UNIP

UNIVERSIDADE PAULISTA

Legislação Computacional e Ética

Autoras: Profa. Irene Kim
Profa. Vanessa Santos Lessa
Colaboradora: Profa. Christiane Mazur Doi

Professoras conteudistas: Irene Kim / Vanessa Santos Lessa

Irene Kim

Mestra em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. Graduada em Ciências Contábeis pela Faculdade Trevisan e em Direito pela Pontifícia Universidade Católica de São Paulo. É palestrante do Conselho Regional de Contabilidade do Estado de São Paulo e perita contábil do Conselho Federal de Contabilidade. Na UNIP, é coordenadora de graduação e professora dos cursos presenciais e a distância de Ciências da Computação, Gestão Financeira, Direito e Ciências Contábeis.

Vanessa Santos Lessa

Doutora em Ciências e Aplicações Geoespaciais pelo Mackenzie, mestra em Engenharia Elétrica com ênfase em Inteligência Artificial Aplicada à Automação pelo Centro Universitário da Fundação Educacional Inaciana e bacharel em Engenharia da Computação pela Universidade São Judas Tadeu. Atua há mais de 18 anos em cargos técnicos e gerenciais na área de computação. É coordenadora do curso de Ciência da Computação na UNIP na modalidade EaD.

Dados Internacionais de Catalogação na Publicação (CIP)

K49l Kim, Irene.

Legislação Computacional e Ética / Irene Kim, Vanessa Santos Lessa. – São Paulo: Editora Sol, 2024.

160 p., il.

Nota: este volume está publicado nos Cadernos de Estudos e Pesquisas da UNIP, Série Didática, ISSN 1517-9230.

1. Legislação. 2. Direito digital. 3. Ética. I. Kim, Irene. II. Lessa, Vanessa Santos. III. Título.

CDU 681.3:340

U519.89 – 24

Sumário

Legislação Computacional e Ética

APRESENTAÇÃO

Como futuro cientista da computação, você precisará ter noções básicas sobre as aplicações dos conceitos do direito, da legislação profissional, de seus aspectos e as tendências aplicadas aos profissionais da área de tecnologia da informação. O conhecimento de leis e de alguns institutos jurídicos fundamentais é indispensável para o exercício profissional dos que atuam no campo da tecnologia da informação.

O objetivo desta disciplina é conscientizar o aluno da importância da ética nas relações profissionais e pessoais, analisando eventuais implicações jurídicas.

Vale acrescentar que este material é escrito em linguagem simples e direta, como se houvesse uma conversa entre as autoras e o leitor. Adicionalmente, são inseridas figuras, que auxiliam no entendimento dos tópicos desenvolvidos. Os itens observação e lembrete são oportunidades para que você solucione eventuais dúvidas. Já o item saiba mais possibilita que você amplie seus conhecimentos. Há, ainda, muitos exemplos para a fixação dos assuntos abordados.

Esperamos que você faça uma boa leitura e se sinta motivado a conhecer mais os assuntos tratados nesta disciplina.

Bons estudos.

INTRODUÇÃO

A legislação computacional, também conhecida como direito da tecnologia da informação ou direito digital, é uma área do direito que lida com questões jurídicas relacionadas à tecnologia da informação, computadores, redes e dados. O crescente papel da tecnologia na sociedade gerou uma série de desafios legais que precisam ser abordados.

A legislação computacional e a ética são dois campos interconectados e de grande importância no mundo digital, que está em constante evolução. A ética na tecnologia envolve a consideração dos princípios éticos ao criar, usar e regular tecnologias.

A relação entre a legislação computacional e a ética é clara: as leis muitas vezes buscam promover práticas éticas e proteger os direitos e interesses das partes envolvidas. No entanto, nem todas as questões éticas têm uma solução legal direta, e é importante que a sociedade continue a debater e desenvolver normas éticas à medida que a tecnologia avança. Além disso, a legislação deve ser adaptada constantemente para acompanhar o rápido ritmo da inovação tecnológica.

O conteúdo deste livro-texto foi dividido em duas unidades. Na unidade I apresentaremos as noções básicas de legislação profissional, evoluindo para o Marco Civil da Internet, direito digital, direito à intimidade e divulgação de notícias falsas. Na unidade II abordaremos os novos modelos econômicos na realidade digital, a ética pessoal e profissional, o código de ética profissional e o profissional de TI e seu mercado de trabalho.

