



centro universitário
unifacvest

Limites e perspectivas legais da informação nas redes sociais

A legislação sobre a segurança da informação no mundo

Objetivos de aprendizagem

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

- Explicar os aspectos comuns quanto à privacidade de dados nos mais diversos países.
- Reconhecer a importância do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (GDPR–EU).
- Descrever as leis de proteção de dados em outros países americanos.

Introdução

O marco zero da relação entre instituições e indivíduo é a transparência, que possibilita maior liberdade na sociedade. Por vezes, o meio de garantir a transparência é a legislação. Quando está em jogo a segurança da informação, as leis de proteção de dados entram em cena. Por meio delas, é possível verificar e auditar se os dados transacionados estão sendo utilizados adequadamente, e não para outros fins que não aqueles previamente acordados.

Diversos países têm criado leis relativas à privacidade de dados. O RGPD, que em inglês tem a sigla GDPR (*General Data Protection Regulation*), por exemplo, é compartilhado pelos países da União Europeia (UE). Por meio do RGPD, esses países buscam padronizar e normatizar as suas legislações, bem como atingir conjuntamente os resultados esperados.

Neste capítulo, você vai estudar a legislação relativa à segurança da informação utilizada no mundo. Além de conhecer melhor o RGPD, você vai se familiarizar com a legislação de outros continentes. Como você vai notar, as prerrogativas legais se tornam cada vez mais universais. Afinal, no mundo todo, um simples dado pode proporcionar ganhos estratégicos para as organizações, porém sempre é necessário agir dentro da lei.

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.

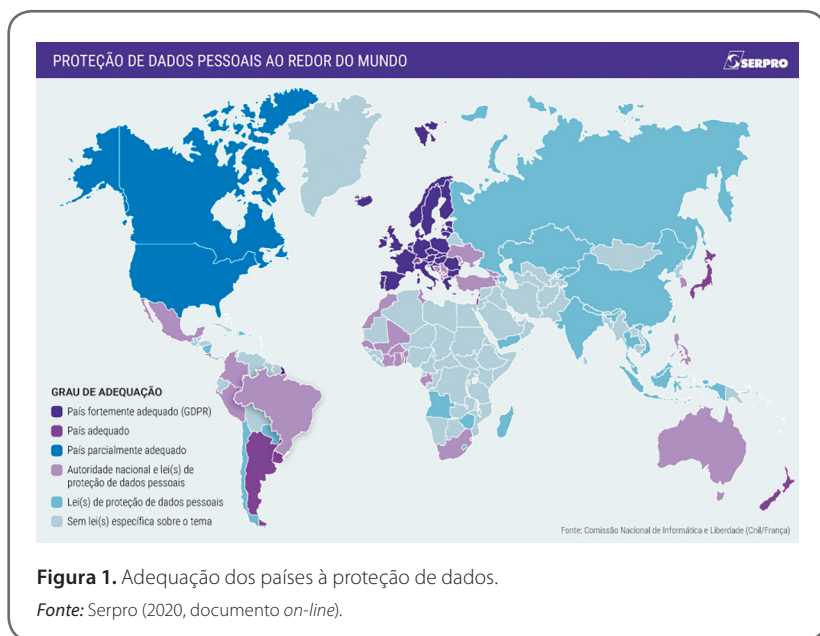
Algumas considerações

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).



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* — Pípeda). Válida para todas as províncias do Canadá, a Pípeda 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 Pípeda 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 integridade das informações referidas em tais *links*.

Ética no mundo digital

Objetivos de aprendizagem

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

- Discutir sobre a ética na sociedade em rede.
- Analisar a questão ética nas redes sociais.
- Identificar o desafio ético relacionado ao acesso desigual à informação.

Introdução

Neste capítulo, você vai estudar a sociedade atual, na qual a famosa Era do Conhecimento é tão explanada e debatida como unânime, mas, como veremos, talvez não seja exatamente assim na realidade. Para isso, você irá refletir sobre o mundo digital, a liberdade de interagir virtualmente com os demais cidadãos do planeta e sobre as consequências dos atos, ou a ausência delas, a partir de uma lógica de causalidade. Também irá repensar seu comportamento ético em espaços de comunicação online, vendo aplicativos de conexão a partir dos quais sua opinião, cultura e seus conceitos ou “pré-conceitos” serão testados – assim, poderá rever a atitude a tomar ou a que, como profissional da área social, deverá ter. Além disso, você se aproximará de alguns conhecimentos sobre as desigualdades ainda existentes no acesso à informação e seus desafios no ambiente real.

A ética e o mundo das redes sociais

“Tudo me é lícito (é permitido)”, mas nem tudo convém. “Tudo me é lícito”, mas nem tudo edifica (1 Co 10: 23). Esta frase foi tirada da Bíblia, de modo que podemos ter uma noção do quão antiga é a ideia sobre como tratar as pessoas da comunidade, ou seja, a ética nas civilizações. Porém, mesmo que se fale e debata, você acha que já temos um equilibrado convívio com nossos iguais ou parece que cada vez mais nos distanciamos do que chamamos de civilidade? Qual é a sua opinião sobre o assunto? Se você concorda com a segunda alternativa, está pensando como a maioria dos brasileiros, que

atestam, em pesquisas de opinião, que estão ocorrendo muitos conflitos entre classes sociais diferentes, espaços de relacionamentos virtuais com excessiva polarização de opiniões e constantes atritos por dificuldade em perceber as diferenças que o outro tem – e até mesmo um despreparo para lidar com as subjetividades ou verdades de cada um. Agora, vamos tentar compreender a sociedade atual e o que significa o conceito de redes, redes sociais e redes sociais digitais, mídias sociais e tudo o que envolve este universo virtual e o que ele tem a ver com ética.

O homem é uma ilha?

Desde os primórdios dos tempos, o homem é um ser de relações. Ele se constrói a partir do outro: inicialmente, seu quadro é familiar e, à medida que cresce, seu círculo vai aumentando. Percebe-se que o outro estabelece nossa identidade na relação de troca; por exemplo, nos reconhecemos mais velhos a partir do olhar que outra pessoa dá e, assim, identificamos a passagem do tempo quando somos chamados pelos apelidos de “Tio/Tia”, “Senhor/Senhora”, “Vô/Vô”, e assim por diante. Embora isso já seja senso comum, a consciência dessa atitude externa vai transformando nosso comportamento ao longo da vida e esses gestos vão formando as interações humanas.

O formato dessas relações tem sofrido transformações em um processo dinâmico e evolutivo. Nota-se que não estávamos preparados para experimentar a velocidade das mudanças: parece que entramos num gigante carrossel e, sem querer, ele disparou, fazendo com que tenhamos que olhar o mundo ao redor muito espaçadamente, de maneira distante e rápida. Há cinquenta anos, havia praticamente apenas o relacionamento presencial, as visitas eram feitas indo na casa da pessoa amiga, os relacionamentos afetivos aconteciam em atividade social ou no ambiente doméstico – tudo era pensado para relacionamentos presenciais (*face to face*). Foi inquestionável o papel da família, na qual preponderavam os valores e princípios passados de pai para filho, o patriarcado não era rebatido e todo o aprendizado vinha de ensinamentos da escola e religião de origem.

E como é hoje? Muito diferente: a juventude nascida nas décadas de 1990/2000 já teve acesso à internet e nem questiona se o contato virtual ou presencial causa desconforto; para esses jovens, falar via Skype ou pessoalmente tem o mesmo valor de comunicação. Provavelmente, eles questionam a necessidade de atender o telefonema da mãe ou de parentes mais velhos em uma época em que já existem aplicativos de comunicação mais efetivos. Se comportamentos simples como o falar ao telefone ou namorar sofreram tantas

modificações, como é transitar pelas redes sociais digitais para pessoas mais velhas e para as mais jovens? Como é conciliar esses pensamentos, valores e atitudes num mesmo instrumento de comunicação virtual mundial?

Vivíamos, nas décadas anteriores, em uma zona de conforto em que as verdades não eram tão questionadas nas famílias, as hierarquias eram seguidas, em sua maioria, por obrigatoriedade parental, e quase não se debatiam conceitos ou pensamentos entre os de seu sangue. Já não é o que acontece na atualidade. Agora, tudo está quase que completamente mudado, vivemos em um mundo em que crianças de quatro/cinco anos já decidem quais produtos comercializados consumir pelo excessivo acesso às diversas mídias sociais, como TV, propagandas e publicações via internet. É uma realidade à que elas têm acesso mesmo sem critérios de compreensão por idade ou outra condição de exclusão, situação pouco explanada ou criticada nos grupos familiares. Todas essas mudanças ocorridas ao longo dos tempos pela humanidade foram sendo estudadas, debatidas e trazidas à luz do conhecimento por filósofos, pensadores e pessoas críticas do cotidiano.

Os gregos foram pioneiros na teorização sobre os costumes e valores da civilização ocidental e, por isso, toda a definição foi pedagogicamente classificada conforme a cultura grega. Constituiu-se a terminologia ética, que faz parte de uma das três grandes áreas da filosofia



Saiba mais

Filosofia: do grego: *philo*+*sophia*. **Philo** deriva de *philia*, que significa amizade, amor fraterno, respeito entre os iguais. **Sophia** quer dizer sabedoria e dela vem a palavra *sophos*, sábio.

A ética está presente no nosso cotidiano o tempo todo, seja nas decisões familiares, políticas, ou no trabalho, por exemplo – é um valor importante na formação de caráter do ser humano. A ética é o estudo geral do que é bom ou mau, correto ou incorreto, justo ou injusto, adequado ou inadequado (GLOCK; GOLDIM, 2003). É, também, compreendida como um conjunto de valores e princípios que norteiam a reflexão e a tomada de decisão sobre a ação.

Mas como saber o que é bom ou mau nesta sociedade em constante modificação? A que valores, conceitos e princípios estamos sendo expostos todos os dias e como julgá-los procedentes para as nossas vidas? Ferreira (2011) traz

o conceito do sociólogo Zygmunt Bauman (LINS, 2016) de “mundo fluido”, um mundo atual caracterizado pela complexidade, sem divisões ou fronteiras, mundo líquido, destituído de formas, sem a certeza, solidez, verdade absoluta e concretude dos tempos anteriores. Agora, vivemos o

[...] dinamismo da relação entre as partes, sistemas abertos, imprevisibilidade, não linearidade, auto-organização, adaptabilidade, criatividade, instabilidade, emergência, incerteza, conectividade e fluxo [...] (FERREIRA, 2011, p. 208).

Essas marcas da contemporaneidade fazem sobressair a era da informação e do conhecimento, na qual as redes emergem como elementos catalisadores da realidade.

Afinal, o que são redes sociais?

A partir desse conceito da não linearidade em que vivemos, parece que a definição de rede é algo novo, construído para esses tempos atuais, mas não é bem assim. Hipócrates, considerado o pai da medicina, já trazia o conceito de rede ao perceber, em seus estudos humanos, como era o circuito das veias e artérias, no qual todas criavam emaranhados semelhantes a uma rede de pesca. Embora fosse um início de pensamento intracorporal, já trazia o princípio da relação da rede. Após isso, matemáticos utilizaram o mesmo processo para decodificar problemas práticos de arquitetura nas vilas, assim como engenheiros também criaram conceitos a partir das redes, entre outros. Na sociologia, o termo também é trazido e é acrescido da palavra “social” para designar o humano da relação. A partir dessa noção de rede, foram elaborados diversos conceitos de redes sociais, um deles como:

[...] uma estrutura social composta por indivíduos, organizações, associações, empresas ou outras entidades sociais, designadas por atores, que estão conectadas por um ou vários tipos de relações que podem ser de amizade, familiares, comerciais, sexuais etc. (FERREIRA, 2011, p. 213).

Com isso, todos que participariam dessa teia desencadeariam movimentos e fluxos nos quais partilhariam crenças, poder, conhecimentos, informações, etc.

Embora isso se configure como uma malha de relações sociais, ainda não se está falando das redes digitais. Até a concepção da rede mundial de acesso digital, no início da década de 1980 nos Estados Unidos e a partir da década de 1990 no Brasil, as interações aconteciam de forma diferente da atual,

mas eram eficazes, ou seja, o objetivo primordial de estabelecer conexões e firmar relacionamentos já era feito independentemente da era digital. O que se modificou foi a ferramenta de acesso e, com isso, foram abertos novos horizontes, o mundo perdeu fronteiras e se tornou fluido, como dizia Bauman (LINS, 2016). O planeta virou uma grande aldeia e as conexões não pararam de acontecer, desde as relacionais até as mercadológicas, científicas, entre outras. O conceito de globalização foi sendo construído e, hoje, é muito praticado no modo de produção capitalista.

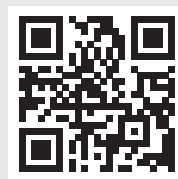
A partir do início desse século, a terminologia de redes sociais foi associada ao conceito das interações feitas pelas ferramentas da Tecnologia da Informação (TI). Os chamados aplicativos de relacionamento (*networking social*) eram instrumentos particulares de alguma rede social ou comunidade mediados por computadores (mídia social) e tinham como objetivo criar novas tramas e teias independentemente da tecnologia. É claro que a melhoria nos processos tecnológicos potencializa e evidencia os relacionamentos, sobretudo nos locais em que há certa dificuldade de contato físico ou relação mais próxima, como espaços pouco habitados da terra ou aqueles de difícil acesso. Embora o termo utilizado seja somente na forma “redes sociais”, sabe-se que estamos falando de redes sociais digitais, nas quais o computador e a internet são ferramentas de conexão entre comunidades e pessoas.



Link

Para entender melhor sobre rede e as transformações sociais, conheça o sociólogo Manuel Castells. Acesse o link ou o código a seguir.

<https://goo.gl/RLaUfU>



A questão ética nas redes sociais

Nosso foco, aqui, será na ética nas redes sociais digitais, pois é essa a que está suscitando mais dilemas e questões para debate. As redes sociais presenciais têm sido muito utilizadas, o que fez com que surgissem alguns desvios; por isso,

a legislação existente está tentando dar conta de normatizar as relações virtuais. Esse novo universo, chamado também de ciberespaço, apresenta um mundo de novidades, em que todos somos parte, influenciadores e influenciados.

Como o tema é bastante relevante, comecemos por uma pergunta: você já pensou sobre o quanto é mais informado do que seus familiares mais velhos? Ao mesmo tempo, pode se questionar: a quantidade de informações obtidas tão facilmente fez de você um ser mais inteligente ou moralmente melhor?

Nem todos param para pensar sobre o tema e talvez você nem questione a dependência e total necessidade com as quais vivemos atualmente em relação às Tecnologias da Informação. Deixar um smartphone em casa significa, hoje, não ter agenda, e-mail, câmera fotográfica, rádio, filmes e séries, além, é claro, do telefone. Toda essa dependência é fruto da modernização das ferramentas e, assim, da individualização das informações e dos conhecimentos, pois não dependemos mais de nossa família, comunidade escolar e demais pessoas para obtermos dados sobre qualquer assunto e em qualquer idioma. Talvez para você seja óbvio, mas essa possibilidade é muito recente: pessoas nascidas nas décadas de 1960 e 1970 não tiveram os mesmos recursos que existem atualmente e a lógica do conhecimento era outra.

Você pode estar se perguntando sobre o que isso tem a ver com a ética, sobre como isso impacta a sociedade. Nem sempre temos resposta para tudo, mas vamos fazer um giro por esse assunto, a partir do seu princípio. Quando falamos em internet, rede social digital, gerações de computadores, ciberespaço (MONTEIRO, 2007) devemos lembrar que, antes disso, ocorreu uma revolução das novas tecnologias: milhares de pessoas perderam seus postos de trabalho quando iniciou a chamada “Terceira Revolução Industrial”, na qual o modo de produção foi sendo automatizado e, com isso, as técnicas de trabalho foram progredindo. Com esse processo em constante evolução, o advento do computador trouxe ainda mais rapidez e, na década de 1990, a internet chegou aos lares brasileiros, provocando verdadeiro tumulto no *modus operandi* dos lares tradicionais de então. Essa onda gigantesca de sucessivas conexões só aumentou e trouxe ainda mais individualidade, autonomia e facilidade aos usuários da rede digital.

O que parecia uma esperança de um mundo feliz, moralizado e próspero com a informação ao toque de dedos não se confirmou, e não é exatamente isso que tem ocorrido em nossa sociedade. Temos visto exemplos de quebra de privacidade, abuso de autoridade, mercantilismo e exposição dos públicos que acessam as redes de comunicação, o que faz com que uma nova dúvida abra espaço: a comunidade usuária tem se perguntado sobre a legitimidade das leis já existentes e se essas conseguem dar conta das demandas do meio virtual.

Talvez você já tenha ouvido falar de alguém que teve seu cartão de crédito clonado, alguma fraude bancária ou então os seus dados privados expostos na rede sem sua aprovação. Tudo isso não era visto há 30 anos, quando as atividades ilegais dependiam da presença da pessoa para acontecer. A partir do momento em que começam a ocorrer ações que fogem à nossa vontade e as mesmas são praticadas em ambiente virtual, surgem novas formas de reação, e isso tem sido bastante debatido na sociedade do conhecimento.

Chauí (2000) define que duas coisas são indispensáveis na vida ética: consciência e responsabilidade. Para ela, ser um sujeito ético depende da capacidade de refletir e reconhecer o outro como um ser igual, em que seus desejos e impulsos não ultrapassam a sua individualidade, controlando e orientando sentimentos, alternativas de vida, escolhas e, assim, admitindo as consequências de suas atitudes, tomando as rédeas de sua conduta.

Essa assertiva parece não fazer eco no ambiente virtual, pois o usuário da internet tem dificuldade de compreender que, embora se trate de um lugar não presencial, deve sofrer as mesmas regras do presencial. Muitas vezes, esse ambiente é tratado como se fosse uma “terra de ninguém”, onde se pode fazer o que der vontade, mesmo que conflite com a privacidade e autonomia do outro. O indiscriminado fornecimento de dados pessoais para as redes de comunicação digital ou para empresas digitais em que o usuário está conectado não tem protegido a privacidade das pessoas, fazendo com que surjam diversas questões de natureza ética, o que foge do conceito de harmonia e equilíbrio na grande rede mundial de computadores conectados (FUGAZZA; SALDANHA, 2017).

Legislação que ampara o usuário conectado na Web

Os inúmeros conflitos éticos que os comportamentos têm gerado na sociedade ocidental provocara debates legislativos e da comunidade virtual. Com isso, estão sendo utilizadas as legislações já existentes e têm surgido novas, específicas para o tema do uso da informática na internet ou do mau uso dos dados privados.

A mais expressiva garantia da proteção da privacidade dos cidadãos foi construída na Declaração Universal dos Direitos das Nações Unidas, especialmente no artigo 19, que informa que:

[...] toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras [...] (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009).

O brasileiro, nesse sentido, conta com a Constituição de 1988, artigo 5º, inciso X, que determina serem “[...] invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação [...]” (BRASIL, 1988); e, no inciso XII do mesmo artigo, que:

[...] é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal [...] (BRASIL, 1988).

Em abril de 2013, entrou em vigor a primeira lei brasileira específica para o ambiente virtual, a Lei nº 12.737/2012, com o apelido de “Lei Carolina Dieckmann”, que modifica o Código Penal para tipificar como infrações uma série de condutas no ambiente digital, em especial o vazamento dos dados. Outra conquista da legislação demarcatória do ambiente virtual no Brasil foi conquistada em 2014, considerada uma das melhores legislações sobre o tema da Internet e denominada Marco Civil da Internet, Lei nº 12.965/2014, que garante, em seu artigo 3º, incisos II e III, respectivamente, a “proteção à privacidade” e a “proteção aos dados pessoais”.



Saiba mais

Assista o vídeo de Leandro Karnal sobre a solidão nas redes sociais no link a seguir.

<https://goo.gl/AMh1NN>

Além disso, você pode se informar sobre o que são os crimes cibernéticos e como se precaver. A reportagem do site Brasil Econômico, disponível no link a seguir, dá algumas dicas.

<https://goo.gl/fBSnxc>

O acesso desigual à informação – desafios éticos

A grande conquista humana da contemporaneidade que é o acesso ao conhecimento e às informações via conexão formada pela rede mundial de

computadores não é tão democrática nem liberada como alguns representantes mundiais querem fazer crer. O fato de algumas regiões do mundo ainda não proporcionarem aos seus habitantes o acesso traz à tona o fato de que as questões político-econômicas caminham juntas com as sociais, e isso reflete na desigualdade aos mecanismos de informação existentes nas comunidades mais ricas.

