminosos leiam e modifiquem qualquer informação transferida, incluindo possíveis detalhes pessoais (GOODRICH; TAMASSIA, 2012). Os dois sistemas podem ser um servidor e um cliente (por exemplo, um *site* de compras e navegador) ou servidor para servidor (por exemplo, um aplicativo com informações de identificação pessoal ou com informações de folha de pagamento).

Ele faz isso garantindo que quaisquer dados transferidos entre usuários e *sites*, ou entre dois sistemas, permaneçam impossíveis de serem lidos. Usa algoritmos de criptografia para embaralhar os dados em trânsito, evitando que

os *hackers* os leiam quando são enviados pela conexão. Essas informações podem ser confidenciais ou pessoais, incluindo números de cartão de crédito e outras informações financeiras, nomes e endereços.

A conexão do SSL é feita entre dois soquetes (origem e destino), sendo quatro os passos básicos para a realização dessa conexão (TANENBAUM; WETHERALL, 2011).

- Negociação de parâmetros entre cliente e servidor.
- Autenticação mútua de cliente e servidor.
- Comunicação secreta.
- Proteção da integridade dos dados.

De forma Geral, o SSL consiste em dois protocolos para estabelecer e usar uma conexão segura. A Figura 6 mostra uma simplificação do funcionamento do SSL.

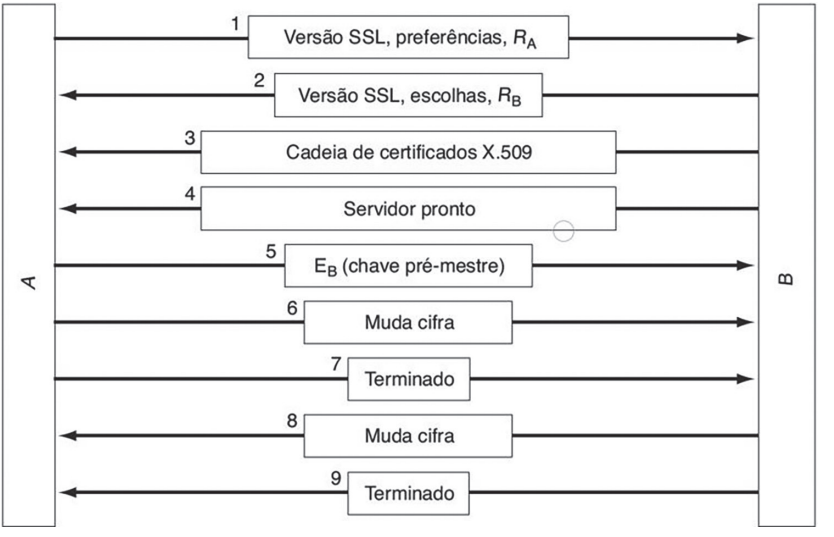

Figura 6. Funcionamento simplificado do SSL.
Fonte: Adaptada de Tanenbaum e Wetherall (2011).

- A primeira mensagem se dá quando *A* solicita para *B* o estabelecimento de uma conexão. Tal solicitação tem a versão e as preferências de criptografia do SSL no emissor, e o R_A, o chamado *nonce*.

Saiba mais

De acordo com Kurose, Ross e Zucchi (2013), o *nonce* é o nome dado a um número relacionado aos protocolos de segurança, como números aleatórios e chaves usados apenas uma vez. É uma simplificação de *number used once* (número usado uma vez).

- A segunda mensagem relaciona-se com a escolha de *B* entre os diversos algoritmos de segurança, enviando seu próprio *nonce* R_B.
- Na terceira mensagem, *B* envia um certificado com sua chave pública.
- A quarta mensagem, após verificação da chave pública de *B* por *A*, é indicado por *B* que o servidor está pronto, e agora *A* é quem vai responder.
- A resposta de *A*, na mensagem 5, indica o envio de uma chave aleatória de 384 bits codificada e enviada com a chave pública de *B*.
- Nesse momento, a chave da sessão entre as partes é calculada. *B* é informado sobre uma nova cifra a ser gerada, além de terminar o estabelecimento de conexão e troca de chaves.
- Ao final, *B* informa o recebimento correto das mensagens de *A*.

TLS (*Transport Layer Security*) é apenas uma versão atualizada e mais segura do SSL. Ainda nos referimos aos nossos certificados de segurança como SSL porque é um termo mais comum, mas quando compramos SSL de entidades certificadoras, na verdade estamos comprando os certificados TLS mais atualizados com a opção de criptografias ECC (Criptografia de Curva Elíptica), RSA ou DSA (COMER, 2016).