Unidade I

1 NOÇÕES BÁSICAS DE LEGISLAÇÃO PROFISSIONAL

As noções básicas de legislação profissional referem-se às leis e às regulamentações que governam a conduta e a prática de profissionais em diversas áreas. Essas leis são projetadas para garantir que os profissionais atuem de maneira ética, responsável e dentro dos limites de sua profissão.

Muitas profissões exigem que os indivíduos obtenham uma licença ou certificação para exercê-las legalmente. Isso geralmente envolve a conclusão da educação formal, a aprovação em exames e o preenchimento de outros requisitos estabelecidos por órgãos reguladores. A prática sem a devida licença pode resultar em penalidades legais.

Algumas profissões têm códigos de ética, que estabelecem padrões de conduta profissional. Esses códigos orientam os profissionais sobre questões éticas, como confidencialidade e imparcialidade, evitando conflitos de interesse e incentivando a responsabilidade com os clientes e a sociedade em geral.

Os profissionais são responsáveis por suas ações no desempenho das funções. Isso significa que eles podem ser responsabilizados legalmente por negligência, má conduta ou ações que causem danos a terceiros. Seguro de responsabilidade profissional é comum em muitas áreas para proteger profissionais nesses casos.

Muitas profissões exigem que os indivíduos continuem se aperfeiçoando ao longo da carreira para se manterem atualizados em relação às melhores práticas e aos avanços na área de atuação. A falta de atualização pode ter consequências legais e éticas.

Os profissionais devem evitar situações em que seus interesses pessoais possam entrar em conflito com os interesses de seus clientes ou empregadores. Conflitos de interesse podem ser considerados antiéticos e levar a ações legais.

A legislação profissional estabelece processos para relatar má conduta de outros profissionais. Isso ajuda a manter a integridade da profissão e a proteger o público de práticas inadequadas.

Há profissões que são regulamentadas por órgãos governamentais ou agências de regulamentação. Essas entidades estabelecem normas e regulamentos que os profissionais devem seguir e podem tomar medidas disciplinares em caso de violações.

Diversas profissões, especialmente na área de saúde, exigem que os profissionais protejam a confidencialidade das informações do cliente ou paciente. A divulgação não autorizada de informações confidenciais pode ter implicações legais e éticas.

As leis de proteção ao consumidor frequentemente se aplicam a profissões que prestam serviços aos clientes. Essas leis visam garantir que os consumidores recebam um serviço de qualidade, estejam bem-informados e tenham recursos para resolver disputas.

É importante notar que as leis e regulamentações variam de uma profissão para outra e de um país para outro. Cabe ao profissional conhecer e cumprir as leis e regulamentações que se aplicam à sua área específica de atuação. Violar essas leis ou códigos de ética pode resultar em sanções legais, perda de licença profissional e danos à reputação. Portanto, é fundamental que os profissionais estejam cientes das noções básicas de legislação profissional e se esforcem para agir de acordo com os padrões éticos estabelecidos.

1.1 A legislação profissional aplicada à internet

A legislação profissional aplicada à internet é um campo em constante evolução que lida com leis, regulamentações e padrões éticos que afetam profissionais que trabalham em ambientes online. Com o rápido crescimento da internet e a diversificação de carreiras digitais, é fundamental entender como as leis se aplicam a esse contexto.

A propriedade intelectual na internet é regulamentada por leis de direitos autorais, marcas registradas e patentes. Profissionais que criam conteúdo online, como escritores, designers, desenvolvedores de software e criadores de mídia, devem estar cientes de como essas leis protegem suas obras e respeitar os direitos de propriedade intelectual de outros.

Destaque

A importância do Marco Civil da Internet para o crescimento do direito e da computação no Brasil

[...]

O Marco Civil da Internet não é apenas a primeira grande demonstração da união entre o direito e a computação, mas é uma garantia de continuidade do progresso destas duas áreas do conhecimento humano.

[...]