Em 2014, a Organização das Nações Unidas (ONU) apresentou um relatório denominado Revolução de Dados para o Desenvolvimento Sustentável, criado por um Grupo Consultivo de Especialistas Independentes, que destacou a invisibilidade de alguns temas e a desigualdade do acesso à informação como os dois grandes desafios globais. O Grupo destacava propostas para tentar erradicar essas lacunas, tais como: incentivo à inovação; a mobilização de recursos para superar as desigualdades entre países desenvolvidos/em desenvolvimento e entre ricos e pobres; a coordenação necessária para que a revolução de dados realize a concretização do desenvolvimento sustentável aos povos vulneráveis.

No final de 2017, a ONU, por meio da UNICEF, seu braço para a infância e juventude, publica o estudo *The State of the World's Children 2017: Children in a digital world*, no qual se demonstra como a tecnologia digital está afetando a vida das crianças e dos jovens no mundo, identificando as oportunidades de vida e os perigos que a rede mundial apresenta. Os benefícios que poderiam oferecer às crianças mais vulneráveis, aquelas que crescem na pobreza ou são afetadas por emergências humanitárias, seria a possibilidade de melhoria do conhecimento, habilidades para o trabalho digital, a sua conexão e a comunicação de seus pontos de vista. Por outro lado, a realidade é muito cruel, pois praticamente um terço da juventude mundial – 346 milhões – não está online, exacerbando as desigualdades e reduzindo a capacidade das crianças de participar em uma economia cada vez mais digital. Além disso, não é somente a impossibilidade de participar que é negativa: percebeu-se a ausência de supervisão dos responsáveis, o que torna mais perigosa a participação online. Também se viu, por meio do relatório, como o uso da internet amplifica a vulnerabilidade de jovens e crianças, que têm perdas em sua privacidade, mau uso das informações, recebem informações advindas de conteúdos prejudiciais a um crescimento saudável e um exacerbado cyberbullying (que são práticas de agressão moral organizadas por grupos, contra uma determinada pessoa, e alimentadas via internet) (TODA MATÉRIA, c2018). Se tudo isso já não fosse muito ruim para a infância já prejudicada, há redes digitais que exploram e abusam, tais como a Dark Web e as criptografias, que possibilitam o tráfico e o abuso sexual infantil “feito sob encomenda” (UNICEF, 2017).

A reprodução digital das desigualdades

Uma pesquisa do Instituto Nacional de Ciências e Tecnologia, Projeto do Observatório das Metrópoles, analisou, por meio da Pesquisa Nacional por Amostras de Domicílio (PNAD) do IBGE (2014), o acesso aos computadores e à internet nos anos de 2000 a 2009 nas regiões metropolitanas do Brasil. Na análise dos dados, verificou-se a influência das questões de desigualdades de renda, de educação dos entrevistados e do espaço de moradia no momento da ascensão, ou não, dos resultados. Os grupos menos abastados ainda têm grande dificuldade na compra de microcomputadores em domicílio: no período estudado, 54% dos domicílios não tinham computadores, ou seja, mais do que a conexão na web em si, muitos brasileiros ainda não têm poder de compra para a máquina.

Além disso, verificou-se que o acesso é estratificado, depende da quantidade de anos de estudo, renda, classe e local de moradia. As desigualdades de acesso e capacidade de usos das Tecnologias de Informação e Comunicação (TICs) reproduzem a problemática socioeconômica em que as desigualdades de oportunidades, as condições de moradia, as dificuldades no acesso ao mercado de trabalho digno se somam aos dados das dificuldades no uso das tecnologias digitais (RIBEIRO, et al., 2011).

De acordo com a 12ª edição da pesquisa TIC Domicílios, divulgada em setembro de 2017 pelo Comitê Gestor da Internet no Brasil (CGI.br), por meio do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), 36,7 milhões de domicílios, ou seja, 54% do total brasileiro, têm acesso à internet. No entanto, essa parcela é desigual, já que depende da esfera social à qual o indivíduo pertence. A proporcionalidade dos acessos continua estratificada por classe social, área e região em que se vive, isto é, pelas condições de vida. Para as classes mais ricas, é uma realidade o acesso à internet (a classe A tem 98% dos lares com internet e a B, 91%); na classe C, 60% dos domicílios têm internet e na D/E, apenas 23%. A alteração:

[...] atinge também as regiões. No Nordeste, 40% dos domicílios (ou 7,2 milhões) estão conectados, bem abaixo do Sudeste, que segue com a maior proporção (64% ou 18,8 milhões) de lares conectados, seguido do Centro-Oeste (56% ou 2,9 milhões) e do Sul (52% ou 5,4 milhões). No Norte, são 46% (ou 2,4 milhões de domicílios) [...] (PRESCOTT, 2017).

A internet, no Brasil, continua restrita a uma faixa abastada da população ou a espaços públicos mantidos por prefeituras ou microempresas, como os telecentros e as *lan houses*, o que continua gerando uma exclusão digital de determinados cidadãos de menor renda socioeconômica (Figura 1).



Figura 1. A charge explicita a realidade de muitos brasileiros no que diz respeito à exclusão digital.

Fonte: MatiuZZi (2011).



Referências

1 CARTA AOS CORÍNTIOS, cap. 10, vers. 23. In: *BÍBLIA ONLINE*. [S.l.: s.n., 2018]. Disponível em: <<https://www.biblionline.com.br/acf/1co/10/23>>. Acesso em: 25 fev. 2018.

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: Presidência da República, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 25 fev. 2018.

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: Presidência da República, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 fev. 2018.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília: Presidência da República, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 25 fev. 2018.

BRASIL. Instituto Brasileiro de Geografia e Estatística. *Síntese de indicadores sociais: uma análise das condições de vida da população brasileira*. Rio de Janeiro: IBGE, 2014.

CASTELLS, M. *Redes sociais e transformação da sociedade*. [S.l.]: Centro Ruth Cardoso, 2010. Disponível em: <<http://www.centroruthcardoso.org.br/wp-content/uploads/2014/12/01-2010.pdf>>. Acesso em: 25 fev. 2018.

CHAUÍ, M. *Convite à filosofia*. São Paulo: Ática, 2000.

FERREIRA, G. C. Redes sociais de informação: uma história e um estudo de caso. *Perspectivas em Ciência da Informação*, Minas Gerais, v. 16, n. 3, p. 208-231, abr. 2011. Disponível em: <<http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/1149>>. Acesso em: 12 dez. 2017.

FUGAZZA, G. Q.; SALDANHA, G. S. Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais. *Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação*, Florianópolis, v. 22, n. 50, p. 91-101, set. 2017. Disponível em: <<https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2017v22n50p91>>. Acesso em: 15 dez. 2017.

GLOCK, R. S.; GOLDIN J. R. Ética profissional é compromisso social. *Mundo Jovem*, Porto Alegre, v. 335, p. 2-3, 2003.

LINS, M. *A fluidez do mundo líquido de Zygmunt Bauman*. Programa Milênio, 29 abr. 2016. Entrevista Programa Milênio/GloboNews. Disponível em: <<https://www.fronteras.com/entrevistas/a-fluidez-do-mundo-liquido-de-zygmunt-bauman>>. Acesso em: 12 dez. 2017.

MATIUZZI, P. [Mundo - desde 2007]. *Exclusão Digital*. 2011. Disponível em: <<http://paulomatiuzzi.blogspot.com.br/2011/04/exclusao-digital.html>>. Acesso em: 29 mar. 2018.

MONTEIRO, S. D. O ciberespaço: o termo, a definição e o conceito. *Pesquisa Brasileira em Ciência da Informação e Biblioteconomia*, Brasília, v. 2, n. 2, 2007. Disponível em: <<http://periodicos.ufpb.br/ojs2/index.php/pbcib/article/view/6989>>. Acesso em: 15 dez. 2017.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Rio de Janeiro: ONU, 2009. Disponível em: <<http://www.onu.org.br/img/2014/09/DUDH.pdf>>. Acesso em: 25 fev. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Desigualdade no acesso à informação continua sendo desafio global, alertam especialistas da ONU*. [S.l.]: ONU, 2014. Disponível em: <<https://nacoesunidas.org/desigualdade-no-acesso-a-informacao-continua-sendo-desafio-global-alertam-especialistas-da-onu-2>>. Acesso em: 15 dez. 2017.

PRESCOTT, R. Preço ainda barra maior inclusão digital e acesso à internet segue desigual. *ABRANET*, 05 set. 2017. Disponível em: <<http://www.abranet.org.br/Noticias/Preco-ainda-barra-maior-inclusao-digital-e-acesso-a-internet-segue-desigual-1593.html?UserActiveTemplate=site#Wjc4SdKnG1s>>. Acesso em: 14 dez. 2017.

RIBEIRO, L. C. Q. et al. A reprodução digital das desigualdades: acesso e uso da internet, posição de classe e território. In: ENCONTRO ANUAL DA ANPOCS, 35., Caxambu, 2011. *Anais...* São Paulo: ANPOCS, 2011. Disponível em: <<http://www.anpocs.org/index.php/papers-35-encontro/gt-29/gt06-13/899-a-reproducao-digital-das-desigualdades-acesso-e-uso-da-internet-posicao-de-classe-e-territorio/file>>. Acesso em: 14 dez. 2017.

TODA MATÉRIA. *Cyberbullying*. [S.l.]: Toda Matéria, 2017. Disponível em: <<https://www.todamateria.com.br/cyberbullying>>. Acesso em: 27 dez. 2017.

UNICEF. *The state of the world's children 2017: children in a digital world*. [S.l.]: UNICEF, 2017. Disponível em: <https://www.unicef.org/publications/index_101992.html>. Acesso em: 16 dez. 2017.

Leitura recomendada

RIBEIRO, L. C. Q. et al. Desigualdades digitais: acesso e uso da internet, posição socioeconômica e segmentação espacial nas metrópoles brasileiras. *Análise Social*, Lisboa, n. 207, p. 288-320, abr. 2013. Disponível em: <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S0003-25732013000200002&lng=pt&nrm=iso>. Acesso em: 16 dez. 2017.

Internet e a mudança no cenário econômico

Objetivos de aprendizagem

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

- Descrever a trajetória da internet no Brasil.
- Analisar o impacto da rede nas pequenas e médias empresas.
- Mensurar o tamanho do mercado de *e-commerce* no Brasil e na América Latina.

Introdução

A internet, por meio do comércio eletrônico, traz uma série de vantagens para as pequenas e médias empresas (PMEs), como o baixo custo de investimento e manutenção, e a oportunidade de atender a nichos de mercado com ofertas de produtos e serviços específicas. No entanto, esse cenário ainda pode ser explorado, tanto no Brasil como na América Latina, uma vez que há muito potencial e muito a evoluir nesse mercado.

Neste capítulo, você vai conhecer a história da internet no Brasil, para que possa compreender melhor o seu impacto na vida das pessoas e no mundo dos negócios. Além disso, conhecerá como o Brasil se organizou e acompanhou essa evolução tecnológica.

A internet no Brasil

Antes de estudar a internet no Brasil, precisamos primeiro voltar um pouco na história e falar sobre a sua origem, para compreender a sua importância na pesquisa científica e no desenvolvimento de outras tecnologias. Segundo Franco Júnior (2006, p. 22), “[...] a internet é derivada da rede militar surgida nos anos 60 ARPANet. A ideia naquela época da ‘guerra fria’ era a criação de uma rede de comunicação segura, mesmo que parte dela sofresse um colapso”.

Inicialmente, o projeto foi desenvolvido pelo Departamento de Defesa dos Estados Unidos com a função de interligar computadores em diversos pontos estratégicos naquele País, como bases militares e centros de pesquisa e tecnologia. Assim, criou-se o conceito de vários **computadores interligados**, cada um exercendo atividades específicas, e não mais uma máquina centralizada.

Com relação ao Brasil, o site da Rede Nacional de Ensino e Pesquisa (RNP) relata que, em 1988:

[...] a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e o Laboratório Nacional de Computação Científica (LNCC) foram duas instituições pioneiras em se conectar à Bitnet, tecnologia anterior à internet e ao World Wide Web, que permitia a transferência de arquivos em texto por correio eletrônico.

Porém, apenas em 1990, a criação do sistema chamado de hipertexto (*world wide web* — WWW) facilitou e impulsionou a navegação.

Limeira (2007, p. 29) destaca “[...] que no Brasil a Rede Nacional de Ensino e Pesquisa (RNP) foi criada em setembro de 1989 pelo então Ministério da Ciência e Tecnologia (MCT). O seu objetivo era construir uma infraestrutura nacional de rede internet de âmbito acadêmico”. A Rede Nacional de Pesquisa — como era chamada no seu início — tinha também a função de disseminar o uso de redes no país.

Conforme Turchi (2019, p. 9), “[...] em dezembro de 1994 a Embratel lançou o serviço experimental de Internet comercial, mas somente em 1995 é que foi possível, pela iniciativa do Ministério das Telecomunicações e do Ministério da Ciência e Tecnologia, a abertura ao setor privado da Internet para exploração comercial” no Brasil. No mesmo ano, foi criado o Comitê Gestor da Internet (CGI).

Nesse cenário, algumas empresas já estavam de olho na internet e foram as pioneiras. De acordo com Prado (2011), em 1995, o jornal Folha de São Paulo colocou na web a sua primeira página; já o Jornal do Brasil (JB) lançou a primeira cobertura completa em 28 de maio de 1996. Na televisão, o casal de protagonistas da novela Explode Coração, da rede Globo, conheceu-se pela internet.

De 1989 a 1996, existiam 851 domínios registrados como “.br”. Nesse período, os domínios eram registrados pela FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo). Em 1996, o CGI lançou o Ato Normativo nº. 01, “Regras sobre a atribuição de nomes de domínio na internet no Brasil”, que foi o primeiro documento que definia o registro de domínios.

Em 2005, a competência para realizar as atividades de registro de nomes de domínio, distribuição de endereços IPs e a sua manutenção na internet foi delegada ao NIC.br (Núcleo de Informação e Coordenação do Ponto BR). Já em 2006, o Brasil bateu a casa de um milhão de domínios “.br” registrados. O NIC apresentou, no seu relatório anual, que somente em 2017 foram registrados 1,2 milhão de novos domínios, e o “.br” ultrapassou a marca de 3,9 milhões registros — em relativa estabilidade, se comparado a 2016.

Turchi (2019, p. 10) aponta que o:

[...] crescimento da rede no Brasil se intensificou, chegando a 120 milhões de usuários em 2014. Naquele ano, no mundo todo, segundo o relatório anual da União Internacional de Telecomunicações (ITU), havia 2,3 bilhões de internautas, ou seja, 33% da população. Em 2014, metade da população mundial estaria conectada à rede, segundo estimativa da entidade.

Dessa forma, podemos observar que o Brasil sempre acompanhou a tendência mundial para adesão à rede, que hoje é denominada comumente como internet. Isso coloca o Brasil próximo dos países com maior desenvolvimento tecnológico, influenciando diretamente o comércio eletrônico. Assim, podemos afirmar que, estruturalmente, o empreendedor nacional consegue acompanhar a tecnologia que vem de fora.

No entanto, é preciso considerar outras questões para o comércio eletrônico, como a parte legal (Código de Defesa do Consumidor, tributação específica, direito digital, etc.) e as políticas públicas para o incentivo desse modelo de negócio.

Quem são os usuários e como eles acessam a internet no Brasil

A Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD) de 2016, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE, 2016), apresentou o tema suplementar tecnologia da informação e comunicação (TIC) com os seguintes resultados em relação aos equipamentos usados para acessar a internet no Brasil:

- 94,6% acessam a internet usando telefone celular;
- 63,7% acessam por microcomputador;
- 16,4% usam tablet.

Isso demonstra claramente que, para o comércio eletrônico, a estratégia deverá ter como foco principal, quando se tratar de consumidor final, o acesso usando celulares. Ainda, a pesquisa apresenta dados importantes para a formação do perfil do usuário de internet (IBGE, 2016):

- 64,7% das pessoas de 10 anos ou mais de idade utilizam a internet;
- 75% das pessoas de 10 anos ou mais de idade que não acessaram a internet não o fizeram por não saberem usá-la ou por falta de interesse.

A pesquisa aponta também a finalidade do acesso à internet (IBGE, 2016):

- 94,2% usam a internet para enviar ou receber mensagens de texto, voz ou imagens por aplicativos diferentes de e-mail;
- 76,4% usam para assistir a vídeos, inclusive programas, séries e filmes;
- 73,3% a utilizam para conversar por chamadas de voz ou vídeo;
- 69,3% usam para enviar ou receber e-mails (correio eletrônico).

Os números sobre o acesso à internet são impressionantes. Turchi (2019) afirma que em 1999 o número de usuários estava na casa de 2,5 milhões, já em 2017 o número cresceu para 139 milhões. A existência de banda larga é um fator determinante para a melhoria da qualidade de acesso, sendo usada em 70% dos domicílios com acesso à internet. Vale lembrar que, até pouco tempo atrás, a participação das *lan houses* e dos *cyber* cafês era superior a 50% do volume de acessos, devido à dificuldade na aquisição de computadores e banda larga pelo público de baixa renda.



Saiba mais

Saiba mais sobre o perfil de quem acessa à internet no Brasil na Pesquisa Nacional por Amostra de Domicílios Contínua, do IBGE, com o tema tecnologia da informação e comunicação:

<https://goo.gl/7YYLkS>



Pequenas e médias empresas e o potencial do comércio eletrônico

As empresas são classificadas no Brasil pelo seu porte, adotando como critério a receita bruta: quanto menor a receita, menor o seu porte. Para ser classificada como pequena, por exemplo, uma empresa deve ter receita anual entre 360 mil e 4,8 milhões de reais.

Essa classificação está prevista na Lei Geral das Microempresas e Empresas de Pequeno Porte. Segundo o Sebrae (2019), são quatro os benefícios dessas empresas:

- simplificação e desburocratização;
- facilidades para acesso ao mercado;
- facilidades para obtenção de crédito e acesso à justiça;
- estímulo à inovação e à exportação.

Apesar de as pequenas empresas terem essas vantagens garantidas por lei e o comércio eletrônico ter um baixo custo para implementação e manutenção, é baixa a adesão a esse canal de vendas por essas empresas. Turchi (2019, p. 7) acrescenta:

[...] apesar de todas as inovações tecnológicas e da disponibilidade de ferramentas gratuitas na Internet, que estão contribuindo para mudar os relacionamentos interpessoais, comerciais e a forma de se fazer negócios, a realidade tem demonstrado que grande parcela das pequenas e médias empresas ainda não usufrui desses recursos como deveria e sequer está familiarizada com as terminologias relativas a essas atividades.

Empresas de pequeno porte ainda não enxergaram o potencial do *e-commerce* para os seus negócios. Isso pode se dar pelo fato de essas empresas terem estruturas enxutas e com foco no que é o seu negócio. Turchi (2019) aponta que entre as principais dificuldades alegadas pelos gestores das PMEs para usar a internet de forma mais intensa estão a falta de tempo, de foco para buscar soluções e de equipe dedicada. Isso se dá porque normalmente os microempresários são os responsáveis por grande parte da operação das suas empresas, desde a compra dos produtos, negociações e pagamentos até as vendas.

Boa parte das microempresas não tem sequer um site institucional. A pesquisa TIC Empresas 2017, realizada pelo NIC.br, aponta que em 2017, apenas 11% das microempresas no Norte e 18% no Nordeste tinham um site. Já no Centro-Oeste, eram 26%, e esse número aumenta quando se trata das regiões Sudeste e Sul, em que 33 e 30%, respectivamente, tinham site (MARTINHÃO, 2018).

Em 2013, segundo Turchi (2019, p. 20), “[...] as PMEs faturaram aproximadamente R\$ 5 bilhões no *e-commerce*, representando cerca de 16% do volume de toda a categoria, devendo atingir 25% até o final de 2017, segundo previsão da ABComm”. Além disso, conforme o Sebrae, as PMEs representavam 75% de todas as lojas virtuais do Brasil em 2016, mas o faturamento ficava em torno de 25%.