HTTPS (*Hyper Text Transfer Protocol Secure*) aparece na URL quando um *site* é protegido por um certificado SSL. As informações do certificado, incluindo a autoridade emissora e a razão social do proprietário do *site*, podem ser visualizadas clicando no símbolo de cadeado na barra do navegador (TANENBAUM; WETHERALL, 2011).

Em relação à segurança e autenticação, devemos nos certificar de que protocolos confiáveis para esse fim serão implementados e validados em um acesso a *sites* em que haja troca de dados confidenciais. A seguir, vamos estudar o protocolo *Kerberos*, um dos responsáveis para a garantia de uma comunicação segura, principalmente no envio de senhas e dados financeiros pela internet.

Protocolo Kerberos

A ideia do Kerberos é autenticar usuários, evitando o envio de senhas pela internet. Esse protocolo pode ser adotado mesmo em redes inseguras, pois

é baseado em uma criptografia forte e desenvolvido em um modelo cliente-servidor. Quando habilitar um serviço para usar a autenticação Kerberos, estamos tornando-o **ciente do Kerberos**. Isso é possível para a maioria dos *softwares*.

De acordo com o *site* disponível do protocolo (RICCIARDI, 2007), as estratégias do Kerberos são inúteis se alguém que obtém acesso privilegiado a um servidor copiar o arquivo que contém a chave secreta. Na verdade, o invasor colocará essa chave em outra máquina e terá apenas que obter um DNS ou endereço IP falsificado simples para que esse servidor apareça aos clientes como o servidor autêntico. Portanto, além do gerenciamento de mensagens, o servidor também deve estar sempre seguro para evitar esses tipos de ataques, invalidando as medidas de autenticação.

Ao autenticar, o Kerberos usa criptografia simétrica e outra parte confiável, que é chamada de **centro de distribuição de chaves (KDC)**. No momento da autenticação, o Kerberos armazena um tíquete específico para aquela sessão na máquina do usuário e qualquer serviço ciente do Kerberos vai procurar por esse tíquete em vez de solicitar que o usuário se autentique por meio de uma senha.

O Kerberos 4 implementa um único tipo de criptografia, a DES com 56 bits (KERBEROS, 2007). Por esse e outros motivos de segurança e vulnerabilidades, a versão 4 tornou-se obsoleta. A versão 5, entretanto, não predetermina o número ou tipo de métodos criptográficos suportados. Cada implementação oferece um suporte para melhor negociar a criptografia que lhe convém. No entanto, essa flexibilidade e expansibilidade do protocolo acentuou os problemas de interoperabilidade entre as várias implementações do Kerberos 5. Para que clientes e servidores de aplicativos e autenticação usem diferentes implementações, deve-se ter pelo menos um tipo de criptografia em comum entre eles. O problema foi posteriormente resolvido com a versão 1.3 do MIT Kerberos 5. Essa versão introduziu o suporte RC4-HMAC, que também está presente no Windows e é mais seguro do que o DES. Entre as criptografias suportadas, vale a pena mencionar o DES triplo (3DES) e os mais novos AES128 e AES256. (RICCIARDI, 2007).

O Kerberos introduz o conceito de TGT (*Ticket Granting Ticket*), uma espécie de:

> [...] credencial concedida ao usuário pelo AS, parte do KDC, do Kerberos. Esse usuário precisa do TGT para fazer requisições de serviços específicos. Quando o programa que ele está usando faz uma requisição de um *ticket* para um servidor Kerberos, este irá solicitar o *login* e a senha do usuário. O servidor responde à requisição do ticket enviando o TGT. Dessa forma, somente esse usuário é capaz

de decriptar o TGT. O TGT expira algumas horas após sua concessão, para evitar invasões e falsificações, e é necessário para que o usuário tenha acesso ao *Ticket Granting Server*, TGS (KERBEROS, 2007, documento *on-line*).

Observe na Figura 7 uma representação básica do funcionamento do Kerberos.

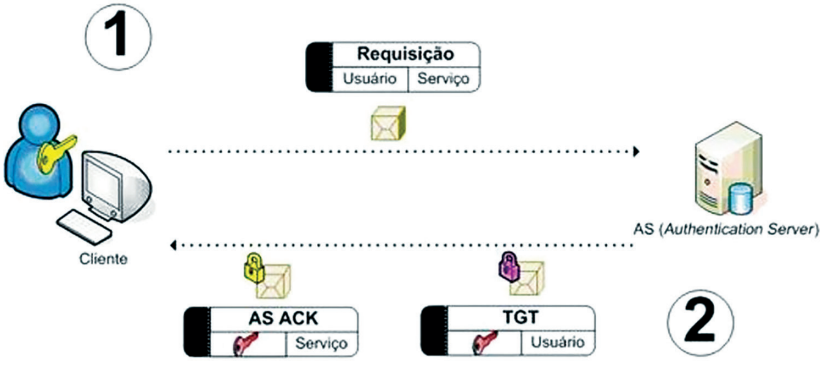

Figura 7. Funcionamento básico do Kerberos.
Fonte: Adaptada de Kerberos (2007).