Podemos elencar diversas invenções que alteraram o curso do mundo, tais como a prensa de Johannes Gutenberg (1450), a máquina a vapor de James Watts (1769) e a penicilina de Alexander Fleming (1928), entre muitas outras. Indiscutivelmente são todas invenções que tiveram um impacto enorme na humanidade, mas o foco principal de cada uma delas sempre foi específico. A primeira máquina universal que o homem produziu foi a Máquina de Turing, ou seja, o computador eletrônico que usamos hoje. Essa máquina dotada da conectividade proporcionada pela internet, aliada a recursos

amplos de acessibilidade, modificou uma série de aspectos que alteraram o cotidiano das pessoas. Essas alterações vão do acesso ao conhecimento e à informação, até a convivência social, do *modus operandi* do comércio até a prestação de serviços. Hoje a nossa noção de espaço ocupado é diferente de anos passados e não se limita mais a territorialidade geográfica, tampouco o conceito de tempo, hoje extremamente explorado pelos zilhões de mensagens e comandos trocados a cada instante.

A internet, criada para fins militares nos Estados Unidos, teve seu início comercial bastante tímido ainda no ano de 1985 com o primeiro serviço comercial de provimento de internet (ISP) chamado "The World"1. Era tempo de acesso discado, o que mesmo assim conseguiu levar milhares de pessoas ao mundo virtual. Nesta época a *National Science Foundation* dos EUA havia proibido o uso comercial da internet. Apenas agências governamentais e universidades estavam autorizadas a usar a rede mundial. Entretanto, nos EUA tudo mudou em 1991 quando a NSF suspendeu a proibição aos ISPs comerciais depois que percebeu que o "The World" havia "aberto as comportas" a um mundo que não seria mais o mesmo. Lembro que o mundo vivia o contexto de abertura ampla. O ano de 1991 também foi o ano do fim da União Soviética, apenas três anos após a queda do muro de Berlim.

[...]

Adaptado de: Ruiz (2023).

Saiba mais

Para ler o texto anterior na íntegra, acesse:

RUIZ, E. E. S. A importância do Marco Civil da Internet para o crescimento do Direito e da Computação no Brasil. *Migalhas*, 19 maio 2023. Disponível em: http://tinyurl.com/2p9499pe. Acesso em: 8 fev. 2024.

No Brasil, a legislação de direitos autorais é regida pela Lei n. 9.610, que entrou em vigor em 19 de fevereiro de 1998. Essa lei é conhecida como a Lei de Direitos Autorais e estabelece os princípios e regulamentos relacionados à proteção de obras intelectuais no país.

A Lei de Direitos Autorais protege várias obras, incluindo textos, músicas, obras de arte, filmes, fotografias, arquitetura, software e outras formas de expressão criativa. Além disso, ela define os direitos exclusivos do autor sobre suas obras, como o direito de reprodução, distribuição, exibição e adaptação.

Lembre-se de que a legislação de direitos autorais no Brasil, assim como em outros países, pode ser atualizada e emendada ao longo do tempo. Portanto, é aconselhável consultar fontes oficiais e atualizadas para obter informações precisas sobre a legislação em vigor.

Saiba mais

Para acessar a Lei de Direitos Autorais no Brasil e obter informações detalhadas sobre a legislação, é preciso entrar no site oficial do Governo Federal do Brasil, que disponibiliza o texto completo da lei. Além disso, conseguimos consultar a Fundação Biblioteca Nacional e o Instituto Nacional da Propriedade Industrial (INPI) para obter informações adicionais e recursos relacionados à legislação de direitos autorais no país.

BRASIL. *Fundação Biblioteca Nacional*. Rio de Janeiro, [s.d.]a. Disponível em: https://tinyurl.com/yr3han2d. Acesso em: 8 fev. 2024.

BRASIL. *Instituto Nacional da Propriedade Industrial*. Rio de Janeiro, [s.d.]b. Disponível em: https://tinyurl.com/4jsu4xvu. Acesso em: 8 fev. 2024.

BRASIL. *Lei n. 9.610, de 19 de fevereiro de 1998*. Brasília, 1998b. Disponível em: http://tinyurl.com/4tt3ah5y. Acesso em: 8 fev. 2024.

Destaque

Inteligência artificial e os seus impactos no direito civil e no direito autoral

[...]

A cantora Elis Regina, uma das mais lindas e potentes vozes da história da música popular brasileira, faleceu na manhã do dia 19 de janeiro de 1982, aos 36 anos, vítima de overdose acidental. Elis não tinha um histórico de consumo de drogas. Daí por que a fatalidade potencializou o impacto da triste notícia no grande público.

Quando Elis morreu, sua filha caçula Maria Rita tinha apenas 4 anos de idade.

Em 2003, Maria Rita lançou seu primeiro disco, que teve participação especial de Milton Nascimento, seu padrinho musical.