A pesquisa *E-commerce Radar 2017* ainda apontou que 21,80% dos pedidos do *e-commerce* vieram da cidade de São Paulo e 13% do Rio de Janeiro. Assim, fica claro diante dos dados que as PMEs que aderiram ao canal de vendas do *e-commerce* estão concentradas geograficamente (em especial em São Paulo) e ainda representam um baixo faturamento.

O mercado de comércio eletrônico ainda é pouco explorado, representando um grande potencial para as PMEs competirem em melhores condições com grandes empresas. Isso é possível por meio de estratégias diferenciadas e oferta de produtos pouco explorados pelas grandes empresas.

Além disso, as grandes empresas não têm a agilidade e a facilidade de atender aos consumidores com maior proximidade, buscando entender as suas necessidades. Para as PMEs costuma ser mais fácil customizar e personalizar produtos e serviços para atender a clientes diferenciados, além de poder ofertar produtos específicos, atendendo a nichos de mercado.



Fique atento

As pequenas lojas virtuais devem planejar as suas ofertas e promoções de forma direcionada para regiões e locais específicos, reduzindo o custo e especializando o seu atendimento.

A cauda longa

Uma loja física tem um custo muito alto para as PMEs. Mantê-la de portas abertas representa um grande montante financeiro, diferentemente da loja

virtual, que fica aberta sete dias, durante 24 horas, podendo ofertar produtos diferenciados.

Simchi-Levi, Kaminsky e Simchi-Levi (2010, p. 437) aponta que:

[...] um dos aspectos interessantes da Internet é que ela é o fenômeno “cauda longa”, que ocorre no mercado quase ilimitado de oferta e demanda aberto pela Internet. Neste mercado, descrito no livro *The Long Tail* (A cauda longa) de Chris Anderson, a falta de restrições físicas ou locais permite que os varejistas se concentrem e engrossem receitas com os itens menos populares de seus catálogos.

Para Baltzan (2016, p. 200):

[...] a teoria de Chris Anderson, descreve as estratégias de negócio eletrônico para nichos de mercado como a captura da cauda longa, referindo-se à cauda de uma típica curva de vendas. Essa estratégia demonstra como os produtos de nicho podem ter modelos de negócios viáveis e rentáveis ao ser comercializados por meio do negócio eletrônico. Nos modelos de venda tradicionais, a loja é limitada pelo espaço de prateleira ao selecionar os produtos para venda.



Fique atento

Nicho de mercado é a menor parcela de um segmento de mercado. Assim, tem características especiais e é formado por um número reduzido de pessoas com necessidades semelhantes. Um nicho de mercado pode ser melhor atendido por PMEs via comércio eletrônico.

Assim, a teoria da cauda longa demonstra claramente as oportunidades para pequenos empreendedores, que podem competir no comércio eletrônico até mesmo com grandes empresas. Para isso, será necessário ofertar produtos e serviços diferenciados, que atendam a nichos de mercado específicos, pois os produtos de massa podem tranquilamente ser vendidos por grandes empresas de *e-commerce*.

Tendo claro que o objetivo é atender às necessidades dos consumidores com produtos específicos, a sua busca também fica segmentada, ou seja, a estratégia de marketing terá um investimento menor, pois estará em um mercado concentrado.

Além do diferencial do produto ou serviço ofertado, o atendimento para nicho consegue ser mais eficaz: o lojista conhece melhor o seu público e as suas neces-

sidades, podendo então personalizar ou customizar as ofertas para esse público. Por outro lado, o consumidor se sente valorizado pela empresa, melhorando a imagem da marca e facilitando o relacionamento. Quando isso acontece, o preço deixa de ser o maior — e talvez o único — motivo na decisão de compra.

Segundo Turchi (2019, p. 24), na visão de Pedro Guasti, diretor geral da Ebit:

Diversos nichos da indústria e do comércio que trabalhavam com a Internet tiveram a chance de perceber que, mais importante do que a grande audiência, o segredo do sucesso estava em estabelecer um relacionamento estreito com o consumidor, oferecendo a ele um produto ou serviço que se adequasse especificamente a cada uma das suas necessidades. Muito mais do que uma simples explicação filosófica, a teoria cooperou efetivamente para que se entendesse a fase de transformação pela qual o mercado passava.



Exemplo

Observe o exemplo descrito por Baltzan (2016, p. 200):

A Netflix oferece um excelente exemplo da cauda longa. Vamos supor que uma loja qualquer da Blockbuster mantém 3 mil filmes em estoque, enquanto a Netflix, sem limitações de prateleiras físicas, pode contar com 100 mil filmes.

Olhando para os dados de vendas, a maior parte da receita da Blockbuster vem de filmes novos que são alugados todos os dias, ao passo que títulos mais antigos são locados somente algumas vezes por mês e não justificam o custo de mantê-los em estoque. Desse modo, a cauda de vendas da Blockbuster termina no título 3 mil.

No entanto, a Netflix, que não tem limitações físicas, pode estender sua cauda para além dos 100 mil (e com streaming de vídeo, talvez 200 mil). Ao estender a sua cauda, a Netflix aumenta as vendas, mesmo se um título é alugado apenas algumas vezes.

Esse exemplo da Netflix demonstra como uma empresa, ao compreender a cauda longa, pode se beneficiar. Nesse caso, boa parte da sua atratividade, principalmente no início, foram os filmes fora do catálogo, ou seja, que não eram lançamentos, mas ela oferecia comodidade (sem necessidade de o consumidor de sair de casa) e baixo preço (assinatura mensal). Essa foi a fórmula do sucesso da empresa. Depois vieram as produções próprias, os filmes exclusivos, a variedade de séries, entre outros. A Figura 1 traz um gráfico exemplificando a cauda longa.

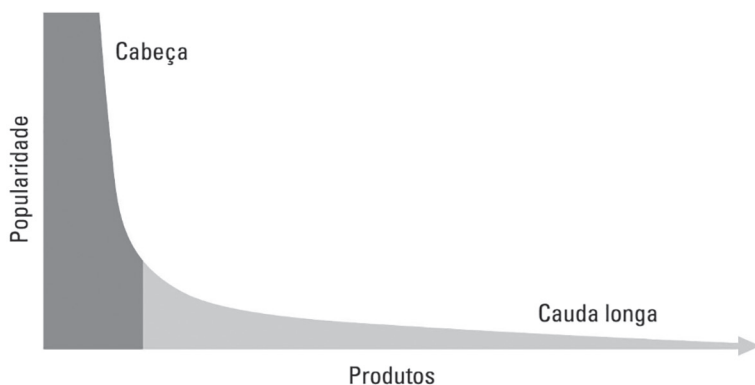


Figura 1. A cauda longa.

Fonte: Baltzan (2016, p. 201).

Potencial do e-commerce no Brasil e na América Latina

O número de brasileiros com 10 anos ou mais que acessaram a internet em 2017 chegou a aproximadamente 126 milhões de usuários — 10 milhões a mais que em 2016, segundo o IBGE. No ano de 2018, apenas nos seis primeiros meses do ano, 27,4 milhões de pessoas fizeram pelo menos uma compra no comércio eletrônico, conforme a pesquisa Webshoppers 2018 (NIELSEN COMPANY, 2018).

Com isso, podemos afirmar que apenas 22 a 25% dos usuários de internet fazem alguma compra utilizando o comércio eletrônico. Esse número ainda é baixo, demonstrando um enorme potencial de crescimento. Apesar das incertezas na economia e na política, esse mercado ainda registra crescimento ano após ano.

A pesquisa Webshoppers ainda aponta regiões com maior desempenho em vendas, sendo a região Sudeste responsável por mais da metade de todas as vendas no Brasil, conforme segue:

- Sudeste – 61,2%;
- Sul – 16,9%;
- Nordeste – 12,4%;
- Centro-Oeste – 6,8%;
- Norte – 2,7%.

O grande filão são as classes C, D e E, que juntas representam 82% dos consumidores no primeiro semestre de 2018 no Brasil. Veja a distribuição de todas as classes sociais:

- Classe A – 4,8%;
- Classe B – 13%;
- Classe C – 35,8%;
- Classe D – 30,0%;
- Classe E – 16,4%.

No período da pesquisa Webshoppers 2018, a maior participação nos pedidos foi do segmento de saúde/cosméticos e perfumaria, com 15,0%, seguido por moda e acessórios, que representou 14,5%. Em volume financeiro, o destaque foi para telefonia/celulares, com 18,9%; em segundo lugar, eletrodomésticos, com 17,9%. Veja os dados completos na Figura 2.

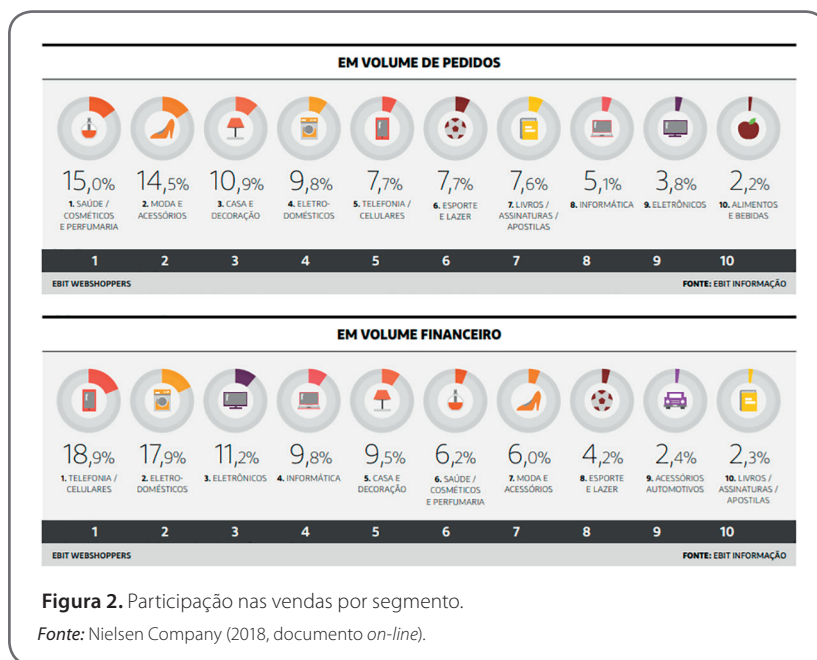


Figura 2. Participação nas vendas por segmento.

Fonte: Nielsen Company (2018, documento on-line).

No B2B também há um grande potencial a ser explorado: há mais empresas que compram pela internet do que as que vendem. Em 2017, 22% das empresas

venderam pela internet e, no mesmo período, 66% compraram, segundo a pesquisa TIC Empresas 2017 (MARTINHÃO, 2018).

Conforme Turchi (2019, p. 18):

[...] na América Latina, o Brasil lidera o *e-commerce*, representando em torno de 41% das vendas, sendo aproximadamente 85% das compras feitas de empresas locais, o que demonstra uma ameaça para novos entrantes internacionais. Comparando, por exemplo, com Porto Rico, em que 95% das compras são provenientes de fora da América Latina, podemos crer que nossa performance se deve a fatores não apenas comerciais, mas também culturais. Porém, os sites internacionais vêm conquistando espaço no *e-commerce* brasileiro ao oferecer preço mais baixo, produto não disponível em lojas brasileiras e lançamentos que não chegaram ao País.

O relatório de 2018 da E-commerce Foundation, publicado pelo site *E-commerce News* (2018), afirma que o faturamento do comércio eletrônico B2C na América Latina cresceu cerca de 60 bilhões de dólares, com uma taxa de crescimento de 13,8%. Esses números devem aumentar no próximo ano, com uma previsão de volume de negócios de cerca de 71 bilhões de dólares e taxa de crescimento de 15,2%.

O relatório ainda traz que os mercados de comércio eletrônico mais maduros encontrados na América Latina incluem o México, com 21 bilhões de dólares em receita de comércio eletrônico, seguidos pelo Brasil, com quase 19 bilhões. Esses dois mercados dominam o comércio eletrônico, enquanto o concorrente mais próximo no faturamento desse tipo, a Argentina, ainda está longe em comparação com os outros, com apenas 6,83 bilhões de dólares (E-COMMERCE NEWS, 2018).

Completando o cenário trazido pelo *E-commerce News* (2018), na América Latina, as estimativas são de que cerca de 60% da população acessou a internet em 2017. Os países que lideraram o uso da internet entre a população em 2016 são Argentina (71%), Costa Rica, Chile e Uruguai (66%), República Dominicana e Brasil (61%).

Todas as pesquisas apontam que tanto o Brasil quanto a América Latina como um todo têm grande potencial para o *e-commerce*. O consumidor tem buscado cada vez mais comprar pelo comércio eletrônico, até porque a nova geração, com os nativos digitais, não tem mais o receio que as gerações anteriores tinham desse tipo de compra.

Nesse cenário, as PMEs podem entrar no mercado e concorrer em condição de igualdade com empresas maiores, desde que ofertem produtos e serviços diferenciados.



Referências

ASSOCIAÇÃO BRASILEIRA DE COMÉRCIO ELETRÔNICO (ABCOMM). Estudo E-commerce Radar 2017. *ABCOMM*, 2017. Disponível em: <https://abcomm.org/noticias/estudo-e-commerce-radar-2017>. Acesso em: 27 fev. 2019.

BALTZAN, P. *Tecnologia orientada para gestão*. 6. ed. Porto Alegre: AMGH, 2016.

COMITÊ GESTOR DA INTERNET (CGI). História. *Cgi.br*, 2017. Disponível em: <https://cgi.br/historicos>. Acesso em: 27 fev. 2019.

E-COMMERCE NEWS. Relatório traça panorama do comércio eletrônico na América Latina. *E-commerce News*, 2018. Disponível em: <https://ecommercenews.com.br/noticias/pesquisas-noticias/relatorio-traca-panorama-do-comercio-eletronico-na-america-latina>. Acesso em: 27 fev. 2019.

FRANCO JÚNIOR, C. F. *E-business na infoera: o impacto da infoera na administração de empresas: internet e telecomunicação, comunicação multimídia digital, tecnologia e sistemas de informação*. 4. ed. São Paulo: Atlas, 2006.

INSTITUTO BRASILEIRO DE ESTATÍSTICA (IBGE). Pesquisa nacional por amostra de domicílios contínua: acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2016. Disponível em: https://agenciadenoticias.ibge.gov.br/media/com_mediaibge/arquivos/c62c9d551093e4b8e9d9810a6d3bafff.pdf. Acesso em: 27 fev. 2019.

LIMEIRA, T. M. V. *E-marketing: o marketing na internet com casos brasileiros*. 2. ed. São Paulo: Saraiva, 2007.

MARTINHÃO, M. S. (coord.). *TIC Empresas: pesquisa sobre o uso das tecnologias da informação e comunicação nas empresas brasileiras* 2017. São Paulo: Comitê Gestor da Internet no Brasil, 2018. Disponível em: https://www.nic.br/media/docs/publicacoes/2/TIC_Empresas_2017_livro_eletronico.pdf. Acesso em: 27 fev. 2019.

NIELSEN COMPANY. Webshoppers 38: e-commerce fatura R\$ 23,6 bilhões no 1º semestre de 2018, alta de 12,1%. *Nielsen*, 2018. Disponível em: <https://www.nielsen.com/br/pt/insights/news/2018/Webshoppers-38-e-commerce-fatura-vingte-e-tres-bilhoes-no-primeiro-semester-de-2018-alta-de-doze-porcento.html>. Acesso em: 27 fev. 2019.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). Relatório de atividades 2017. Disponível em: https://www.nic.br/media/docs/publicacoes/9/RA_CGI_NIC_2017_livro_eletronico.pdf. Acesso em: 27 fev. 2019.

PRADO, M. *Webjornalismo*. Rio de Janeiro: LTC, 2011.

REDE NACIONAL DE ENSINO E PESQUISA (RNP). A história por trás dos 20 anos da internet comercial no Brasil. *RNP*, 2018. Disponível em: <https://www.rnp.br/destaques/historia-por-tras-20-anos-internet-comercial-brasil>. Acesso em: 27 fev. 2019.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS (SEBRAE). Confira as diferenças entre microempresa, pequena empresa e MEI. *Sebrae*, 2019. Disponível em: <http://www.sebrae.com.br/sites/PortalSebrae/artigos/entenda-as-diferencas-entre-microempresa-pequena-empresa-e-mei,03f5438af1c92410VgnVCM100000b272010aRCRD>. Acesso em: 27 fev. 2019.

SIMCHI-LEVI, D.; KAMINSKY, P.; SIMCHI-LEVI, E. *Cadeia de suprimentos, projeto e gestão: conceitos, estratégias e estudos de caso*. 3. ed. Porto Alegre: Bookman, 2010.

TURCHI, S. R. *Estratégias de marketing digital e e-commerce*. 2. ed. São Paulo: Atlas, 2019.

Legislação e convenções

Objetivos de aprendizagem

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

- Reconhecer a legislação que permeia a propriedade intelectual.
- Praticar as legislações ordinárias.
- Explicar a atuação das convenções internacionais.

Introdução

A globalização, o desenvolvimento da tecnologia e a disputa de mercados internacionais por empresas com os seus produtos são cada vez mais frequentes. Os direitos referentes à propriedade intelectual de produtos, marcas, patentes e criações alcançaram um nível em que é necessária a criação de legislação em cada nação e convenções internacionais como meio de proteção e solução de conflitos.

Neste capítulo, você vai ler sobre a legislação que protege a propriedade intelectual, além de verificar o que cada uma delas protege e é aplicada.

Legislação que permeia a propriedade intelectual

A legislação relativa à propriedade intelectual tem fontes nacionais (as leis ordinárias) e internacionais (convenções), também devendo ser respeitada a aplicação da legislação pertinente de cada país na proteção do direito de autor. No caso do Brasil, há previsão legal primeiramente na Constituição Federal de 1988. No art. 5º, XXVII, XXVIII e XXIX, é tratado diretamente o direito de autor. A aplicação das normas se dá primeiro pela Constituição Federal e, na sequência, pelas convenções internacionais. De forma subsidiária, aplicamos a legislação ordinária pertinente à matéria, como, por exemplo, a Lei nº. 9.279, de 14 de maio de 1996, no que tange à propriedade industrial, a patentes e marcas.

Não há, de forma expressa, uma hierarquia estabelecida para a aplicação da legislação internacional, em especial em relação às convenções. Sabemos que qualquer norma deve respeitar o estabelecido na Constituição Federal de 1988 e que,

somente se respeitado o seu texto, ela será válida. Não pode haver conflito entre o que ambas determinam, sob pena de não ser possível a aplicação da convenção.

Ainda assim, aplicamos subsidiária e concomitantemente a legislação internacional e nacional. A proteção aos direitos inerentes à propriedade intelectual é resultante dos esforços de diversos órgãos estatais. Por exemplo, os Ministérios da Cultura, da Agropecuária e da Indústria, Comércio Exterior e Serviços são responsáveis pela edição de legislação, fiscalização e criação do órgão regulador, como no caso do Instituto Nacional de Propriedade Industrial (INPI). A legislação internacional carece de homologação, conforme o seu tipo ou trâmite. As sentenças estrangeiras e cartas rogatórias são homologadas pelo Superior Tribunal de Justiça (STJ). Já os tratados e as convenções, após a adesão do Brasil, devem ser homologados por legislação pertinente.

A forma de aplicação dos tratados em território brasileiro é divergente, como é o caso do Supremo Tribunal Federal (STF), que defende, em certas decisões, que a sua aplicação somente será válida após ratificação por decreto executivo, sendo equiparados à legislação ordinária. Assim, estariam nos mesmos patamares de validade e eficácia das normas brasileiras. O único tipo de tratado que não se submete a essa hierarquia seriam os relativos a direitos humanos.

Em relação à **legislação ordinária brasileira**, podemos destacar a Lei nº. 9.279/1996, que possui maior proteção sobre o direito de autor, tratando de patente, marcas, desenhos industriais e indicação geográfica. A Lei nº. 10.973, de 2 de dezembro de 2004, também conhecida como Lei da Inovação, trouxe importantes elementos acerca do incentivo à pesquisa científica e tecnológica. Ainda dentro da legislação brasileira, a Lei nº 9.610, de 19 de fevereiro de 1998, também chamada de Lei do Autor, abrangeu obras artísticas e culturais, seus autores e intérpretes. A Lei nº. 9.456, de 25 de abril de 1997, conhecida como Lei de Proteção de Cultivares, posteriormente regulamentada pelo Decreto nº. 2.366, de 5 de novembro de 1997, protege o melhoramento genético, as plantações e o desenvolvimento de novas cultivares.