A seguir, está a descrição das etapas.

- O PC Cliente faz *logon* no domínio. Uma solicitação concessão de tíquete (TGT) é enviada a um Kerberos KDC (1).
- O Kerberos KDC retorna um TGT e uma chave de sessão para o PC Cliente (2).
- Uma solicitação de tíquete para o servidor de aplicativos é enviada ao Kerberos KDC. Essa solicitação consiste no PC Cliente, TGT e um autenticador (1).
- O Kerberos KDC retorna um tíquete e uma chave de sessão para o PC Cliente (2).
- O tíquete é enviado ao servidor de aplicativos (1). Ao receber o tíquete e o autenticador, o servidor pode autenticar o PC Cliente.
- O servidor responde ao PC Cliente com outro autenticador (2). Ao receber esse autenticador, o PC Cliente pode autenticar o servidor.

Como estudamos neste capítulo, diferentes métodos são usados para criptografia e acesso seguro a servidor remoto e outros tipos de aplicações, como *web* e *e-mail*. Geralmente, os procedimentos de autenticação e transmissão

de dados ocorrem pela combinação de padrões e protocolos, como o SSH, que combina autenticação com criptografia. Outros métodos implementam um centro de distribuição de chaves (KDC), como o Kerberos, mas que precisa se manter disponível (servidor) para que usuários não tenham problema de acesso.

Referências

ALISHIRVANI, N.; MORTAZAVI, B. Guaranteeing of trust and security in e-commerce by means of improved SET protocol. *Bulletin de la Société Royale des Sciences de Liège*, v. 85, p. 1136-1147, 2016. Disponível em: https://popups.uliege.be/0037-9565/index.php?id=5933&file=1. Acesso em: 28 jun. 2021.

CERT.BR. *Ransomware*. [*S. l.*]: CERT.br, 2018. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 28 jun. 2021.

COMER, D. E. *Redes de computadores e internet*. 6. ed. Porto Alegre: Bookman, 2016.

FOROUZAN, B. A.; MOSHARRAF, F. *Redes de computadores*: uma abordagem top-down. Porto Alegre: AMGH, 2013.

GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2012.

KERBEROS. *O Ticket Granting Ticket (TGT)*. Rio de Janeiro: UFRJ, 2007. Disponível em: https://www.gta.ufrj.br/grad/07_1/Kerberos/OTicketGrantingTicket(TGT).html. Acesso em: 28 jun. 2021.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. *Redes de computadores e a internet*: uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

LINN, J. *Privacy enhancement for internet electronic mail*: part I: message encryption and authentication procedures. [*S. l.*]: IETF Datatracker, 1993. Disponível em: https://datatracker.ietf.org/doc/html/rfc1421. Acesso em: 28 jun. 2021.

RAFAEL H. *Como usar o PuTTy SSH e se conectar com sua hospedagem*. Florianópolis: Hostinger, 2020. Disponível em: https://www.hostinger.com.br/tutoriais/como-se-conectar-servidor-vps-usando-terminal-ssh. Acesso em: 29 jun. 2021.

RICCIARDI, F. *Kerberos protocol tutorial*. Cambridge: MIT Kerberos Consortium, 2007. Disponível em: https://www.Kerberos.org/software/tutorial.html. Acesso em: 28 jun. 2021.

TANENBAUM, A. S.; WETHERALL, D. *Redes de computadores*. 5. ed. São Paulo: Pearson Education do Brasil, 2011.

TECHTARGET CONTRIBUTOR. *Secure Electronic Transaction (SET)*. Newton: TechTarget, c2021. Disponível em: https://searchsecurity.techtarget.com/definition/Secure-Electronic-Transaction-SET. Acesso em: 28 jun. 2021.

TIWARI, A. *et al*. A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. *In*: IADIS INTERNATIONAL CONFERENCE APPLIED COMPUTING, 2007, Salamanca. *Proceedings* [...]. Salamanca: IADIS, 2007.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

editora
papervest

Publicação da Papervest Editora
Av. Marechal Floriano, 947 - CEP: 88503-190
Fone: (49) 3225-4114 - Lages / SC
www.unifacvest.edu.br