Elis foi a primeira cantora conhecida a gravar uma música de Milton. "Canção do Sal" foi gravada por ela em 1966. Elis Regina disse que "Se Deus cantasse, teria a voz de Milton Nascimento".

Desolado com a sua morte, Milton, que era um grande fã e amigo de Elis Regina, sequer conseguiu ir ao enterro da cantora. Elis foi madrinha musical de Milton. E, tempos depois, Milton foi o padrinho musical de Maria Rita.

Pois bem. Em 2023, a inteligência artificial permitiu que Maria Rita e Elis Regina cantassem juntas a música "Como nossos pais", de Belchior, num anúncio publicitário da Volkswagen, que comemorava 70 anos da filial brasileira.

O anúncio fez um estrondoso sucesso.

Ganhou muitos elogios, mas também severas críticas.

O filho mais velho de Elis, João Marcelo Bôscoli, elogiou o filme publicitário: "Ver Elis cantando ao lado da filha que ela não viu crescer, isso me comoveu muito".

O anúncio não informou ao consumidor que as imagens eram sintenizadas, criadas por inteligência artificial (IA). Tal omissão será analisada, em breve, pelo Conar (Conselho Nacional de Autorregulamentação Publicitária).

[...]

Adaptado de: Gagliano e Moraes (2023).

Saiba mais

Para ler o texto anterior na íntegra, acesse:

GAGLIANO, P. S.; MORAES, R. Inteligência artificial e os seus impactos no direito civil e no direito autoral. *Migalhas*, 25 jul. 2023. Disponível em: http://tinyurl.com/yetkksc8. Acesso em: 8 fev. 2024.

A legislação relacionada ao comércio eletrônico abrange questões como contratos online, proteção ao consumidor, direitos de devolução e regulamentações fiscais. Profissionais que operam lojas virtuais, vendem produtos ou serviços online ou realizam transações comerciais devem cumprir essas leis. A Lei do E-commerce, oficialmente denominada como Lei n. 12.965/2014, é mais conhecida no Brasil como o Marco Civil da Internet. Ela estabelece princípios, direitos e deveres para o uso da internet no país. A lei foi aprovada em 2014 e entrou em vigor em 23 de junho do mesmo ano.

O Marco Civil da Internet é uma legislação que visa definir as diretrizes e os regulamentos para a utilização da internet no Brasil, abordando questões como neutralidade da rede, privacidade, responsabilidade de provedores de internet e proteção de dados.

A coleta e o processamento de informações pessoais online são regulamentados por leis de privacidade de dados. Isso é especialmente relevante para profissionais de marketing digital, desenvolvedores de aplicativos e qualquer pessoa que lide com dados pessoais.

O Regulamento Geral de Proteção de Dados (GDPR) é uma legislação de proteção de dados que entrou em vigor na União Europeia (UE) em 25 de maio de 2018. Ele estabelece regras abrangentes para coleta, processamento e proteção de dados pessoais de indivíduos na UE, bem como para a transferência de dados pessoais para fora da UE. O GDPR visa proteger a privacidade dos cidadãos europeus e unificar as regulamentações de proteção de dados em toda a UE.

Os Estados Unidos não têm uma regulamentação de proteção de dados unificada como o GDPR, em parte devido à natureza descentralizada do sistema legal no país. No entanto, existem leis e regulamentos específicos relacionados à proteção de dados em setores específicos e em níveis estaduais. Por exemplo, a Lei de Proteção de Dados do Consumidor da Califórnia (California Consumer Privacy Act – CCPA) é uma das leis de privacidade mais abrangentes nos EUA e concede aos residentes da Califórnia certos direitos relacionados à privacidade de dados, incluindo saber quais dados pessoais estão sendo coletados e recusar a venda de seus dados.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em setembro de 2020, inspirada no GDPR. A LGPD estabelece princípios e regulamentações para o tratamento de dados pessoais, semelhantes aos do GDPR. Ela visa proteger a privacidade dos indivíduos e impõe obrigações às organizações que coletam, processam ou armazenam dados pessoais no país. A LGPD também inclui direitos para os titulares dos dados, como o direito de acesso, correção, exclusão e portabilidade dos dados pessoais. Assim como o GDPR, a LGPD impõe sanções significativas às organizações que não cumprem as regras.