Já na **legislação internacional**, seja em forma de tratados, convenções, atos ou acordos, destaca-se a Convenção de Paris, iniciada em meados de 1880, tendo como principal tema a proteção dos direitos de propriedade industrial. A Convenção de Berna, em 1886, tratou da proteção de direitos relativos a obras artísticas e culturais. O Tratado de Haia de 1925 foi importante na tentativa de proteção aos desenhos industriais. Já a Convenção de Roma de Direitos Conexos, de 1961, protegeu principalmente as produções musicais, sejam as pessoas que as interpretam, executam, compõem ou transmitem.

Ainda sobre a legislação internacional, o Acordo de Madrid de 1981 se coloca como instituidor de uma legislação internacional sobre o registro de

marcas. O Tratado da Organização Mundial da Propriedade Intelectual sobre *Copyright* foi responsável pela sistematização da propriedade intelectual nos últimos anos. O Tratado de Cooperação em Patentes de 1978 veio para ser um facilitador dos procedimentos de solicitação, busca e exame de patentes. Finalizando a exemplificação de normas internacionais, a Rodada Uruguai de 1986 figura como um momento de discussão sobre o comércio internacional.

A Figura 1 apresenta a aplicação e as principais normas sobre propriedade intelectual na legislação brasileira.

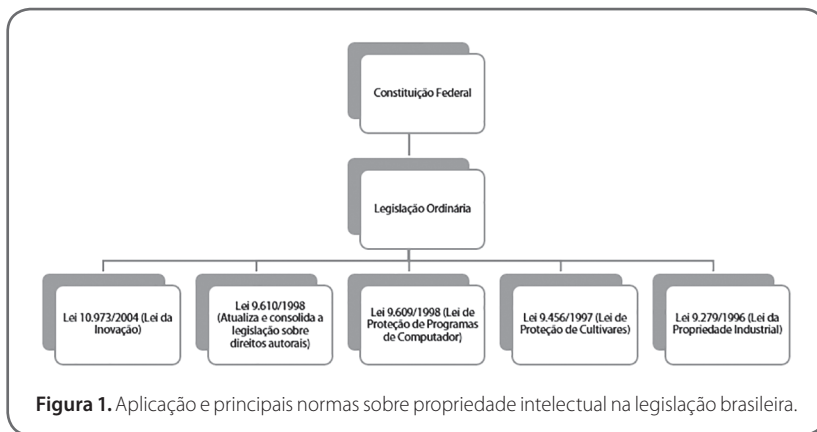


Figura 1. Aplicação e principais normas sobre propriedade intelectual na legislação brasileira.



Fique atento

A Constituição Federal de 1988 protege, no seu art. 5º, o direito de autor. Assim é o Texto Constitucional:

Art. 5º [...]

XXVIII — são assegurados, nos termos da lei:

- a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas;
- b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de que participarem aos criadores, aos intérpretes e às respectivas representações sindicais e associativas;

XXIX — a lei assegurará aos autores de inventos industriais privilégio temporário para sua utilização, bem como proteção às criações industriais, à propriedade das marcas, aos nomes de empresas e a outros signos distintivos, tendo em vista o interesse social e o desenvolvimento tecnológico e econômico do País (BRASIL, 1988).

Legislação ordinária

A legislação ordinária brasileira que protege a propriedade intelectual é relativamente recente. Enquanto as convenções internacionais já tratavam do tema em meados de 1900, a legislação brasileira começou a abranger esses direitos, de forma objetiva, na década de 1990. Mesmo que já se tenham adesões por parte do governo brasileiro até mesmo na década de 1970, a sua atuação efetiva na proteção de direito de autor é bem mais contemporânea.



Link

O site do INPI traz uma coletânea da legislação aplicada à propriedade intelectual. Neste link, você poderá encontrar legislação ordinária, convenções e outras normas que possuem relação com o tema:

<https://goo.gl/aFBfWV>



A **Lei nº. 9.279/1996** merece especial atenção, pois foi um grande avanço na efetivação da proteção estatal em relação à propriedade intelectual. A lei regula direitos e obrigações em relação à propriedade intelectual, devido ao grande interesse econômico gerado pelo tema. O seu primeiro título trata de patentes, estabelecendo requisitos para o seu pedido e a sua concessão, além de determinar as suas nulidades e o que é protegido. O seu tempo de vigência será de 20 anos, e a patente de modelo de utilidade terá vigência de 15 anos contados da data de depósito. A lei ainda faz uma ressalva em relação aos prazos, informando que não serão inferiores a 10 anos para a patente de invenção e a 7 anos para a patente de modelo de utilidade, a contar da data de concessão, com exceção na hipótese de o órgão regulador “estar impedido de proceder ao exame de mérito do pedido, por pendência judicial comprovada ou por motivo de força maior” (BRASIL, 1996).

A mesma lei trata dos desenhos industriais, estabelecendo os limites em relação à concessão e extinção do pedido de registro, determinando que o prazo de registro é válido por 10 anos, contados da data do depósito, o qual pode ser prorrogado por três vezes, em períodos sucessivos de 5 anos cada. Em relação ao registro de marca, notamos uma diferença em relação à contagem do prazo. Enquanto a concessão é válida partindo da data do depósito, no registro de

marca, ela iniciará sua vigência a partir do registro efetivo, tendo validade de 10 anos, prorrogáveis por períodos iguais e sucessivos.

Finalizando os tipos de propriedade intelectual protegidos, a Lei nº. 9.279/1996 estabelece, em relação à indicação geográfica, a divisão e a diferenciação entre indicação de procedência e denominação de origem. Estão previstos também os casos em que a proteção é perdida, não se estabelecendo prazo de vigência, o qual durará enquanto os requisitos e as características perdurarem. O seu texto ainda prevê (BRASIL, 1996):

- crimes contra a propriedade intelectual;
- prazos de âmbito geral;
- regramentos em relação a contratos de transferência de tecnologia e de franquia;
- questões de disposição geral.

A **Lei nº. 10.973/2004**, conhecida como Lei da Inovação, trouxe fomento e incentivo à pesquisa científica e tecnológica, mas o principal ponto de interesse é a proteção a inventores independentes, que são aqueles que não possuem função pública, não são pessoa jurídica e que são possuidores ou autores de criação. Assim, há também o estabelecimento do conceito de **criação**:

[...] criação: invenção, modelo de utilidade, desenho industrial, programa de computador, topografia de circuito integrado, nova cultivar ou cultivar essencialmente derivada e qualquer outro desenvolvimento tecnológico que acarrete ou possa acarretar o surgimento de novo produto, processo ou aperfeiçoamento incremental, obtida por um ou mais criadores (BRASIL, 2004).

A **Lei nº. 9.610/1998**, conhecida como a Lei de Autor, trouxe uma proteção importante para as criações e interpretações artísticas, por representarem uma gama imensa dentro da economia. As obras de caráter literário, artístico ou científico são protegidas e reguladas por essa lei, mas, mesmo possuindo grau de uso da tecnologia, as invenções como *software* são protegidas pela Lei nº. 9.609, de 19 de fevereiro de 1998. Podemos perceber que o legislador quis estabelecer uma diferenciação e separação entre ambas, até pela evolução de *software*, que se faz muito mais célere. A aplicação da Lei nº. 9.610/1998 em relação aos *software* ocorre apenas quando a Lei nº. 9.609/1998 se torna omissa ou quando ambas tenham quesitos em comum, como, por exemplo, a forma de registro.

Dentro ainda da legislação ordinária, a **Lei nº. 9.456/1997** (Lei de Proteção de Cultivares), posteriormente regulamentada pelo Decreto nº. 2.366/1997,

protege o melhoramento genético, as plantações e o desenvolvimento de novas cultivares. Segundo a legislação, **cultivar** seria:

[...] a variedade de qualquer gênero ou espécie vegetal, que seja claramente distinguível de outras conhecidas por uma margem mínima de características descritas, pela denominação própria, homogeneidade, capacidade de se manter estável em gerações sucessivas, além de ser passível de utilização (BRASIL, 1997a).

Assim, na legislação brasileira, há uma proteção heterogênea da propriedade intelectual, tentando abranger diversas manifestações de direito de autor.



Saiba mais

A aplicação dos tratados internacionais na legislação brasileira foi discutida na Ação Direta de Inconstitucionalidade 1480/DF, que discutia a aplicação de tratado em matéria trabalhista, aderido pelo Presidente da República, sem apreciação do Congresso Nacional. Segue a decisão proferida pelo ministro do STF, Celso de Melo (BRASIL, 1997b):

É na Constituição da República — e não na controvérsia doutrinária — que se deve buscar a solução normativa para a questão da incorporação dos atos internacionais ao sistema de direito positivo interno brasileiro. O exame da vigente Constituição Federal permite constatar que a execução dos tratados internacionais e a sua incorporação à ordem jurídica interna decorrem, no sistema adotado pelo Brasil, de um ato subjetivamente complexo, resultante da conjugação de duas vontades homogêneas: a do Congresso Nacional, que resolve, definitivamente, mediante decreto legislativo, sobre tratados, acordos ou atos internacionais (CF, art. 49, I) e a do Presidente da República, que, além de poder celebrar esses atos de direito internacional (CF, art. 84, VIII), também dispõe — enquanto Chefe de Estado que é — da competência para promulgá-los mediante decreto. O iter procedimental de incorporação dos tratados internacionais — superadas as fases prévias da celebração da convenção internacional, de sua aprovação congressional e da ratificação pelo Chefe de Estado — conclui-se com a expedição, pelo Presidente da República, de decreto, de cuja edição derivam três efeitos básicos que lhe são inerentes: (a) a promulgação do tratado internacional; (b) a publicação oficial de seu texto; e (c) a executoriedade do ato internacional, que passa, então, e somente então, a vincular e a obrigar no plano do direito positivo interno.

Convenções internacionais

O Brasil já era membro participante de convenções sobre propriedade intelectual de maneira ativa, mas tendo a sua ratificação (homologação) de forma bem mais tardia. Em relação à legislação internacional, estão em vigor alguns tratados e convenções internacionais, resultados do acordo comum entre diversos países sobre a proteção dos direitos relacionados a criações literárias, artísticas e científicas, invenções, desenhos industriais, marcas, *software*, entre outros.

A Convenção de Paris, como vimos, iniciou como um encontro diplomático em meados de 1880. O principal tema e motivo de proteção por parte dela foram os **direitos de propriedade industrial**, sendo considerada o primeiro esforço para tutelá-los. O texto original passou por atualizações posteriores, em reuniões ocorridas em Roma, onde nenhum país aderiu ao que foi contemplado. Posteriormente, em Bruxelas, ocorreu outra reunião por volta de 1900, seguida por outras reuniões em:

- Washington (por volta de 1911);
- Haia (por volta de 1925);
- Londres (em 1934);
- Lisboa (em 1958);
- Estocolmo (em meados de 1967).

O Brasil aderiu à Convenção de Estocolmo, mas somente em 1992. Outra importante convenção foi a ocorrida em Berna, em 1886. Ela visou à proteção de direitos relativos a **obras artísticas**, tendo sido completada em Paris, em 1896, porém:

- passou por revisões em Berlim (em 1908);
- foi completada de novo em Berna (em 1914);
- foi novamente revista em Roma (em 1928), em Bruxelas (em 1948), em Estocolmo (em 1967) e em Paris (em 1971).

O Tratado de Haia de 1925 foi importante na tentativa de proteção aos **desenhos industriais**, com o intuito de se tornar uma espécie de referência de registros internacionais. Três atos compõem esse tratado, os quais ocorreram em:

- Londres (em 1934);
- Haia (em 1960);
- Genebra (em 1999).

Apesar de tentar formar uma referência para o depósito e os pedidos de registros de desenhos industriais, o Tratado de Haia faz algumas exigências para que isso ocorra, como, por exemplo, o autor do pedido estar domiciliado ou ser natural de algum dos países membros do tratado. Nesse caso, ainda não é tão abrangente a proteção que ele oferece.

A Convenção de Roma de Direitos Conexos, de 1961, protege principalmente as **produções musicais**, sejam as pessoas que as interpretam, executam, compõem ou transmitem. O Tratado da Organização Mundial da Propriedade Intelectual sobre *Copyright*, que acabou por resultar na Conferência Diplomática sobre Questões Relativas aos Direitos de Autor e Direitos Conexos de 1996, é decorrente do desenvolvimento científico e tecnológico alcançado principalmente nos anos 1980.

O Acordo de Madrid de 1981 é responsável pela instituição de uma legislação internacional sobre o registro de marcas. O Acordo de Madri, junto com o Protocolo de Madrid de 1989, ambos com aplicação iniciada somente em 1996, visam à facilitação do registro de **marcas**, protegendo, assim, marcas de produtos e serviços com abrangência internacional. Tal registro equivaleria também a uma reunião de registros, ou seja, existindo o registro internacional, não é necessário ter este e mais o registro nacional, sendo necessária apenas uma única renovação posteriormente, facilitando inclusive alterações de titularidade e de informações cadastrais, por meio apenas de um único processo administrativo.

O Tratado da Organização Mundial da Propriedade Intelectual sobre *Copyright* foi responsável pela sistematização da propriedade intelectual nos últimos anos e tem se tornado alvo dos mais diversos tratados.

O Tratado de Cooperação em Patentes de 1978 surgiu na Convenção de Paris, em 1978. A sua principal função é racionalizar os procedimentos de solicitação, busca e exame de patentes, bem como a divulgação de informações técnicas que nela constam. Tornou-se um dos acordos mais utilizados, pois tem contribuído muito com o avanço na cooperação internacional de patentes.

A Rodada Uruguai de 1986 foi criada pelo General Agreement on Tariffs and Trade (GATT), com o propósito de rediscutir os temas oriundos do comércio internacional. As suas negociações encerraram no Uruguai — Montevideu, em 1994. A sua aprovação ocorreu no final da rodada, no texto do tratado que passou a ser conhecido como Trade-Related Aspects of Intellectual Property Rights (TRIPS), sob a tutela da Organização Mundial do Comércio (OMC).



Fique atento

O TRIPS estabelece os patamares mínimos de proteção aos direitos de propriedade intelectual, com o objetivo de facilitar o comércio internacional entre membros da OMC. Essa talvez tenha sido uma das convenções mais importantes da atualidade.

Existem ainda outros tratados, acordos e convenções de menor expressividade e adesão que podem ser citados, por tratarem de temas expressos ou pertinentes à propriedade intelectual, como:

- Acordo Neuchâtel, assinado entre o Brasil e a Universidade de Neuchâtel, sobre cooperação científica;
- Convenção de Bruxelas de 1974 sobre a distribuição de sinal via satélite.



Exemplo

O Brasil ratificou um tratado em 2015 que facilita o acesso à cultura de deficientes visuais e pessoas com dificuldades de leitura. O Tratado de Marraquexe reduziu a proteção dos direitos autorais das obras, para que o acesso fosse priorizado e facilitado.



Referências

BRASIL. *Lei nº. 10.973, de 2 de dezembro de 2004*. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. 2004. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/10.973.htm>. Acesso em: 9 jan. 2018.

BRASIL. *Decreto nº. 2.366, de 5 de novembro de 1997*. Regulamenta a Lei nº. 9.456, de 25 de abril de 1997, que institui a Proteção de Cultivares, dispõe sobre o Serviço Nacional de Proteção de Cultivares - SNPC, e dá outras providências. 1997a. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1997/d2366.htm>. Acesso em: 9 jan. 2018.

BRASIL. Supremo Tribunal Federal. *Medida cautelar na ação direta de inconstitucionalidade*: ADI-MC 1480. Relator: Ministro Celso de Mello. Julgamento: 4 de setembro de 1997. Brasília: [S.n.], 1997b.

BRASIL. *Lei nº. 9.279, de 14 de maio de 1996*. Regula direitos e obrigações relativos à propriedade industrial. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9279.htm>. Acesso em: 21 jan. 2018.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. Instituto Nacional da Propriedade Intelectual. *Convenção de Paris*. Disponível em: <<http://www.inpi.gov.br/images/stories/CUP.pdf>>. Acesso em: 10 dez. 2017.

ASSOCIAÇÃO BRASILEIRA DA INDÚSTRIA DE MÁQUINAS E EQUIPAMENTOS. *Manual da propriedade intelectual*. Disponível em: <www.abimaq.org.br/Arquivos/Html/IPDMAQ/10Propriedad Ind, Manual - IPDMAQ.pdf>. Acesso em: 9 dez. 2017.

Leituras recomendadas

BASSO, M. *O Regime Internacional de Proteção da propriedade intelectual da OMC/ TRIPS*. In: AMARAL JÚNIOR, A. do (Coord.). *OMC e o comércio internacional*. São Paulo: Aduaneiras, 2002.

BERMUDEZ, J. A. Z. et al. *O acordo TRIPS da OMC e a produção patentária no Brasil: mudanças recentes e implicações para a produção local e o acesso da população aos medicamentos*. Rio de Janeiro: Fiocruz/ENSP, 2000.

BRASIL. Instituto Da Nacional Da Propriedade Industrial. *Legislação geral e pareceres*. 2018. Disponível em: <<http://www.inpi.gov.br/sobre/legislacao-1>>. Acesso em: 21 jan. 2018.

BRASIL. Ministério da Cultura. *Entenda a lei de direitos autorais*. 2014. Disponível em: <<http://www.brasil.gov.br/cultura/2009/11/entenda-a-lei-de-direitos-autorais>>. Acesso em: 21 dez. 2018.

BRASIL. Ministério da Indústria, Comercio Exterior e Serviços. *Legislação de propriedade intelectual*. 2009. Disponível em: <<http://www.mdic.gov.br/legislacao/9-assuntos/categ-comercio-exterior/569-legislacao-de-propriedade-intelectual>>. Acesso em: 21 jan. 2018.

CORREA, C. M. de A. *O direito internacional frente ao instituto da propriedade intelectual: OMC/Trips* (Trade Related Aspects os Intellectual Property Rights). *Revista Paradigma*, Ribeirão Preto, v. 17, 2004. Disponível em: <<http://www9.unaerp.br/revistas/index.php/paradigma/article/view/20/26>>. Acesso em: 21 jan. 2018.

FALABELLA, B. *Propriedade intelectual*. [2018]. Disponível em: <http://www.jurisway.org.br/v2/cursoonline.asp?id_curso=220&pagina=2&id_titulo=2245>. Acesso em: 21 jan. 2018.

FURTADO, L. R. *Sistema de propriedade industrial no direito brasileiro*. Brasília: Livraria e Editora Brasília Jurídica, 1996.

MENCHISE, R.; FERREIRA, D. M. *Aspectos da propriedade intelectual: normas gerais, leis brasileiras, jurisprudências e acesso à cultura e informação*. [2018]. Disponível em: <http://ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=14790>. Acesso em: 21 jan. 2018.

ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL. *Acordo de Haia referente ao registo internacional dos desenhos e modelos industriais: principais características e vantagens*. 2012. Disponível em: <http://www.wipo.int/edocs/pubdocs/pt/designs/911/wipo_pub_911.pdf>. Acesso em: 21 jan. 2018.

PAESANI, L. M. *Manual de propriedade intelectual*. 2. ed. São Paulo: Atlas, 2015.

PIMENTEL, L. O. *Propriedade intelectual e contratos: conceitos básicos*. [2007]. Disponível em: <<http://www.propesquisa.ufsc.br/arquivos/Pimentel-Definicoes-Ago2007.pdf>>. Acesso em: 21 jan. 2018.

SANTANA JÚNIOR, M. B. *O contexto da implantação do acordo TRIPS*. *Revista Brasileira de Direito Internacional*, Curitiba, v. 4, n. 4, jul./dez. 2006. Disponível em: <<http://revistas.ufpr.br/dint/article/view/7539/6643>>. Acesso em: 21 jan. 2018.

SILVEIRA, N. *Propriedade intelectual: propriedade industrial, direito de autor, software, cultivares, nome empresarial e abuso de patentes*. 5. ed. São Paulo: Manole, 2014.