Profissionais que geram ou compartilham conteúdo online, como blogueiros, jornalistas e influenciadores, devem estar cientes das leis de difamação, discurso de ódio e responsabilidade por conteúdo gerado pelo usuário.

Plataformas de redes sociais têm as próprias políticas e regulamentações. Profissionais que utilizam essas plataformas para fins comerciais, de publicidade ou de comunicação pública devem cumprir as diretrizes delas.

Os profissionais de tecnologia da informação e de segurança cibernética precisam entender as leis relacionadas a ataques cibernéticos, invasões de privacidade, proteção de dados e a obrigação de notificar incidentes de segurança. Os profissionais de marketing digital devem estar cientes das regulamentações de publicidade online, como o uso de anúncios direcionados e a transparência nas práticas de publicidade.

A legislação profissional também lida com a acessibilidade da internet e a discriminação online. É importante que profissionais de design de web e desenvolvimento de software garantam que seus produtos e serviços sejam acessíveis a todos, incluindo pessoas com deficiência. Além das leis, os

profissionais que trabalham na internet devem seguir padrões éticos. Isso inclui evitar práticas enganosas, respeitar a privacidade dos usuários e manter a integridade em suas ações online.

É fundamental que profissionais que atuam na internet estejam cientes das leis e regulamentações relevantes em sua área de atuação. A ignorância das leis não é uma desculpa aceitável em casos de violação. Além disso, à medida que a tecnologia e a legislação continuam a evoluir, é importante manter-se atualizado e adaptar as práticas profissionais conforme necessário para cumprir as regulamentações vigentes e conservar altos padrões éticos.

1.2 Legislação internacional

Lei Sarbanes-Oxley (SOX)

A Lei Sarbanes-Oxley, também conhecida como Sarbanes-Oxley Act (SOX) ou SOX Act, é uma legislação internacional de grande importância, principalmente para os Estados Unidos. Essa lei foi promulgada em 2002 em resposta a uma série de escândalos financeiros corporativos, como o colapso da empresa Enron e a fraude contábil na WorldCom. A SOX estabelece regulamentações rigorosas para melhorar a transparência, a integridade e a responsabilidade nas empresas de capital aberto nos Estados Unidos. Embora seja uma lei dos Estados Unidos, suas ramificações se estendem a empresas que têm ações listadas nas bolsas de valores dos EUA, independentemente de sua localização geográfica.

Principais pontos da SOX

Criação da PCAOB: a SOX estabeleceu a Public Company Accounting Oversight Board (PCAOB), uma organização independente responsável pela regulamentação e supervisão das empresas de auditoria que auditam sociedades de capital aberto.

Responsabilidade dos CEOs e CFOs: a lei torna os CEOs (*chief executive officers*) e os CFOs (*chief financial officers*) pessoalmente responsáveis pela precisão das informações financeiras divulgadas pela empresa. Eles devem certificar a exatidão dos relatórios financeiros.

Controles internos e procedimentos de auditoria: a SOX exige que as empresas estabeleçam e mantenham controles internos eficazes para garantir que suas informações financeiras sejam precisas. As auditorias internas são necessárias para verificar a autenticidade desses controles.

Retenção de documentos: a lei exige que as empresas mantenham registros e documentos financeiros por períodos específicos e proíbe a destruição de documentos financeiros de forma intencional.

Revisão independente: as empresas devem submeter seus controles internos a revisões independentes para garantir que estejam em conformidade com as regulamentações da SOX.

Denúncia de irregularidades: a SOX estabelece proteções aos denunciantes que relatam irregularidades financeiras em empresas publicamente negociadas. Os denunciantes são protegidos contra retaliação.

Exemplos de aplicações da SOX

A SOX tem sido fundamental na garantia de relatórios financeiros precisos e transparentes. Ela desempenhou um papel significativo na restauração da confiança dos investidores no mercado de capitais dos EUA após os escândalos corporativos da virada do milênio. A lei tornou os CEOs e CFOs mais responsáveis pela precisão das informações financeiras divulgadas pelas empresas. Isso reduziu o risco de práticas contábeis fraudulentas e incentivos para esconder informações financeiras.

A criação da PCAOB aumentou a supervisão das empresas de auditoria e melhorou a qualidade das auditorias financeiras. A SOX incentivou os funcionários a denunciar irregularidades financeiras sem temer retaliação, contribuindo para a identificação e resolução de problemas mais cedo. A lei promoveu melhor governança corporativa, com foco na transparência, na ética e na responsabilidade dos conselhos de administração e da gestão corporativa.