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 <i>sites</i> , 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 <i>sites</i> .	Permanece igual.	<i>Sites</i> 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 <i>versus</i> conteúdo ilegal/ofensivo	Provedores não são punidos por publicações de terceiros. Já <i>sites</i> 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)
Monito- ramento na <i>web</i>	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 ressaltar 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://opinioao.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 nº 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 CGL.br/RES/2012/010/P*. Posicionamento do CGL.br em relação ao parecer final do Deputado Alessandro Molon ao Marco Civil da Internet no Brasil. São Paulo: CGL.br, 2012. Disponível em: <http://www.cgl.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,f9f3a0b2993de310VgnVCM3000009acceba0aRCRD.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 integridade das informações referidas em tais links.

Privacidade e segurança nas transações eletrônicas

Objetivos de aprendizagem

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

- Definir as implicações do armazenamento de dados pessoais *on-line*.
- Avaliar os riscos de exposição de nomes de usuários e senhas pela internet.
- Identificar as formas mais seguras de uso de redes domésticas e públicas.

Introdução

O comércio eletrônico se desenvolveu a partir da internet, que é uma rede pública com acesso a computadores espalhados praticamente pelo mundo todo, conectando vendedores e compradores. Essa interatividade oferece aos profissionais de *marketing* oportunidades antes inexistentes, uma vez que esse modelo de negócio digital permite a criação de vários relatórios que não são possíveis no negócio físico.

Conhecer o perfil de cada consumidor, saber a origem do seu acesso em instantes e ainda saber todo o seu histórico de compras e formas de pagamento são dados importantíssimos para qualquer empreendedor. Porém, toda essa facilidade abre espaço para um problema: a guarda desses dados. Essa tarefa requer das empresas muita atenção e investimento em segurança da informação.

Neste capítulo, você vai entender como são graves as consequências para empresas e usuários que têm os seus dados vazados ou roubados. Além disso, você vai conhecer mais sobre as redes domésticas e as públicas, em relação ao quesito segurança.

Armazenamento de dados pessoais *on-line*

O comércio eletrônico apresenta grandes vantagens em relação aos negócios físicos. Um dos benefícios é poder conhecer de forma quantitativa os hábitos de compra e o perfil dos clientes. Tudo o que é feito nesse mundo virtual é registrado e acumulado, virando uma grande fonte de informações. Todavia, esse cenário não apresenta apenas vantagens.

Stair e Reynolds (2015) apresentam os três **desafios** principais para o comércio eletrônico:

1. preocupação contínua com a privacidade do cliente;
2. superação da falta de confiança do cliente;
3. superação das questões globais.

Essas preocupações chegam a atingir um terço de todos os adultos usuários da internet, que afirmam que não comprarão nada em lojas virtuais por preocupação com a privacidade ou pela falta de confiança nesse tipo de comércio.

Turchi (2019, p. 136) afirma que “[...] se por um lado esse futuro se mostra fascinante em termos de oportunidades de novos negócios e de agilidade na obtenção de informações, por outro tem trazido à tona questionamentos sobre privacidade das informações e ética”. Assim, o desafio a ser perseguido pelas empresas é resolver — ou pelo menos minimizar — as questões ligadas à privacidade.

A segurança na internet é uma questão que gera prejuízos às companhias quando dados de clientes são vazados ou furtados. Por outro lado, esse aspecto eleva o custo da operação, em função do aumento dos investimentos em **segurança da informação**.

Se as empresas estão investindo em segurança, em contrapartida os seus usuários e/ou clientes podem estar tendo os seus dados usados sem consentimento. Pinheiro (2016, p. 94) afirma que:

[...] por um lado, cresce a cada dia o número de empresas que disputam os consumidores da Internet e, consequentemente, a publicidade virtual, com preenchimento de formulários e cadastros, por outro lado, cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual Código do Consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem as pratica.

Ainda que o consumidor esteja resguardado pelo Código do Consumidor, o direito à privacidade não pode superar o interesse público. Paesani (2014, p. 34) lembra:

[...] podem ser impostos limites à normal esfera de privacidade até contra a vontade do indivíduo, mas em correspondência à sua posição na sociedade, se for de relevância pública. Nesses casos, será possível individualizar, se há interesse público em divulgar aspectos da vida privada do indivíduo. O interesse será relevante somente com relação à notícia cujo conhecimento demonstre utilidade para obter elementos de avaliação sobre a pessoa como personalidade pública, limitando, desta forma — e não eliminando — a esfera privada do próprio sujeito.

Assim, as empresas devem manter dados dos seus usuários, para o caso de serem solicitados pela Justiça, em situações de usuários envolvidos em alguma demanda judicial e quando esses dados forem de interesse público.

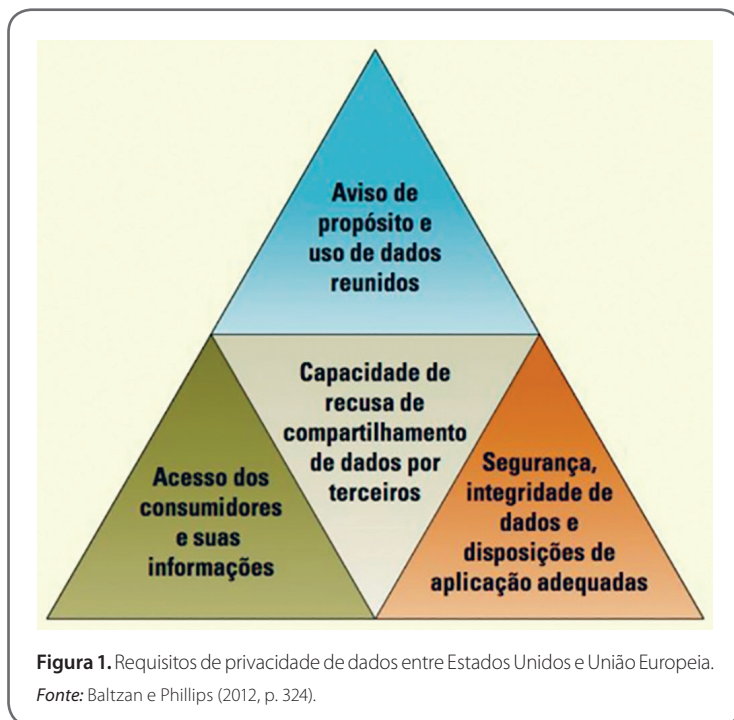
Para Pinheiro (2016, p. 81):

[...] a prova é outra questão importante para a correta aplicação do Direito no mundo digital. Há hipóteses de inversão do ônus da prova devido, principalmente, aos princípios já protegidos pelo Código de Defesa do Consumidor. Um exemplo são as empresas que montam banco de dados de seus usuários na Internet: se o banco de dados for utilizado de forma incorreta ou ilegal, não cabe ao usuário que se sentiu lesado provar tal fato, mas à empresa acusada provar que não agiu dessa forma.

O comércio eletrônico nem sempre se limita a uma área geográfica, nem mesmo a um país. Por isso, empresas de *e-commerce* devem ficar atenta às informações que trafegam nessas vias internacionais, como os dados transfronteiriços, que não passam pelas vias normais de fiscalização física. Segundo Baltzan e Phillips (2012), muitos países, como os que compõem a União Europeia, consideram a circulação de dados transfronteiriços uma violação da legislação de privacidade vigente para essa comunidade. Isso se dá, de acordo com a autora, porque muitas vezes esses dados sobre os usuários ultrapassam as fronteiras de um país sem haver garantias de privacidade rigorosas.

Na Figura 1, você pode ver as disposições de um acordo de confidencialidade de dados entre Estados Unidos e União Europeia. De acordo com Baltzan e Phillips (2012), o acordo isenta empresas dos Estados Unidos envolvidas em *e-business* internacional de sanções da União Europeia quanto à confidenciali-

dade de dados se as empresas participarem de um programa de autorregulação que oferece aos consumidores da União Europeia informações básicas sobre como seus dados pessoais são utilizados, além de controle sobre o processo.



Em relação ao armazenamento de dados pessoais dos clientes — ou mesmo de não clientes — no comércio eletrônico, de modo geral, a empresa tem a tecnologia como um facilitador que não apresenta limites próximos. São várias as formas e os subterfúgios para armazenar as informações dos usuários.

Com essas informações em mãos, a empresa pode criar ações e produtos personalizados para grupos semelhantes ou mesmo para indivíduos específicos, além de determinar padrões de consumo e antecipar cenários no desenvolvimento estratégico. Qualquer *e-commerce* vislumbra essa assertividade nas suas estratégias. Nesse contexto, a privacidade e a segurança dessas informações são como efeitos colaterais, que podem ter sérias consequências.



Link

Acesse, por meio do *link* a seguir, a reportagem “O que você não sabe sobre o uso de seus dados pelo Facebook”, que trata sobre o uso de dados de usuários por essa rede social.

<https://qrqo.page.link/SvQ1g>

Como você viu, o direito à privacidade sofre pressão social, exigindo a criação de normas que regulamentem e penalizem a exposição de dados pessoais. Além disso, há ainda a própria autorregulação do mercado, com os usuários evitando e expondo marcas com práticas não confiáveis.

Segundo Pinheiro (2016), no Brasil há uma grande confusão técnica a respeito do tema. Não há clareza e consenso, do ponto de vista técnico, sobre o uso de dados do cidadão brasileiro. Assim, é necessária a criação de uma lei específica para essas situações. Isso ajudaria a garantir mais segurança tanto para o cidadão quanto para o mercado.

Para que a empresa tenha o seu risco minimizado, é importante dar atenção a duas medidas básicas, descritas por Pinheiro (2016) como ações preventivas:

- Ter uma política de privacidade atualizada já com a nova Lei do Marco Civil da Internet, publicada em todos os canais digitais da empresa (portal, perfis e *fanpages* das mídias sociais, canal de aplicativos na Apple Store ou na Google Store), e requerer marcação de *check-box* com a concordância.
- Inserir cláusulas de privacidade e proteção de dados pessoais em contratos com pessoa física (relação de consumo) para deixar claros os tipos de uso, a possibilidade de guarda em terceiro autorizado (fornecedor), de uso de serviço de *cloud computing*, bem como a possibilidade de guarda, acesso e uso por outras empresas do mesmo grupo econômico, inclusive fora do Brasil.

Essas são medidas simples do ponto de vista técnico e que podem minimizar situações de risco para as empresas de comércio eletrônico.

Riscos de exposição de dados de usuários

A exposição dos dados de usuários na internet é um risco tanto para as empresas como para os próprios usuários. Ambos podem ser prejudicados: por um lado, empresas necessitam de maior investimento para evitar esse risco; por outro, consumidores ficam receosos de realizar compras pelo comércio eletrônico.

Para a empresa, além do investimento em segurança, o maior risco é o vazamento de dados. As consequências podem ser indenizações gigantescas, além do desgaste da marca. Nesse caso, o impacto pode até mesmo ser irreversível, já que uma empresa que venda via loja virtual precisa garantir a segurança da informação.

Segundo Limeira (2007), essa é:

[...] uma das barreiras para o internauta realizar compras na rede e divulgar seus dados pessoais, como RG, CPF e número do cartão de crédito, é a segurança na transmissão de dados. Essa preocupação por parte do usuário tem fundamento, uma vez que essas transmissões por meio de redes de comunicação, como é o caso da internet, muitas vezes são vítimas de falhas técnicas e humanas ou interceptadas por *hackers*, gerando grande transtorno aos usuários de serviços virtuais.

Stair e Reynolds (2015) afirmam que o crescimento do uso da internet apresenta riscos, como um eventual aumento de ações criminosas como as de *hackers* com o objetivo de obter acesso a informações confidenciais. Logo, as empresas precisam enfrentar a desconfiança do usuário em realizar transações no comércio eletrônico, o risco do vazamento de informações por falha humana ou de sistema e, por último, ações de *hackers* invadindo a sua base de dados e expondo falhas de segurança.

Ao invadir a base de dados de uma empresa, o *hacker* poderá usar os dados obtidos para benefício próprio, realizando compras, desviando recursos financeiros ou extorquindo usuários e empresas. Stair e Reynolds (2015) mostram alguns exemplos de violação de segurança, que causaram grandes prejuízos às empresas.

- Uma quebra de sigilo maciça na rede PlayStation, da Sony, comprometeu as informações pessoais de mais de 100 milhões de usuários.
- Alguns dos 24 milhões de clientes da Zappos.com, um *site* de sapatos e roupas na Web, foram informados que os dados das suas contas podiam ter sido acessados ilegalmente por partes não autorizadas.

- *Hackers* conseguiram acessar nomes, números de contas e informações de contato de 2 milhões de clientes do Citigroup.
- O site SEGA Pass, que apresenta informações sobre novos produtos para membros registrados da empresa de jogos SEGA, foi invadido por *hackers*. Nomes, datas de nascimento, endereços de e-mails e senhas criptografadas de 1,3 milhão de pessoas foram comprometidos.

Para além da ação de *hackers*, várias práticas via sistemas de informação envolvem o uso indevido de dados de empresas e de usuários. Audy, Andrade e Cidral (2007, p. 189) apresentam algumas delas. Veja-as a seguir.

- O *hacking* pode ser considerado a forma mais conhecida de invasão de privacidade no campo dos sistemas de informação, e consiste em invadir um sistema de informação para obter dados sem autorização. Em alguns casos, os *hackers* não apenas se apropriam de forma indevida de dados como propositalmente danificam o sistema. Em alguns círculos, faz-se a distinção entre *hackers* e *crackers*. A palavra *hackers* designaria os peritos na área de TI que podem se especializar em atividades relacionadas à segurança de sistemas de informação. A palavra *crackers* seria usada para designar *hackers* com más intenções e que efetivamente utilizam os seus conhecimentos para provocar danos em sistemas e se apropriar de forma ilícita de informações.
- O *jamming* consiste em bloquear o acesso a um sistema de informação por meio de rotinas de *software* específicas. Em situações de acesso via internet, os serviços oferecidos pelo sistema atacado não são disponibilizados, podendo causar danos que extrapolam o âmbito do fornecedor do serviço e atingem uma série de outras pessoas e organizações.
- O *sniffing* é uma forma de interceptar informações que trafegam por uma rede por meio de rotinas de *software* específicas. As informações capturadas podem ser usadas de maneira ilícita.
- O *spoofing* consiste em obter informações passando-se por outros. No âmbito da internet, podem ser construídos *sites* falsos, que enganam os usuários e obtêm dados de forma fraudulenta.
- O *spamming* é a prática de enviar e-mails para alguém sem que essa pessoa ou organização tenha autorizado. O *spam* pode ser empregado na oferta de produtos e serviços ou na divulgação de informações. Essa prática tem importunado pessoas e organizações na medida em que pode consumir recursos e causar transtornos para quem recebe esses e-mails.

- O vírus de computador consiste em um *software* que ataca sistemas com o intuito de danificar dados e *softwares* ou prejudicar a *performance* do processamento. Os vírus causam grandes transtornos a pessoas e empresas. Além dos prejuízos, o ataque por vírus tem exigido o investimento de recursos na sua prevenção. Isso é feito com a implementação de políticas de segurança e aquisição de *software* antivírus.

Como você pôde ver, são várias as práticas que podem trazer risco às empresas e aos usuários. Algumas delas devem ser evitadas pela empresa, outras pelo próprio usuário — que são as duas pontas nesse processo.

De um lado, quando um usuário que é cliente de um *e-commerce*, por exemplo, tem os seus dados pessoais e de compra roubados, é como se a sua “identidade” fosse roubada. A partir dessas informações da sua identificação, pessoas mal-intencionadas poderão realizar compras em outros *e-commerces* usando os seus dados pessoais e o seu número de cartão de crédito. Além disso, podem ainda solicitar empréstimos e realizar transferências bancárias.

Mesmo aplicativos (*apps*) de bancos para *smartphones*, tidos como de segurança elevada, estão sujeitos a esse tipo de crime. Por isso, não importa o tamanho do comércio eletrônico, a preocupação com o risco de vazamento ou roubo de informações dos usuários deve ser constante.

Ainda, vale lembrar que empresas podem ser processadas pela exposição de dados roubados dos seus clientes. Grandes corporações como a Zappos — empresa que pertence à gigante do comércio eletrônico Amazon — e o LinkedIn tiveram prejuízos com processos desse tipo. Recentemente, no Brasil, o Banco Inter, que é totalmente digital, também teve dados vazados e sofreu um processo de indenização por danos morais na ordem de R\$ 10 milhões. Além disso, o banco ainda foi vítima de extorsão feita por *hacker*, com ameaça de exposição de dados pessoais, fotos de cheques, transações e senhas de quase 100 mil clientes.

Entretanto, existe um risco que não é financeiro — ou não está diretamente ligado ao investimento com segurança ou despesas com indenizações. É o risco da perda de credibilidade, ou seja, da falta de confiança dos clientes. Esse é um limitador no desenvolvimento do comércio eletrônico, impedindo o aumento nas vendas de lojas de *e-commerce*.

Stair e Reynolds (2015, p. 368) relatam que “[...] com frequência, a falta de confiança nos vendedores *on-line* é uma das razões mais citadas pelos clientes para não desejarem comprar *on-line*”. Assim, empresas de comércio eletrônico precisam investir em procedimentos e tecnologias para minimizar os constantes riscos de exposição de dados dos usuários pela internet.

Uso de redes domésticas e públicas

O comércio eletrônico é baseado na comunicação entre computadores ligados em rede, que pode ser do tipo doméstica ou pública. Os usuários dependem dessa conexão em rede para realizar compras e interagir com a empresa.

Segundo Baltzan e Phillips (2012, p. 180), “[...] uma rede é um sistema de comunicações, de troca de dados e de partilha de recursos criada pela ligação de dois ou mais computadores e com o estabelecimento de normas ou protocolos, de modo que eles possam trabalhar juntos”. As redes são o elo entre empresas de comércio eletrônico, fornecedores, transportadoras, clientes, bancos, enfim, todos os agentes envolvidos no processo de transação eletrônica.

Lojas físicas já usam redes há muito tempo nas suas ligações e trocas de dados com bancos, fornecedores, filiais, mas com o surgimento de lojas híbridas e as exclusivamente virtuais, o uso dos sistemas de comunicação aumentou. Assim, o *e-commerce* adotou esses padrões inclusive para a comunicação com os seus clientes, as compras e o acompanhamento dos pedidos. Os modelos mais adotados pelas empresas de *e-business* são *virtual private network* (VPN) e *value added network* (VAN).

Pinheiro (2016, p. 611) define VPN como o “[...] termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura”. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Para Dantas (2016, documento *on-line*), VAN seria o seguinte:

[...] uma central de comunicação que recebe pedidos de compras e os distribui para as organizações em tempo e formato apropriados. Ela pode fornecer outros serviços similares e é também conhecida como uma rede terceirizada. A VAN no Brasil é muito usada por varejistas e grandes empresas de serviços que usam essas VANs para receberem dos bancos, adquirentes, *gateways* e sistemas de processamento, arquivos com dados de pagamento e cobrança. Ela faz justamente o intercâmbio com agentes financeiros.

Segundo Baltzan e Phillips (2012, p. 184), os “[...] *e-business* confiam amplamente em VPNs, VANs, e outros *links* dedicados que lidam com as transações de intercâmbio de dados eletrônicos”. No entanto, ainda de acordo com os autores, essas tecnologias apresentam desafios significativos. Veja-os a seguir.

- Ao lidar apenas com tipos limitados de informações de negócios, elas pouco contribuem para uma estrutura de relatórios destinada a proporcionar uma visão abrangente das operações comerciais.
- Elas oferecem pouco suporte à integração em tempo real dos processos de negócios que serão essenciais no mercado digital.
- Relativamente caras e de implementação complexa, as tecnologias convencionais dificultam a expansão ou alteração das redes como reação às mudanças do mercado.

Stair e Reynolds (2015) afirmam que as redes domésticas, usadas em muitas casas e em pequenos negócios, servem para compartilhar acesso a internet, impressora e troca de arquivos. Ainda, podem ser incluídos nessas redes, além de computadores, consoles de *videogames*, *smartphones*, câmeras fotográficas e vários outros dispositivos eletrônicos com conexão em rede. Esse tipo de rede tem um *firewall* que filtra as informações que chegam da internet para a rede.

Baltzan e Phillips (2012, p. 181) mostram que “[...] uma rede de área local (LAN, *Local Area Network*) é projetada para conectar um grupo de computadores próximos, como em um prédio comercial, uma escola ou uma casa. Ela é útil para compartilhar recursos, como arquivos, impressoras, jogos ou outros aplicativos”.