Embora a SOX tenha sido introduzida nos Estados Unidos, seus princípios de responsabilidade, transparência e governança corporativa influenciaram as práticas contábeis e regulatórias em todo o mundo. Empresas de capital aberto em todo o globo, mesmo aquelas que não estão listadas nas bolsas de valores dos EUA, muitas vezes adotam algumas práticas e padrões estabelecidos pela SOX para manter a confiança dos investidores e cumprir os requisitos regulatórios internacionais.

Regulamentações no Brasil

No Brasil, não existe uma lei exatamente equivalente à SOX, mas o país adotou medidas e regulamentações para melhorar a governança corporativa e a transparência das empresas listadas em bolsas de valores. Alguns aspectos das práticas de governança corporativa no país incluem:

- **Código de melhores práticas**: o Brasil tem um Código Brasileiro de Governança Corporativa, que designa recomendações e diretrizes para empresas cotadas na Bolsa de Valores de São Paulo (B3).

- **Regulamentações e agências**: a Comissão de Valores Mobiliários (CVM) é o órgão regulador do mercado de capitais no Brasil e desempenha um papel fundamental na regulamentação e fiscalização das empresas listadas. A CVM emitiu resoluções e regulamentações para promover a governança corporativa e a transparência.

- **Regras de contabilidade e auditoria**: as empresas devem seguir as normas contábeis internacionais (IFRS) e garantir auditorias independentes de suas demonstrações financeiras.

- **Responsabilidade dos gestores**: a legislação estabelece regras de responsabilidade para gestores de empresas listadas em bolsas de valores, e eles devem prestar contas a acionistas e reguladores.

As práticas de governança corporativa e as regulamentações do mercado de capitais brasileiras buscam promover a transparência, a responsabilidade e a confiança dos investidores nas empresas listadas. O país também tem entidades – como o Instituto Brasileiro de Governança Corporativa (IBGC) – que promovem princípios de governança corporativa em empresas brasileiras.

Saiba mais

Para entender melhor o caso da Enron, assista:

ENRON: os mais espertos da sala. Direção: Alex Gibney. Estados Unidos: Magnolia Pictures, 2005. 109 min.

1.3 Aspectos gerais no contexto histórico, social e econômico do Brasil

Direito pelo Estado

O direito pelo Estado pode ser interpretado de diferentes maneiras, mas geralmente se refere ao conjunto de leis e regulamentações criadas e aplicadas pelo governo ou Estado. Esse termo engloba a legislação e as regras que governam a sociedade e a vida das pessoas em determinada jurisdição.

O direito pelo Estado é derivado de várias fontes, incluindo a Constituição, as leis elaboradas pelo poder Legislativo, as regulamentações criadas por agências governamentais e os precedentes estabelecidos pelo Poder Judiciário. A Constituição é geralmente considerada a lei suprema em muitos sistemas legais e serve de base para toda legislação e regulamentação subsequentes.

O governo, por meio dos poderes Executivo e Judiciário, é responsável pela execução e aplicação das leis. Isso inclui a aplicação das leis para resolver disputas, garantir a ordem pública e proteger os direitos dos cidadãos.

Um dos principais papéis do direito pelo Estado é proteger os direitos e as liberdades dos cidadãos. Isso inclui direitos civis, como liberdade de expressão e igualdade perante a lei, e direitos econômicos e sociais, como o direito à educação e à saúde. O direito pelo Estado é utilizado para regular várias áreas, incluindo negócios, propriedade, contratos, relações trabalhistas, meio ambiente, comércio e muito mais. Ele define as regras e os padrões que as pessoas e as empresas devem seguir para garantir a ordem e o funcionamento adequado da sociedade.

O estado é responsável por garantir que as leis sejam aplicadas de maneira justa e consistente. Isso envolve a prestação de contas das autoridades públicas, garantindo que elas cumpram as leis e respeitem os direitos dos cidadãos. O direito pelo Estado não é estático e pode evoluir com o tempo para refletir as mudanças da sociedade e das necessidades dos cidadãos. Reformas legislativas e judiciais são frequentemente implementadas para abordar questões emergentes ou inadequações nas leis existentes.

As leis e regulamentações podem variar significativamente de um país para outro e, em alguns casos, até mesmo entre estados ou regiões de um país. Cada sistema legal é influenciado pela cultura, história e valores específicos da jurisdição em questão.