Tanto as redes públicas como as domésticas, independentemente do porte, exigem atenção à segurança. Um erro comum para pequenos empreendedores do comércio eletrônico — que também é cometido por usuários — é o uso de redes domésticas sem o devido cuidado, acreditando que, por estar em casa, por exemplo, a segurança está garantida.

Muitos desses usuários, ao adquirirem um roteador de acesso, adotam a configuração de fábrica, comum a todos os usuários. Portanto, é fundamental contratar o serviço de um profissional para garantir a correta parametrização de segurança do seu equipamento.

Os microempreendedores também devem ter esse cuidado, por menor que seja o seu negócio, priorizando a segurança. Alguns desses empreendedores acabam realizando transações em Wi-Fi gratuito, que é outro erro comum. Na próxima seção, você verá quais são os riscos dessa prática.

Redes públicas com Wi-Fi grátis

A proposta de utilizar Wi-Fi de forma gratuita parece tentadora, mas quanto maior a praticidade desse modelo de rede, provavelmente menor será a sua segurança.

Segundo Baltzan e Phillips (2012, p. 199):

[...] o *wireless fidelity* (WiFi) é um meio de ligação entre computadores por sinais infravermelhos ou de rádio. O Wi-Fi, ou o que é por vezes referido como LANs sem fio, representa apenas uma pequena proporção de LANs em operação hoje, mas que cresce rapidamente. A tecnologia Wi-Fi tem vantagens óbvias para as pessoas em movimento que necessitam de acesso à internet.

As pessoas estão cada vez mais dependentes de dispositivos com acesso à internet. Quando estão em casa ou no trabalho, há uma segurança maior, uma vez que se trata de uma rede doméstica na qual provavelmente haverá um roteador com proteção criptografada. Porém, quando está fora dessa rede doméstica e inicia o acesso em uma rede pública, normalmente com o *smartphone*, o usuário pode estar acessando uma rede sem a proteção necessária.

Usuários podem se conectar a redes gratuitas para realizar transações de *m-commerce*, acessar as redes sociais e mesmo para trabalhar ou estudar. Segundo o *site* Kapersky (um antivírus de origem russa) (COMO..., [2019], documento *on-line*):

[...] os mesmos recursos que tornam os pontos de acesso de Wi-Fi gratuito ótimos para os clientes também são atraentes para os *hackers*, pois não há necessidade de autenticação para estabelecer uma conexão de rede. Isso cria uma ótima oportunidade para que um *hacker* obtenha acesso ilimitado a dispositivos desprotegidos na mesma rede. A maior ameaça à segurança do Wi-Fi gratuito é a capacidade de um *hacker* posicionar-se entre você e o ponto de conexão. Então, em vez de falar diretamente com o ponto de acesso, você está enviando suas informações para o *hacker*, que pode retransmiti-las.

Assim, ao saberem desse risco, empresas de comércio eletrônico e usuários devem se adiantar e criar procedimentos de segurança para evitar surpresas desagradáveis.



Referências

AUDY, J. L. N.; ANDRADE, G. K.; CIDRAL, A. *Fundamentos de sistemas de informação*. Porto Alegre: Bookman, 2007. E-book.

BALTZAN, P.; PHILLIPS, A. *Sistemas de informação*. Porto Alegre: AMGH, 2012. E-book.

COMO evitar riscos à segurança em redes Wi-Fi públicas. Kaspersky Lab, [s. /], [2019]. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi-risks>. Acesso em: 14 maio 2019.

DANTAS, R. O que é uma VAN? *Vindi*, São Paulo, 20 jan. 2016. Disponível em: <https://blog.vindi.com.br/o-que-e-uma-van/>. Acesso em: 14 maio 2019.

LIMEIRA, T. M. V. *E-marketing*. 2. ed. São Paulo: Saraiva, 2007.

PAESANI, L. M. *Direito e internet: liberdade de informação, privacidade e responsabilidade civil*. 7. ed. São Paulo: Atlas, 2014.

PINHEIRO, P. P. *Direito digital*. 6. ed. São Paulo: Saraiva, 2016.

STAIR, R. M.; REYNOLDS, G. W. *Princípios de sistemas de informação*. São Paulo: Cengage Learning, 2015.

TURCHI, S. R. *Estratégias de marketing digital e e-commerce*. 2. ed. São Paulo: Atlas, 2019.

Proteção de dados pessoais

Objetivos de aprendizagem

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

- Caracterizar a sociedade da informação.
- Identificar os mecanismos de sigilo e privacidade de dados pessoais.
- Analisar o protagonismo do consentimento.

Introdução

Antes mesmo do surgimento da internet, já havia um consenso corporativo: a informação poderia maximizar o desenvolvimento de uma organização, ampliando os seus resultados econômicos. O taylorismo foi uma das teorias da administração que buscou estudar o processo de produção e, com isso, identificar de que maneira os operários ou as máquinas poderiam ser ainda mais produtivos. Isso comprova que a informação é considerada estratégica para as organizações ao menos desde a sociedade industrial (século XIX).

Por sua vez, o direito do indivíduo é discutido e legislado desde a Antiguidade Clássica. Com o passar do tempo, as sociedades foram se moldando às necessidades e amadurecendo os seus dispositivos de controle. Atualmente, existem algumas legislações relativas à proteção de dados. Apesar de recentes, tais legislações já estão sofrendo alterações. Isso ocorre porque as leis não conseguem acompanhar a velocidade das mudanças tecnológicas e informacionais. Portanto, antes de tudo, é necessário estabelecer premissas básicas, como o direito universal do indivíduo à sua liberdade. Com base em pilares como esse, é possível definir uma legislação adequada.

Neste capítulo, você vai ler sobre a proteção de dados pessoais. Primeiramente, você vai estudar algumas características da sociedade contemporânea, também chamada de “sociedade da informação”. Em seguida, você vai conferir alguns mecanismos de sigilo e privacidade de dados pessoais. Por fim, vai conhecer a legislação a respeito da

proteção dos dados do cidadão, com foco na legislação brasileira, que avançou para se adaptar às normas internacionais, mas também para se alinhar a questões fundamentalmente nacionais.

1 Características da sociedade da informação

Para tratar das características da sociedade da informação, é necessário voltar um pouco no tempo. Como afirma Bioni (2019), a sociedade foi se modificando ao longo da sua história, e a cada mudança estrutural surgiram certos marcos. Considere, por exemplo, a sociedade agrícola: nela, a fonte da riqueza era a terra, e as transações entre as pessoas ocorriam com base nos produtos cultivados, seja por meio de escambos ou, posteriormente, da utilização da moeda em mercados.

Com o passar do tempo, a sociedade se tornou industrial, devido ao surgimento e à utilização em escala da máquina a vapor e da eletricidade. Após a Segunda Guerra Mundial, a sociedade passou por um novo remanejo econômico, dando início à fase pós-industrial, com o surgimento das prestações de serviços. Assim, além da capacidade industrial de produzir, passou a ganhar destaque a forma como serviços (assistência médica, setor bancário, educação, etc.) geravam e movimentavam riquezas.

No entanto, a sociedade mais uma vez deu um passo à frente e, a partir da evolução da tecnologia, em especial da internet, foram criados mecanismos capazes de processar e transmitir dados em quantidade e velocidade nunca antes atingidas. A partir daí, as barreiras físicas ficam de lado, e surgem diversas formas de transacionar e de interagir, como as populares redes sociais (Facebook, Instagram, etc.). Para designar a sociedade configurada a partir dessas mudanças, passou-se a utilizar a expressão “sociedade da informação”. As principais sociedades que se estabeleceram do século XVIII até o XXI (BIONI, 2019) foram:

- sociedade agrícola (século XVIII);
- sociedade industrial (século XIX);
- sociedade pós-industrial (século XX);
- sociedade da informação (século XXI).

A informação, conforme Bioni (2019), tem o mesmo peso que já tiveram o uso agrícola da terra, a máquina a vapor, a eletricidade e os serviços. Tenha em mente que a importância da informação na sociedade atual não se restringe ao ambiente virtual. Hoje, a informação é um recurso que impacta diretamente os setores de serviço, comércio e indústria, isto é, a própria economia, transformando o sistema de produção e gerando, por efeito colateral, diversos impactos para o cidadão, sejam eles positivos ou negativos. A ciência jurídica busca mapear esses impactos e, partir dessa análise, criar leis para regulamentar as formas de transação nesse ambiente cada vez mais complexo marcado pelo protagonismo da informação nas relações sociais.

A economia da informação cresceu, ganhou escala e potencial graças aos alicerces nos quais ela está ancorada. Afinal, diferentemente de produtos agrícolas ou industriais, a informação produzida na contemporaneidade não exige meios tangíveis (como terras, estradas ou livros) para ser armazenada e transmitida. Boa parte da infraestrutura da economia da informação é abstrata ou virtual. Naturalmente, lidar com informações também requer o uso de servidores, prédios, etc., porém a proporção de meios físicos exigidos é muito menor se você comparar a sociedade da informação com a sociedade industrial, por exemplo.

A economia da informação, quando bem estruturada e organizada, oferece um tempo de resposta praticamente instantâneo. Por exemplo, se você for procurar um livro em uma estante, apesar de toda a organização das bibliotecas, você dispende algum tempo. Porém, ao fazer a mesma busca utilizando um computador com acesso à internet, você chegará ao mesmo livro em apenas alguns segundos. Esse ganho de velocidade exponencial fez com que o potencial humano fosse utilizado como jamais antes na história da humanidade.

Com base na forma como as pessoas criam e utilizam a tecnologia, foi possível comprimir a informação de maneira quantitativa e qualitativa. Isso, aliado à internet e à virtualização dos dados, provocou a passagem do modelo industrial fordista de produção para o modelo atual. A transição dos modelos industrial e pós-industrial para a sociedade da informação alterou justamente a forma como os dados circulam: se antes eles eram centralizados e verticais, no modelo em rede passaram a ser descentralizados e horizontais. Ademais, entraram em cena dinâmicas mais colaborativas e sem fronteiras de lidar com as informações.



Exemplo

Desde 2015, a empresa italiana de moda Benetton processa basicamente um conjunto de informações, buscando se antecipar às tendências do mercado consumidor. Com base nessa massa de dados, ela envia as diretrizes para as suas fábricas (que estão em vários países). Então, as novas coleções são produzidas e posteriormente distribuídas para lojas da marca ou de parceiros no mundo todo.

Atualmente, diversas empresas trabalham em um formato de rede. Esse formato de trabalho só é possível devido à evolução tecnológica. Por meio dela, a sociedade da informação supera em escala, produtividade e ganhos os demais tipos de sociedades antes vigentes (BIONI, 2019). Porém, é importante você atentar à importância da inteligência dos dados. Isto é, um conjunto de dados agrupados não gera resultados por si só; é necessário tratar, processar e organizar os dados, buscando transformá-los em informação e, posteriormente, em conhecimento. Esse conhecimento, por sua vez, deve ser aplicado, gerando o resultado esperado inicialmente.

Por isso, os dados são a matéria-prima da economia da sociedade da informação. Se os dados são tão valiosos, como é possível obtê-los? Isso passa obrigatoriamente pela coleta e pelo tratamento dos dados dos cidadãos, atividades que representam uma nova forma de capital: menos tangível, porém com grande potencial de gerar riqueza. Considere o seguinte:

Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (*marketing*) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.

E com a possibilidade de organizar tais dados de maneira mais escalável (e. g. *Big Data*), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma “economia de vigilância” que tende a posicionar o cidadão como um mero espectador das suas informações (BIONI, 2019, p. 9).

Bioni (2019) ainda aponta que a publicidade foi a ciência mercadológica que mais evoluiu na sociedade da informação, buscando adaptar as estratégias *off-line*, como a publicidade contextual e segmentada, ao novo mercado que surgia. Nesse contexto, a estratégia é mapear o comportamento do usuário a partir de uma série de dados, o que é feito a partir de ferramentas de mercado,

por exemplo, o Google Ads e as redes sociais. Estas últimas ganharam ainda mais força devido ao tempo de uso dos usuários, que passam diversas horas do dia conectados. Durante esse período de conexão, eles fornecem uma gama imensa de informações pessoais, que funcionam como uma engrenagem extremamente importante desse novo tipo de economia digital.

Porém, vale reforçar que a internet possibilitou muito mais do que o desenvolvimento de hábitos de navegação dos usuários. Em paralelo a isso, surgiu a tecnologia móvel, a partir dos celulares, o que possibilitou o avanço ainda maior das ações publicitárias. O fácil acesso à internet nos dias de hoje permitiu um passo além, que é o monitoramento da localização geográfica do usuário a partir de satélites por GPS (Global Positioning System — sistema de posicionamento global). O monitoramento de navegação, alinhado ao controle por geolocalização, elevou a estratégia mercadológica a um patamar inédito.



Saiba mais

Esse novo cenário criou um tipo de serviço que por vezes acaba passando despercebido, pois parece gratuito, já que não implica desembolso financeiro. Esse tipo de serviço é chamado de “freemium”. Basicamente, trata-se de uma relação transacional bilateral: para utilizar o serviço, o usuário acaba fornecendo os seus dados, sejam eles pessoais ou comportamentais. Um exemplo é o Facebook, que monitora todas as suas curtidas, compartilhamentos e comportamentos, seja por *status* ou *emojicons*. Posteriormente, ele utiliza esses dados para mapear o seu perfil e, com isso, entender qual é o produto ou serviço que mais se adapta aos seus desejos.

2 Mecanismos de sigilo e privacidade de dados pessoais

Os direitos individuais, conforme Bioni (2019), já constavam nas leis gregas e romanas, sendo os pilares que ajudaram a moldar a sociedade até os dias de hoje. Tais direitos foram sendo adaptados e aperfeiçoados com o passar do tempo. Por exemplo, após a Segunda Guerra Mundial, o princípio da dignidade humana passou a fazer parte de diversas constituições. Além disso, nesse período foi elaborada a Declaração Universal dos Direitos Humanos, da Organização das Nações Unidas (ONU).

Mais recentemente, a proteção dos dados pessoais passou a ser o novo direito da personalidade do cidadão. Nesse contexto, são consideradas duas perspectivas:

- a) a percepção da personalidade enquanto um atributo, prolongamento ou projeção da própria individualidade da pessoa humana;
- b) a percepção de que o ser humano é, por excelência, um ser social, devendo-se assegurar a ele a sua esfera relacional.

Assim, os dados pessoais ganharam uma categoria jurídica. A função dos direitos da personalidade é promover e assegurar o valor das pessoas e demais cláusulas de proteção. Esse paradigma sofre alterações decorrentes dos avanços das novas tecnologias, o que acrescenta novos desafios à questão.

A personalidade consiste em um conjunto de características que diferencia uma pessoa da outra. Esse conjunto de características não diz respeito apenas ao indivíduo físico, mas engloba seus dados pessoais e de cidadania (nome, CPF, RG, endereço, etc.). Isso acaba por justificar esse espectro jurídico que se estende para além da pessoa propriamente dita.

Uma das formas de antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele em que não existe “nome nem rosto”. A **anonimização** envolve diversas técnicas. A seguir, veja as principais.

- **Supressão:** por exemplo, a supressão do CPF, que pode ser capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único. Logo, a sua disponibilização, ainda que parcial (cinco primeiros dígitos), não seria prudente.
- **Generalização:** com a generalização da localização geográfica, por exemplo, em vez de se disponibilizar o número completo do CEP, se divulgaria apenas os primeiros dígitos. Assim, haveria uma localização menos detalhada, a fim de quebrar o vínculo de identificação entre a informação e determinado sujeito.
- **Randomização:** faz referência a uma “desordem” controlada de informações. Por exemplo, em uma folha de pagamento, os dados referentes ao nome e ao CPF estariam misturados, o que não permitiria a associação do salário com o sujeito titular da informação.
- **Pseudonimização:** é semelhante à solução randômica, porém estão em jogo dados anonimizados com nomes não existentes na base vigente ou

dados em maior aleatoriedade, principalmente em relação ao nome e ao sobrenome. Por vezes, a pseudonimização acaba sendo mais trabalhosa, devido à maior inteligência necessária para trabalhar com os dados.

Essas técnicas estão sendo cada vez mais utilizadas pelas empresas brasileiras que desejam se adequar à Lei nº. 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). Elas podem ser usadas separadamente, mas também em conjunto. Vale reforçar que a implementação dessas engenharias de controle de informação ainda está amadurecendo, ou seja, nenhuma das técnicas garante com 100% de certeza que as bases não serão estratificadas e que, a partir de uma reengenharia, não será possível obter os dados originais.

A própria LGPD, no seu art. 12, apresenta o conceito da razoabilidade no tratamento da anonimização dos dados do indivíduo (BRASIL, 2018):

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

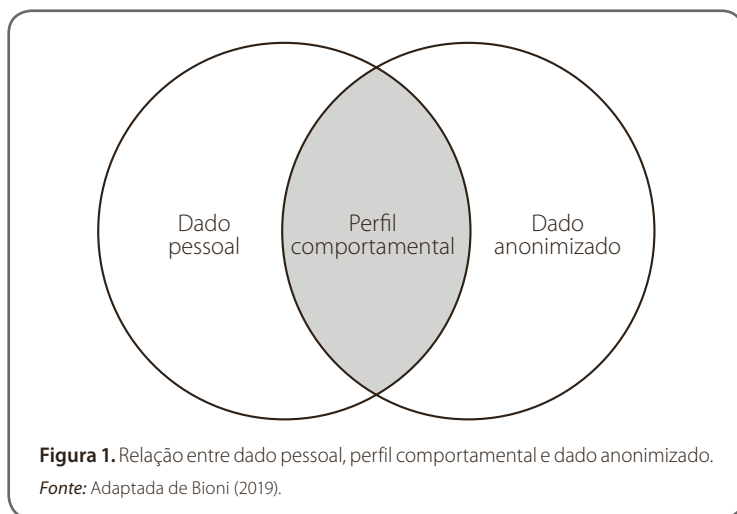
I — A determinação de que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

II — Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

III — A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Isso acaba sendo uma estratégia normativa, alinhada à premissa de que todo dado é passível de reversão. Assim, há um risco aceitável e tolerável relativo à reversibilidade do processo de anonimização, porém isso não justifica a falta de cuidado e dos demais tratamentos necessários da informação (BIONI, 2019).

Até aqui, você leu a respeito dos dados pessoais e dos dados anonimizados. Todavia, existe uma “zona cinza” que consiste justamente na junção das duas categorias: o perfil comportamental. É exatamente nessa região que as empresas buscam operar dentro dos limites da lei. Para compreender melhor, observe a Figura 1, a seguir.



Como destaca Bioni (2019), as empresas por vezes controlam o histórico de navegação dos usuários, porém não necessariamente conseguem saber se determinado usuário é ele mesmo. Isto é: elas monitoram o endereço IP (Internet Protocol — protocolo de internet) do computador. Pelo controle constante e repetitivo, essas empresas conseguem identificar o perfil comportamental daquele equipamento e, por consequência, têm uma razoável certeza do perfil do titular que o utiliza, seja para trabalho, estudo ou interesses pessoais. Logo, a publicidade comportamental busca, a partir das características mapeadas nessa zona cinza, identificar de forma mais assertiva os desejos do usuário e, com isso, apresentar bens e serviços que ele se interesse em consumir e utilizar.

Por sua vez, os dados sensíveis são um subgrupo de dados pessoais. Eles compreendem um conteúdo que pode oferecer uma especial vulnerabilidade discriminatória. São itens que podem conter informações a respeito da personalidade sexual, religiosa, política, racial, bem como informações sobre estado de saúde e filiação sindical. Assim, a preocupação é que possa haver alguma discriminação de uma pessoa justamente devido a aspectos da sua personalidade.

Portanto, há cuidados necessários no emprego do *big data*, que, justamente pelo seu potencial de correlacionamento, pode identificar uma série de dados que mapeiam comportamentos e acontecimentos. Nesse contexto, a partir de dados triviais, é possível chegar a conclusões a respeito dos dados sensíveis do cidadão. Decorre disso tudo a importância de haver uma legislação relativa

à proteção de dados que tenha como espinha dorsal a preservação da individualidade das pessoas, impedindo ações discriminatórias e apropriação não autorizada de dados.

3 Protagonismo do consentimento

Após a Segunda Guerra Mundial, conforme Bioni (2019), a máquina administrativa pública passou a identificar o potencial do uso das informações pessoais dos seus cidadãos. Afinal, tais dados permitem organizar e planejar ações, possibilitando o crescimento sustentável das economias nacionais. A tecnologia viabilizou os intuítos do Estado. Isto é, a ciência computacional tornou processáveis tais informações quantitativas e qualitativas obtidas a partir dos dados pessoais, elevando o nível da tomada de decisão dos governantes.

Em paralelo a isso, surgiu a primeira geração de leis de proteção de dados, justamente devido ao cuidado necessário no uso massivo de tais informações. Porém, no cenário existente então, o foco acabou recaindo sobre a própria tecnologia, que deveria seguir valores democráticos; ou seja, todo e qualquer de banco de dados para esse tipo de transação precisaria de uma concessão do Estado para funcionar. Portanto, essa primeira geração de leis teve como foco o esforço governamental e a viabilidade técnica do controle. A ideia era monitorar quando e como seriam criados bancos de dados. No entanto, esse cenário rapidamente rompeu a esfera governamental, sendo necessária uma nova estrutura normativa.

A segunda geração de leis de proteção de dados pessoais é caracterizada por uma mudança mais profunda no entendimento da regulação. Essa geração não contempla somente a área pública, mas também a área privada. Isso decorre justamente do avanço da área privada no uso da tecnologia, que aconteceu mais rapidamente do que o avanço da esfera pública.

Além da iniciativa privada e do Estado, o titular também é responsável por proteger os seus dados, não é? Assim, a terceira geração de leis dá mais protagonismo ao cidadão na hora de ele consentir com a entrega dos seus dados pessoais; a ideia é que o indivíduo saiba como ocorrem a coleta e o compartilhamento dos seus dados. Justamente por esse consentimento, o titular se tornou o vetor principal das legislações a respeito da proteção de dados. Porém, isso gerou diversos complicadores na aplicabilidade dessas premissas, de modo que surgiu a quarta geração de leis, que buscou preencher a lacuna deixada pelas gerações anteriores.

Nessa geração, o protagonismo do consentimento permanece, bem como a noção de que os dados registram as características da pessoa. A grande mudança é o maior esclarecimento a respeito da aplicabilidade da lei. O Regulamento Geral sobre a Proteção de Dados (RGPD), da comunidade europeia, por exemplo, elencou as premissas e diretivas a serem seguidas pelos Estados-membros, bem como as restrições que os demais países deveriam seguir para o fechamento de acordos comerciais com a União Europeia.

Considere também a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), organismo internacional e multilateral criado logo após a Segunda Guerra Mundial (1948) e que tem por missão promover o bem-estar econômico e social global. A OCDE teve uma participação importante no redimensionamento do papel da tecnologia da informação na sociedade como um todo. Ela criou diversos guias com padrões normativos para a proteção de dados, tendo em vista que o comércio é cada vez mais global e que as fronteiras digitais necessitam de maior controle e monitoramento.

No Brasil, a legislação também foi amadurecendo e se adaptando ao novo cenário, buscando não somente aderir às boas práticas internacionais, mas também aprimorar os relacionamentos comerciais vigentes. Nesse contexto, destaca-se, naturalmente, a proteção dos dados individuais, como você vai ver a seguir.

Código de Defesa do Consumidor

O Código de Defesa do Consumidor (Lei nº. 8.078, de 11 de setembro de 1990) disciplina, em seu art. 43, os bancos de dados e cadastros de consumidores (BRASIL, 1990). Note a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito.

A lei buscou alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor. O consumidor deve ser notificado a respeito da abertura de um banco de dados pessoais não solicitado por ele. Esse dever de comunicação prévia permite que o consumidor acompanhe o fluxo de seus dados pessoais, já que tal atividade deve ser comunicada a ele e, em última análise, ser transparente. Isso possibilita ao consumidor acompanhar de forma dinâmica a circulação de suas informações pessoais.

Lei do Cadastro Positivo

A Lei do Cadastro Positivo (Lei nº. 12.414, de 9 de junho de 2011) disciplina a formação de banco de dados sob um conjunto de dados relativos às operações financeiras e de adimplemento para fins de concessão de crédito (BRASIL, 2011). Com isso, a situação econômica do postulante ao crédito não é mais somente analisada a partir de dados relativos a dívidas não pagas, mas também a partir de outras informações que possam exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento. Por isso, tal legislação foi apelidada de “Cadastro Positivo”, já que a avaliação do crédito terá uma amplitude maior do que o exame de informações a respeito de dívidas inadimplidas, cuja conotação seria negativa.

LGPD

A LGPD foi debatida por quase 10 anos. É possível coletar registros de debates públicos sobre o tema. A parte referente ao consentimento seguiu as premissas da legislação europeia e também da quarta geração de leis de proteção dos dados pessoais. O consentimento deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral; em alguns casos, deve ser ainda específico.

Isso ocorre pois grande parte dos princípios da lei são gravitacionais no indivíduo, e devem existir preceitos como a transparência e o propósito na forma como o dado será coletado, tratado, armazenado e utilizado. Após o titular ter ciência de como os seus dados serão usados, ele pode decidir se dá ou não o consentimento. Vale reforçar que esse consentimento precisa seguir algumas diretrizes, como as listadas a seguir.

- O consentimento deve ser extraído por meio de cláusulas contratuais destacadas.
- As autorizações genéricas (sem uma finalidade determinada) são nulas.
- Nas hipóteses em que não há consentimento, deve-se observar os direitos e princípios da LGPD, de modo que haja a possibilidade de o titular dos dados pessoais se opor ao tratamento de seus dados.

Na LGPD, a palavra “consentimento” aparece um pouco mais do que três dezenas de vezes, porém vale reforçar que isso não se trata apenas de uma análise quantitativa, mas também qualitativa: o consentimento é a espinha dorsal dessa lei.



Fique atento

Estava tudo pronto para a LGPD entrar em vigor em agosto de 2020. Enquanto se esperava a criação da Autoridade Nacional de Proteção de Dados, foi editado um Projeto de Lei para adiar o início da vigência da LGPD e, no fim de abril de 2020, foi publicada a Medida Provisória (MP) 959, adiando o início da vigência da LGPD para maio de 2021. Isso quer dizer que a LGPD entrará em vigor apenas em maio de 2021? Não! A LGPD entrará em vigor em maio de 2021 somente se essa MP for aprovada pela Câmara e pelo Senado no prazo de 120 dias. Caso a MP 959 não seja votada e aprovada pelas duas casas dentro desse prazo, volta a valer o início da vigência original — agosto de 2020.



Referências

BIONI, B. R. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2019. 328 p.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Casa Civil da Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 3 maio 2020.

BRASIL. *Lei nº 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Casa Civil da Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 3 maio 2020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Casa Civil da Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 3 maio 2020.

Leituras recomendadas

ALENCAR, O. *Projeto de Lei nº 1027, de 2020*. Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais - LGPD - para 16 de fevereiro de 2022. Brasília: Senado Federal, 2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141225>. Acesso em: 3 maio 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. 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: 3 maio 2020.

BRASIL. *Lei nº. 13.853, de 8 de julho de 2019*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília: Casa Civil da Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 3 maio 2020.

BRASIL. *Medida Provisória nº. 959, de 29 de abril de 2020*. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Brasília: Casa Civil da Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm. Acesso em: 3 maio 2020.

O QUE MUDA com a nova lei de dados pessoais. *LGPD Brasil*, São Paulo, ago. 2018. Disponível em <https://www.lgpdbrasil.com.br/o-que-muda-com-a-lei>. Acesso em: 3 maio 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*.

Questões legais do E-business

Objetivos de aprendizagem

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

- Identificar implicações de questões legais e éticas no comércio eletrônico.
- Diferenciar os principais tipos de crimes virtuais.
- Reconhecer as características básicas do marco civil da internet e seu impacto sobre os usuários.

Introdução

As relações de compras entre consumidores e fornecedores passam por várias fases. No meio físico, normalmente o consumidor pesquisa, entra de estabelecimento em estabelecimento, compara produto e atendimento, encontra o produto ou serviço que atende a sua necessidade, negocia e adquire o produto, podendo, até mesmo, tocar no produto, abrir e em alguns casos o experimentar.

Esse tipo de relacionamento sempre existirá e não é excludente da nova forma de relacionamento entre cliente e fornecedor, que hoje chamamos de comércio eletrônico, também conhecido por e-commerce. Outra denominação que está presente atualmente para esse termo é o e-business “negócio eletrônico”, que também promove o comércio eletrônico entre fornecedores e empresa, mas engloba as negociações da empresa na internet não sendo necessariamente comercial, essa é a diferença básica dos dois termos.

Dessa forma, tanto o e-commerce como o e-business são alvos de tentativas de golpes e crimes virtuais, os quais precisam ser conhecidos, combatidos e punidos. Neste texto, você irá conhecer algumas questões éticas e legais e os instrumentos que podemos utilizar para minimizar os impactos negativos desses crimes.

Comércio eletrônico

Para definirmos comércio eletrônico, precisamos unir o comércio tradicional às ferramentas da tecnologia da informação (TI), dessa união teremos processos mais rápidos com aplicações inovadoras e revolucionárias para o atingimento das metas e objetivos empresariais. O comércio eletrônico está presente em todos os ramos da economia, atuando fortemente para melhorar as relações entre os consumidores e fornecedores de bens e serviços.

A evolução do termo modernizou essas relações em um caminho sem volta. Cerca de 40 anos (décadas de 1970-1980) atrás tínhamos casos de que um consumidor fazia uma lista de compras, se deslocava até um estabelecimento comercial chamado de “venda”, comprava os itens que necessitava, anotava esses itens em um caderno de compras chamado de “livreta” durante todo o mês, no mês seguinte ele voltava, pagava as compras anteriores e repetia a ação. Hoje, um consumidor em casa pode adquirir os produtos que atendam a sua necessidade e os receber em casa, efetuando o pedido e o pagamento eletronicamente. As empresas, então, podem realizar seus negócios e suas comercializações pela rede de computadores. Ganhou-se o tempo, agilidade e confiança nos processos.

Não há mais como ficar sem utilizar os recursos da TI para a integração dos mercados, a TI proporciona para as pessoas e, principalmente, para as empresas as melhores formas de se adaptarem, sobreviverem e obterem vantagens nesta nova realidade econômica.



Figura 1. Comércio eletrônico.

Fonte: FecomercioSP (2016).

O mercado eletrônico que se formou, é o responsável pela coordenação do fluxo de materiais e serviços entre os fornecedores e os consumidores, ou seja, atua na oferta e demanda dos mais variados itens ofertados e demandados, além das transações resultantes dessas interações.

Tem em si as facilidades de ser onipresente, facilidade de acesso à informação e baixos custos de transações. Veja no Quadro 1 as principais características desse mercado.

Quadro 1. Características do mercado eletrônico.

Redução de custos	Os custos podem ser reduzidos no caso dos fornecedores no que tange a distribuição e oferta massificada de seus produtos ou serviços; e no caso dos consumidores podem ser reduzidos, por exemplo, pela obtenção de informações sobre fornecedores e produtos alternativos, buscando uma melhor concorrência entre os ofertantes das mercadorias.
Melhor concorrência na oferta	O mercado eletrônico fica mais atraente com a entrada de novos fornecedores, com isso, quanto maior for a base de consulta, melhor será para os consumidores adquirirem produtos que atendam as suas necessidades.
Inovação constante	O mercado eletrônico requer inovação constante aos seus participantes, principalmente buscando formas de processamento com menores custos operacionais.
Investimento	Essa forma de mercado requer um bom investimento para ser implantado e processado, com isso o retorno virá pelas economias de escala e escopo.
Ponderações sobre incertezas	As incertezas sobre os benefícios sempre irão existir se os mesmos não puderem ser mensurados. As organizações terão que constantemente avaliar a participação no mercado de uma forma quantitativa e qualitativa.
Meios de pagamentos eletrônicos	As inovações realizadas nos meios de pagamento on-line permitiram a evolução e o crescimento das transações comerciais, servindo de base para todo o comércio eletrônico, facilitando, por exemplo, para os clientes que podem pagar contas na rede, por intermédio de um serviço on-line de pagamentos e realizar todos os pagamentos por um único site.

Assim sendo, os mercados eletrônicos vieram para não mais voltar, estão presentes em nosso dia a dia, tanto em nossas relações pessoais de interação

eletrônica como nas relações das empresas com outras empresas ou com seus consumidores. Eles promovem a coordenação dessas atividades negociais pelas formas de mecanismos de mercado, pela real globalização das informações e pela simplicidade na oferta aos usuários.

Entre benefícios desse tipo de comércio podemos citar:

- promoção de produtos, feita por meio de um contato direto e interativo;
- novo canal de vendas, podendo ser utilizado como forma alternativa para demonstração dos produtos ofertados pela organização, pois tem uma ligação direta e rápida com os potenciais consumidores;
- economia direta, pois tem redução significativa de custos por utilizar processos compartilhados com informação e integração eletrônica;
- redução do tempo de comercialização, como ele aproxima o consumidor do produto, acaba por eliminar algumas etapas do processo, por exemplo, um consumidor pode pesquisar o produto em casa, ver imagens desse produto, tomar a decisão de compra e até mesmo já efetuar a compra, ou ir a uma loja física para concretizar a compra;
- novas oportunidades de negócios, pois viabiliza negócios antes não sonhados pelas organizações, como uma empresa que tem lojas físicas em um número pequeno de municípios, com o comércio eletrônico oferta seus produtos a um número bem maior de municípios.



Saiba mais

Cyberspace: o **ciberespaço** é o ambiente criado de forma virtual por meio do uso dos meios de comunicação modernos, destacando-se, entre eles, a internet. Esse ambiente tornou-se possível em razão de uma grande infraestrutura técnica na área de telecomunicação composta por cabos, fios, redes, computadores, etc. O termo surgiu como o autor de ficção científica Willian Gibson, em 1984, no livro *Neuromancer*, sendo utilizado para designar um ambiente artificial onde trafegam dados e relações sociais de forma indiscriminada. Para Gibson, ciberespaço é um espaço não físico no qual uma alucinação consensual pode ser experimentada diariamente pelos usuários. Já para Lévy, o ciberespaço é definido como o espaço de comunicação formado pela interconexão mundial dos computadores e das suas memórias. Constituindo-se em um espaço virtual de trocas simbólicas entre pessoas e que pode ser entendido como o espaço de troca de informação na cultura contemporânea (SÓ PEDAGOGIA, c2008-2017).

TI e o mercado eletrônico

Você verá agora os principais conceitos das aplicações da TI no mercado eletrônico. Sem essas interações não haveria mercado ou comércio eletrônico, nem mesmo negociações eletrônicas.

- **Comunicação eletrônica:** trata da troca de informações entre as partes envolvidas em um processo, podendo ser duas empresas, uma empresa e um consumidor ou vários agentes. Essa comunicação ganha velocidade, segurança e tempo de processamento pelas tecnologias envolvidas, além de redução de custos.
- **Intermediação eletrônica:** as informações têm livre acesso, tanto por parte do fornecedor para o cliente, do cliente para o fornecedor e entre fornecedores, com isso há uma redução de custos em todas as etapas do processamento. Como a intermediação ocorre no formato eletrônico, também há um ganho nas possibilidades de alternativas disponíveis, aumentando o leque de opções para os envolvidos, completando as vantagens da redução de custos com o aumento da qualidade.
- **Integração eletrônica:** é o fator que permite que todos estejam conectados eletronicamente, sem essa integração não haveria mercado eletrônico.

Esses processos vão definir o atendimento das demandas da empresa, e o formato escolhido vai ser distrito no planejamento estratégico (nele a empresa vai dizer qual a expectativa e nível de serviço escolhido), com isso irá realizar os investimentos necessários para deixar o sistema funcional, prevalecendo às decisões sobre o desenvolvimento relacional com parceiros, fornecedores e clientes.

O aspecto segurança também vai estar no planejamento da empresa, visto que, para proteger o serviço ofertado ou demandado, a empresa terá que tomar alguns cuidados com as informações processadas, como monitorar e-mails recebidos e enviados e alguns tipos de rastreamento na web, para verificarmos os acessos ao seu site ou ambiente de comércio eletrônico.

A integração eletrônica utiliza uma relação entre a troca eletrônica de dados Electronic Data Interchange (EDI) e Interorganizational Systems (IOS). O EDI é uma plataforma técnica baseada em um conjunto de padrões estruturados e conhecidos por todas as organizações, ou seja, os arquivos, por exemplo, de uma carteira de cobranças, sai de uma empresa qualquer e é transmitido e recebido em uma organização financeira qualquer, havendo, obviamente

um contrato entre elas. O IOS estabelece os padrões dessas comunicações e as interconecta.



Saiba mais

O EDI é hoje uma das formas mais importante de comércio eletrônico existente, pois possui o potencial de aumentar a velocidade das operações, a eficiência dos processos e de reduzir os custos operacionais e de processamento de informações entre as organizações. Contudo, a implementação do EDI não é fácil, exigindo mudanças no *modus operandi* da organização quanto à padronização dos processos, além da existência de vários protocolos de transmissão, o que leva muitos a não adotarem o processo (DIAS, 2011).

Crimes virtuais

Os crimes virtuais são atos dirigidos contra um usuário ou um conjunto de usuários que utilizam sistemas de informática para realizar suas atividades pessoais ou empresariais, podem ser atos contra o computador propriamente dito ou atos contra os dados ou programas armazenados nessas unidades.



Figura 2. Crime virtual.

Fonte: Corrêa (c2017).

Os crimes virtuais também são chamados de Cyber crimes, ou crimes eletrônicos ou cibernéticos, contudo, independentemente do nome, são fatos

e atos ocorridos no ambiente da rede de computadores considerados pela legislação penal como crimes ou contravenções penais.

Essas infrações, normalmente são contra o patrimônio da pessoa ou empresa, ocasionando de alguma forma perdas financeiras ou materiais. Além disso, encontramos também as infrações contra a liberdade individual e a propriedade intelectual das pessoas ou organizações.

Em nosso país, esse tipo de crime aumentou em progressão geométrica, com o aumento de usuários e empresas que utilizam a rede de computadores para o seu dia a dia, porém, os dados podem ser ainda mais altos, pois há o fator de que por vergonha de assumir que foi enganada a pessoa não faz a denúncia aos órgãos competentes.

Assim como as pessoas de bem e as empresas sérias aumentaram suas participações na rede de computadores, também entraram nesse processo algumas pessoas ou empresas que são criminosos e deslumbraram uma forma de se beneficiar com essas novidades. O campo ficou fértil para os golpes, porque ainda hoje muitos usuários não sabem se proteger desses crimes, tornando-se vítimas fáceis para esses criminosos.

A legislação brasileira, em razão do aumento desse tipo de crime, teve que criar leis para eventuais punições aos crimes praticados. Em novembro do ano de 2012, foi promulgada a Lei nº 12.737, da qual transcrevemos o primeiro artigo: “Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências” (BRASIL, 2012).



Saiba mais

Em geral, dividimos os crimes virtuais em três tipos: o puro, o comum e o misto. O comum é aquele que utiliza da rede de computadores para ser feito, sendo a rede um instrumento para cometer o delito; o puro é aquele que tem as condutas ilícitas direcionadas à parte virtual de um computador ou até mesmo a sua parte física; e os mistos são a união desses dois, praticados pela internet e afetando o software ou hardware.

São alguns exemplos desses crimes: ameaça, difamação, injúria, calúnia, discriminação, estelionato, pedofilia e falsa identidade.

Segue uma relação com os crimes que mais ocorrem e são praticados por criminosos.