O direito pelo Estado é fundamental na organização da sociedade e na resolução de conflitos. É uma parte essencial da governança e da manutenção da ordem, fornecendo estruturas legais e mecanismos para proteger os direitos e interesses dos cidadãos e das instituições. Além disso, a evolução contínua do direito pelo Estado reflete as mudanças sociais e tecnológicas em curso e as necessidades da sociedade.

Lei de talião: "olho por olho, dente por dente"

A expressão "olho por olho, dente por dente" é um princípio da lei de talião, um conceito legal e moral que se refere à ideia de retribuição na mesma medida ou de punição proporcional pelo dano causado. A lei de talião é frequentemente associada a um sistema de justiça primitivo, em que a punição pelo crime ou ofensa cometida é diretamente relacionada ao dano infligido à vítima.

Figura 1 – Charge, de autor desconhecido, sobre a lei de talião

Disponível em: http://tinyurl.com/59eaxvsu. Acesso em: 14 fev. 2024.

O termo talião tem origem na palavra latina *talio*, que significa tal ou igual. A ideia por trás da lei de talião é que a punição deve ser equivalente à gravidade da ofensa. Ela é frequentemente expressa em termos de danos físicos, como a perda de um olho para alguém que tenha cegado outra pessoa ou a perda de um dente para alguém que tenha agredido outra pessoa.

A lei de talião foi historicamente aplicada em muitas sociedades antigas e é mencionada em textos antigos, incluindo o Código de Hamurabi, um antigo código de leis babilônico do século XVIII a.C. Ela também é mencionada na Bíblia, especificamente no Antigo Testamento, como parte da lei de Moisés. No entanto, a sua aplicação literal e estrita diminuiu ao longo do tempo.

Figura 2 – De acordo com a lei de talião, a punição deve ser proporcional ao crime cometido

Disponível em: https://tinyurl.com/3mtvv5rr. Acesso em: 14 fev. 2024.

Hoje em dia, a maioria das sociedades modernas adotou sistemas de justiça mais complexos e abrangentes, que levam em consideração uma série de fatores, como a intenção do agressor, as circunstâncias do crime, a reabilitação do infrator e a justiça para a vítima. A aplicação rigorosa da lei de talião, muitas vezes tida como vingança, é considerada desproporcional e contraproducente na maioria dos sistemas legais contemporâneos.

Em vez disso, o sistema legal moderno procura punir os infratores de maneira justa e equitativa, buscando também a proteção da sociedade e a reabilitação do infrator sempre que possível. Embora a lei de talião possa ter sido relevante em sociedades antigas e seja considerada um conceito de justiça primitiva, os sistemas de justiça atuais buscam soluções mais refinadas e justas para lidar com ofensas e crimes.

Na maioria das sociedades contemporâneas, o sistema de justiça é guiado por princípios mais complexos e humanitários, que vão além da simples retribuição física por uma ofensa. Embora a punição deva ser proporcional à gravidade do crime, a proporção pode ser interpretada de maneira mais abrangente.

Muitos sistemas legais buscam soluções que incluam a restauração e a reconciliação, quando apropriado, em vez de meramente impor punições. Ao invés de meramente penitenciar o infrator, os sistemas legais modernos frequentemente buscam reabilitar o infrator para que ele possa reintegrar-se à sociedade como um cidadão responsável.

A justiça moderna também se concentra na prevenção de futuros delitos, por meio de medidas como a reeducação e a supervisão de infratores. As vítimas também são consideradas no sistema legal atual, e medidas de proteção e apoio são implementadas para garantir que elas sejam tratadas com dignidade e consideração.

Embora a lei de talião possa ter sido um princípio primitivo de justiça, a evolução das normas éticas, morais e legais levou a sistemas de justiça mais sofisticados e humanitários, que buscam abordar os delitos de maneira mais equitativa e justa. No entanto, a expressão "olho por olho, dente por dente" ainda é usada metaforicamente para descrever a ideia de punição proporcional em alguns contextos.

Código Penal

O Código Penal é um conjunto de leis que estabelece os crimes, suas penas e regras gerais para o sistema de justiça criminal em uma jurisdição. Ele é uma parte fundamental do sistema legal de muitos países e desempenha um papel crucial na manutenção da ordem e na definição das condutas consideradas ilegais.