- **Furto de dados, promoções e estelionato:** os criminosos podem criar situações para furtrar dados dos usuários e depois utilizar esses dados de alguma forma para ganhar vantagem, podem, por exemplo, criar promoções falsas para iludir os usuários, facilitando a obtenção desses dados. Utilizam para isso páginas falsas, perfis falsos em redes sociais entre outros. Podem ser enquadrados no crime de estelionato, art. 171 do código penal que é “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.” (BRASIL, 2012).
- **Difamação, calúnia e injúria:** neste caso podemos encontrar campanhas contra empresas, por exemplo, difamando seus produtos com informações não verdadeiras; e no caso de pessoas físicas, em redes sociais, por antigos companheiros depois de uma separação, colocar falsas ou informações íntimas do outro sem a devida permissão. Segue o artigo penal que fala sobre esse assunto: “Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro...” E temos a difamação como nos mostra o art. 139 do Código Penal “Difamar alguém, imputando-lhe fato ofensivo à sua reputação” (BRASIL, 2012).
- **Pedofilia:** essa é uma grande chaga da sociedade que deve ser punida, infelizmente há um grande número de casos para serem tratados, existem muitos sites com esses conteúdos e muitos pedófilos que se passam por outras pessoas com perfis falsos com o objetivo de atrair vítimas para satisfazer suas perversas necessidades. Segue um exemplo de jurisprudência sobre esses casos: “Penal. Pedofilia ou pseudossexualidade. Reprodução fotográfica. Fotografar ou publicar fotos de crianças e adolescentes em pose eróticas. Inserção em rede bbs/internet de computadores. Crime. Art. 241 do estatuto da criança e do adolescente com a redação ditada pela Lei 10.764, de 2003. Crime de ação múltipla.”
- **Ameaça:** é o crime de escrever ou mostrar uma imagem que ameace alguém para conseguir alguma vantagem ou criar um constrangimento, mesmo que por brincadeira ou piada.
- **Falsa identidade:** ocorre quando uma pessoa mente dados de seu nome, idade, estado civil, sexo e outras características para cometer algum dos atos ilícitos descritos acima, para enganar ou prejudicar outra pessoa.
- **Pirataria:** quando uma pessoa ou empresa copia ou reproduz algum conteúdo sem autorização do autor, há muitos exemplos desse crime os mais usuais são realizados com músicas, livros e criações artísticas, no âmbito das pessoas físicas, e nas empresas furto de projetos e processos industriais e utilização de softwares sem o pagamento das licenças de uso.

Para que um crime ocorra são necessários basicamente dois sujeitos: os passivos, que são as pessoas ou empresas que sofrem algum tipo de dano a imagem ou ao patrimônio; e os sujeitos ativos que são aqueles que cometem diretamente os crimes, algumas vezes fáceis de serem identificados, outras vezes com difícil identificação e localização. O crime de racismo, por exemplo, pode ser praticado na forma de envio de mensagens com conteúdo discriminatório, entre outras formas disfarçadas em figuras ou imagens, outro exemplo seria a sabotagem, que consiste em destruir ou danificar as estações de trabalho dos usuários com objetivo de encobrir delitos.

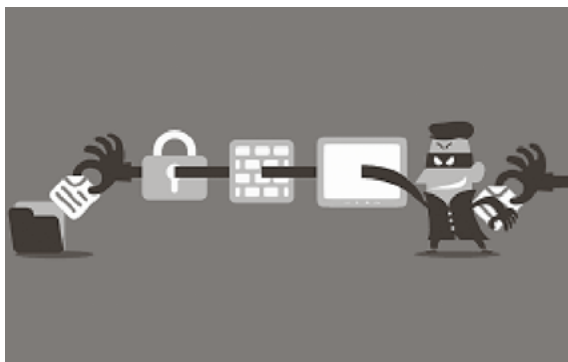


Figura 3. Sujeitos do crime.

Fonte: Abril Branded Content (2017).

Esses criminosos podem receber vários nomes, os mais conhecidos são *hacker*, *phreaker* e *pirate*. O **pirate** normalmente atua na produção de cópias e distribuição de softwares sem autorização dos proprietários (protegidos por copyright); o **phreaker** atua na área de captura de dados via rede de telefonia e o **hacker** atua invadindo sistemas e máquinas sem a autorização do proprietário, seja uma pessoa física ou uma organização.

Esses crimes são penalizados pelo Código Penal (BRASIL, 2012), contudo alguns ainda não têm um artigo específico, visto que a cada dia surgem maneiras diferentes e mais revolucionárias. Esses novos crimes acabam por entrar de forma analógica nos artigos do Código Penal (arts. 138, 139 e 140), como crime de ameaça (art. 147 do CP); furto (art. 155 do CP); extorsão (art. 158 do CP); extorsão indireta (art. 160 do CP); apropriação indébita (art. 168 do CP).

Maiores golpes da internet

Partindo do pressuposto que existem inúmeros crimes virtuais, você verá, agora, seis golpes que são praticados atualmente na rede de computadores, eles possuem várias modelagens para chegar ao usuário final ou dentro das organizações, e a formação do conhecimento sobre eles é que vai definir as melhores formas de evitar e reconhecer os mesmos, evitando assim os dissabores das perdas ocasionadas por eles.

- **Boletos bancários:** atualmente não há mais uma data certa para esse tipo de golpe, antigamente eles vinham no começo do ano, na forma de registro de entidades de classe, impostos a pagar ou doações a entidades filantrópicas. Hoje eles estão todo o dia, seja na caixa de entrada de e-mails pessoas ou e-mails corporativos, são provenientes de empresas falsas, com dados bancários falsos e aparentemente reais, algumas vezes os pagadores têm seus dados interceptados e os criminosos se fazem passar pelo próprio fornecedor real, mas os dados dos boletos são redirecionados a contas fantasmas e seus valores são perdidos. O sistema financeiro está tomando medidas para minimizar esse tipo de golpe, inclusive acabando com as cobranças sem registro e adotando medidas para processamento on-line das cobranças, com o objetivo de minimizar esse tipo de golpe.
- **Falsos e-mails de instituições financeiras:** como é bom receber um e-mail de uma instituição financeira que lembrou que eu não atualizei os dados, solicita meus dados bancários e senhas para agilizar o processo e, depois, vem a notícia, sua conta foi acessada, muito cuidado. Normalmente as instituições financeiras não enviam malas diretas, não enviam links para acesso e essas solicitações sempre devem ser confirmadas com a instituição antes de qualquer fornecimento de dados. Esses e-mails devem ser evitados e seus anexos nunca abertos, são uma porta de entrada para os criminosos capturarem seus dados e fazerem uma má utilização deles como acesso a contas bancárias ou compras em outras instituições.
- **Oportunidades de emprego falsas:** na mesma proporção dos golpes financeiros, também encontramos os golpes que prometem vantagens ou empregos on-line, com vagas de trabalho em casa ou em grandes corporações, com ganhos acima da média de mercado. Os golpistas têm mecanismos para iludir as vítimas prometendo ganhos financeiros e fazem com que ela de alguma maneira envie para eles algum tipo de

reembolso ou adiantamento de receitas a processar. Antigamente, esse golpe era chamado de “golpe do bilhete”, alguém afirmava que tinha um bilhete premiado, mas que não tinha tempo para aguardar o prêmio ou tinha que se ausentar e pedia uma pequena quantia pelo bilhete, assim a vítima com a possibilidade de ganho fácil comprava esse bilhete por um preço baixo para ganhar futuramente um valor maior e eis que esse bilhete era falso. Mudaram os nomes, mudaram as tecnologias, mas os golpes ainda estão no mercado, portando você teve ser muito cuidado.

- **Furto de identidade:** acontece quando, de alguma forma, seus dados são furtados e outra pessoa assume a sua identidade para, por exemplo, abrir uma conta bancária ou contratar algum serviço de telefonia ou mesmo internet, podem ocorrer até casos de aberturas de empresas na rede de computadores, podem ser criadas contas nas redes sociais e e-mails para envio de mensagens passando-se por você. Quando mais informações você deixa disponível na internet, maiores são as chances dessas informações caírem em mãos erradas.
- **Phishing:** É uma de fraude eletrônica que tem como objetivo adquirir informações sigilosas dos usuários e empresas, como números de cartões de crédito e senhas. A palavra significa “pescar”, os criminosos tentam pescar esses dados, por meio de e-mails falsos, páginas falsas, sites duplicados, telas de *login* falsas entre outras formas.



Saiba mais

A URL é uma identificação que determinado elemento obtém na internet com a finalidade de ser referido e dar acesso aos usuários. Na verdade, o uso da internet continua usando este tipo de referência, embora não seja percebido. Um caso emblemático é o das páginas web, que devem ser identificadas com o nome de domínio do servidor e o caminho a seguir de um arquivo. Neste caso, a URL precisa também do protocolo utilizado para fazer uso desse elemento (CONCEITOS, c2010-2017).

Marco civil da internet

O marco civil da internet data de 2014, e é hoje um forte instrumento para regulamentação de um serviço que, até então, não contava com um documento exclusivo de regulamentação, as boas ações e más ações praticadas por esse

canal de comunicação não tinham um norte a seguir, ele é um compilado de tentativas anteriores. Desde os anos de 1999 tínhamos uma primeira proposta feita pelo deputado Luiz Piauhyino, que ficou conhecido como o PL dos Crimes Digitais.

Infelizmente, a velocidade das inovações na área de TI é bem superior do que a velocidade que a legislação consegue acompanhar, ficando, assim, muitos delitos sem previsão legal e contando com a insegurança jurídica. Como todo o cuidado é pouco, você deve saber que se tratando de pessoas físicas o dano pode ser grande, agora, imaginem em empresas, em que os dados podem ser bem maiores.

Por um longo período o marco civil foi discutido no Brasil, é um texto pioneiro no que se refere às regras, direitos e deveres os usuários pessoas físicas e jurídicas no ambiente virtual. Mesmo tendo sido sancionado em 2014, até hoje uma grande parte dos usuários desconhece o seu conteúdo e as alterações que essa lei causa nesse ambiente. Ele assegura a liberdade de expressão, a privacidade e a garantia da neutralidade da rede, definindo os atores que interagem neste ambiente, e, o principal, os direitos e deveres de cada um. Por exemplo, um provedor de internet pode coletar usar, armazenar e tratar os dados pessoais de seus usuários, desde que essas tarefas estejam especificadas no contrato de prestação de serviços ou nos termos de uso das aplicações da internet.

No texto, em seu art. 29, a Lei (BRASIL, 2014) diz que o usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, essa medida é uma forte aliada para o combate a pornografia infantil por exemplo.



Link

Lembrando os grandes administradores, só gerenciamos o que conhecemos e, para conhecermos, usamos os sistemas de informação para nos auxiliar. Para você que irá atuar fortemente na área de TI, recomendamos a leitura da lei nº 12.965, de 23 de abril de 2014 (Brasil, 2014), que você pode acessar pelo link ou código a seguir:



<https://goo.gl/fj8a4q>

Lembre-se dos possíveis riscos da internet (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2017):

- **Acesso a conteúdos impróprios ou ofensivos:** ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.
- **Contato com pessoas mal-intencionadas:** existem pessoas que se aproveitam da falsa sensação de anonimato da internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes.
- **Furto de identidade:** assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, o que coloca em risco a sua imagem.
- **Furto e perda de dados:** os dados presentes em seus equipamentos conectados à internet podem ser furtados e apagados pela ação de ladrões, atacantes e códigos maliciosos.
- **Invasão de privacidade:** a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serão repassadas.
- **Divulgação de boatos:** as informações na internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo. Enquanto isso pode ser desejável em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.
- **Dificuldade de exclusão:** aquilo que é divulgado na internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você e acessada por diferentes pessoas, desde seus familiares até seus chefes.
- **Dificuldade de manter sigilo:** na internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.
- **Plágio e violação de direitos autorais:** cópia, alteração ou distribuição não autorizada de conteúdos e materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras.



Exercícios

- 1.** O ritmo das inovações tecnológicas é mais intenso do que a legislação consegue acompanhar, ocasionando problemas como crimes sem previsão legal e insegurança jurídica. Se tratando de comércio eletrônico, o impacto desses problemas é ainda maior, pois os valores financeiros envolvidos atualmente são muito grandes. Além dos aspectos legais, o uso de Tecnologias da Informação (TI) ainda está diretamente relacionado a questões éticas que, direta ou indiretamente, causam conflitos com seus usuários. Analise as afirmações sobre aspectos éticos relacionados com TI e comércio eletrônico:
- Muitas empresas utilizam programas capazes de monitorar todos os e-mails recebidos e enviados por seus funcionários, o que necessariamente não caracteriza um crime.
 - O rastreamento web é um recurso frequentemente utilizado pelas empresas para se obter informações específicas de cada visitante do seu site ou ambiente de comércio eletrônico.
 - A diminuição de postos de trabalho e a maneira como são tratados os trabalhadores que perdem seus cargos são exemplos práticos dos benefícios sociais ocasionados pelo comércio eletrônico.
- Está correto o que se afirma apenas em:
- I e II.
 - I e III.
 - II e III.
 - I, II e III.
 - Nenhuma das afirmativas.
- 2.** Os meios de pagamento estão diretamente relacionados aos aspectos legais do comércio eletrônico. Como a maioria dos sistemas de pagamento tradicionais não atendem às demandas do comércio eletrônico, ou seja, das empresas e de seus clientes, foram desenvolvidos métodos mais adequados aos processos eletrônicos. A partir de inovações realizadas nos meios de pagamento on-line, eles ficaram relativamente seguros e confiáveis, permitindo a evolução e o crescimento das transações comerciais tendo como base a estrutura da internet. Analise as afirmações a seguir sobre pagamentos eletrônicos e identifique a correta.
- A transferência eletrônica de fundos é um método de pagamento no qual o dinheiro é transferido da conta do pagador para uma conta intermediária até que ele receba o produto comprado.
 - O método da cobrança direta permite que o cliente efetue um único pagamento para compras realizadas em diferentes sites, agilizando todo o processo de aprovação de crédito e envio dos produtos.
 - Os micropagamentos são faturas eletrônicas geradas a partir da acumulação de dívidas do cliente com compras de alto valor.

- d)** Para pagar contas na internet, o cliente pode se cadastrar em um serviço on-line de pagamento de contas e realizar todos os pagamentos a partir de um único site.
- e)** Todos os cartões de crédito eletrônicos utilizados em transações no ambiente virtual são encriptados, aumentando o nível de segurança para os usuários.
- 3.** O Brasil avança, mesmo que lentamente, no combate aos crimes pela internet. Desde fraudes localizadas e de menor dano até crimes envolvendo pedofilia e tráfico de drogas, é possível rastrear os autores e processá-los pelos seus atos. Entretanto, esse rastreamento não é simples e demanda profissionais altamente qualificados, além de tempo e equipamentos adequados para essa tarefa. Em relação aos crimes virtuais, analise as seguintes afirmações:
- I.** Em função de restrições legais, no Brasil ainda não é permitida a realização de investigações no submundo da rede mundial de computadores (a internet), o que faz com que criminosos continuem a utilizar esse ambiente para praticarem seus crimes.
- II.** Um aspecto positivo das inovações tecnológicas é que elas estão disponíveis apenas para empresas e pessoas idôneas.
- III.** O crime de racismo praticado por meio da rede mundial de computadores consuma-se com o envio das mensagens com conteúdo discriminatório.
- Está correto somente o que se afirma em:
- a)** I.
b) II.
c) III.
d) I, II e III.
e) Nenhuma das afirmações.
- 4.** Crimes virtuais são aqueles em que o computador ou equipamentos tecnológicos são utilizados como meio ou instrumento para atingir propósitos ilícitos. Assim como ocorre nos crimes tradicionais, os crimes virtuais precisam de provas para serem julgados. No caso do ambiente virtual, essas provas podem variar de formato, sendo aceitas desde uma mídia com arquivos até postagens comprovadas em uma rede social. Infelizmente, os criminosos já descobriram como tirar proveito das inovações tecnológicas para alcançarem seus objetivos de diversas maneiras e na aplicação de variados crimes. A sabotagem é um dos crimes virtuais mais cometidos e consiste em:
- a)** alteração, inclusão ou omissão de dados com o objetivo de conseguir vantagens econômicas.
b) destruição ou danificação de computadores ou seus componentes.
c) distribuição pela internet de material ofensivo a uma pessoa ou empresa.
d) utilização de meios fraudulentos para conseguir alguma vantagem ilícita.
e) utilização e acesso indevidos a um ambiente ou sistema de computação.
- 5.** Durante quatro anos, o marco civil da internet foi discutido no Brasil,

sendo atualmente considerado um texto pioneiro no que se refere a regras, direitos e deveres das pessoas e empresas no ambiente virtual. O projeto recebeu sugestões em diversas audiências públicas realizadas no país, além de contribuições enviadas por meio de plataformas on-line, como o Twitter. A lei foi sancionada pela Presidência da República em 2014. Mesmo com ampla divulgação, a maioria dos usuários da internet ainda desconhece o conteúdo da lei e as alterações que ela provoca neste ambiente. Sua principal característica é o reforço da liberdade de expressão, a proteção da privacidade e a garantia da neutralidade da rede. Além disso, a lei define os atores que interagem neste ambiente e os direitos e deveres de cada um. Em relação ao marco civil da internet, identifique a afirmativa correta.

- a)** A conexão com a internet pode ser suspensa pela operadora a qualquer momento, mesmo que o cliente não possua débito diretamente decorrente de sua utilização.
- b)** A disciplina do uso da internet no Brasil tem por objetivo a promoção da inovação e do direito de acesso exclusivo à rede mundial de computadores por pessoas com renda mensal familiar *per capita* superior a um salário mínimo.
- c)** Em relação à neutralidade de rede, o responsável pela transmissão dos dados pode (mesmo sem regulamentação) tratar de forma diferenciada determinados pacotes de dados.
- d)** O provedor responsável pela guarda poderá disponibilizar os registros de conexão e de acesso às aplicações de internet, inclusive nos casos que envolvem ordens judiciais.
- e)** Um provedor de internet pode coletar, usar, armazenar e tratar os dados pessoais de seus usuários, desde que essas tarefas estejam especificadas no contrato de prestação de serviços ou nos termos de uso das aplicações de internet.



Referências

ABRIL BRANDED CONTENT. Ameaças digitais exigem novas soluções de segurança em empresas. *Exame*, São Paulo, 17 fev. 2017. Disponível em: <<http://exame.abril.com.br/tecnologia/ameacas-digitais-exigem-novas-solucoes-de-seguranca-em-empresas/>>. Acesso em: 14 set. 2017.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Brasília, DF, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 10 ago. 2017.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Brasília, DF, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 ago. 2017.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. *Cartilha de segurança para internet*: 1. Segurança na internet. [S.l.]: CERT.br, 2017. Disponível em: <<https://cartilha.cert.br/seguranca/>>. Acesso em: 10 ago. 2017.

CONCEITOS. *URL*: conceito, o que é, significado. [S.l.], c2010-2017. Disponível em: <<https://conceitos.com/url/>>. Acesso em: 10 ago. 2017.

CORRÊA, R. *Delegacia de crimes virtuais. Entenda melhor!* Serra, c2017. Disponível em: <<http://rafaelcorrea.com.br/delegacia-de-crimes-virtuais/>>. Acesso em: 14 set. 2017.

DIAS, L. L. Electronic Data Interchange (EDI): benefícios x custos para implementação. *Administradores*, João Pessoa, 13 jul. 2011. Disponível em: <<http://www.administradores.com.br/artigos/economia-e-financas/electronic-data-interchange-edi-beneficios-x-custos-para-implementacao/56625/>>. Acesso em: 10 ago. 2017.

FECOMERCIO.SP. *Comércio eletrônico fatura R\$ 3,6 bilhões no Estado de São Paulo no primeiro trimestre de 2016*. São Paulo, 2016. Disponível em: <<http://www.fecomercio.com.br/noticia/comercio-eletronico-fatura-r-3-6-bilhoes-no-estado-de-sao-paulo-no-primeiro-trimestre-de-2016-1>>. Acesso em: 14 set. 2017.

SÓ PEDAGOGIA. *Ciberespaço e cibercultura*: definições e realidades virtuais inseridas na práxis do homem moderno. [S.l.], c2008-2017. Disponível em: <http://www.pedagogia.com.br/artigos/ciberespaco_cibercultura/?pagina=1>. Acesso em: 18 ago. 2017.

Leituras recomendadas

BRASIL. Câmara dos Deputados. *Marco civil da internet*. 2. ed. Brasília, DF, 2015. (Série Legislação).

CCM. *E-comércio*: como verificar se um site é seguro. [S.l.], 2017. Disponível em: <<http://br.ccm.net/faq/17615-e-comercio-como-verificar-se-um-site-e-seguro>>. Acesso em: 10 ago. 2017.

DIÓGENES, Y.; MAUSER, D. *Certificação Security+*: da prática para o exame SY0-401. 2. ed. Rio de Janeiro: Novaterra, 2015.

SAMPAIO, J. H. P.; LIMA, A. F. S. *Crimes virtuais*: conceito e seus tipos. [S.l.]: Jusbrasil, 2016. Disponível em: <<https://carmo311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus-tipos>>. Acesso em: 10 ago. 2017.



editora
papervest

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