O Código Penal define os crimes, descrevendo em detalhes as condutas que são consideradas ilegais. Isso inclui uma ampla gama de ações, desde crimes contra a pessoa, como homicídio e agressão, até crimes contra a propriedade, como furto e roubo. Ele estabelece as penas e punições para cada crime. Isso pode incluir prisão, multas, liberdade condicional, serviço comunitário e outras formas de punição. As penas variam de acordo com a gravidade do crime e as circunstâncias envolvidas.

No Código Penal, geralmente há regras e procedimentos para a condução de processos criminais. Isso pode abranger questões como a investigação, a acusação, o julgamento e o recurso. Também pode conter disposições sobre defesas legais disponíveis para os acusados, como legítima defesa, insanidade ou consentimento da vítima.

O princípio da legalidade é um conceito fundamental no direito penal. Ele estabelece que uma pessoa somente pode ser condenada por um crime se sua conduta estiver claramente definida como criminosa em uma lei preexistente. Os códigos penais podem ser revisados e atualizados para refletir as mudanças na sociedade, na moral e na ética. Reformas podem incluir a descriminalização de certas condutas, a introdução de novos crimes ou a alteração das penas.

O Código Penal é uma parte do sistema de justiça criminal e envolve polícia, promotores, advogados de defesa, juízes e tribunais. Todos esses atores desempenham um papel na aplicação das leis penais e na garantia dos direitos dos acusados. O Código Penal também deve respeitar os direitos e as garantias dos acusados, incluindo o direito a um julgamento justo, o direito a permanecer em silêncio e o direito a um advogado.

Cada país pode ter o próprio Código Penal, adaptado às suas leis e tradições legais. Muitas vezes, os códigos penais são complementados por outras leis que abordam questões específicas, como o direito penal econômico, o direito penal ambiental e assim por diante.

É importante observar que o Código Penal é apenas uma parte do sistema legal mais amplo de um país e que a aplicação da lei e a administração da justiça também dependem de outros elementos, como a jurisprudência, a regulamentação e as práticas judiciais específicas de cada país.

Decreto-Lei n. 2.848, de 7 de dezembro de 1940

O **artigo 345** do Código Penal brasileiro, que é regido pelo Decreto-Lei n. 2.848, de 7 de dezembro de 1940, estabelece o seguinte:

> Art. 345 – Fazer justiça pelas próprias mãos, para satisfazer pretensão, embora legítima, salvo quando a lei o permite:
>
> Pena – detenção, de quinze dias a um mês, ou multa, além da pena correspondente à violência.
>
> Parágrafo único – Se não há emprego de violência, somente se procede mediante queixa (Brasil, 1940).

Esse artigo trata do crime de "fazer justiça pelas próprias mãos". Isso significa que alguém age de forma ilegal para satisfazer uma pretensão, mesmo que esta seja legítima. Em outras palavras, a pessoa comete um ato ilegal em busca de uma solução para um problema, em vez de recorrer ao sistema legal estabelecido.

Figura 3 – Ao fazer justiça com as próprias mãos, o cidadão está sujeito à aplicação da lei

Disponível em: https://tinyurl.com/fzccjv3c. Acesso em: 15 fev. 2024.

No entanto, o próprio artigo estabelece uma exceção: quando a lei permite a ação direta. Em alguns casos, a lei brasileira permite que os cidadãos tomem medidas legais por conta própria, como em legítima defesa, ou quando a própria lei prevê que determinada ação pode ser tomada diretamente pelas partes envolvidas.

Esse artigo visa manter a ordem e a aplicação da justiça por meio do sistema legal estabelecido, em vez de permitir que as pessoas tomem a lei em suas próprias mãos. Fazer justiça pelas próprias mãos é, muitas vezes, considerado ilegal e pode resultar em punições legais. Portanto, é importante que as pessoas busquem solucionar seus problemas por meio dos procedimentos legais disponíveis, em vez de recorrer à violência ou a ações ilegais.

Sistema jurídico

A resolução de conflitos é uma parte essencial do funcionamento de qualquer sociedade, e os sistemas jurídicos desempenham um papel importante nesse processo.

Figura 4 – As soluções para interesses individuais ou coletivos muitas vezes envolvem a intervenção do Estado por meio da jurisdição

Disponível em: https://tinyurl.com/4v9kbszm. Acesso em: 15 fev. 2024.

O contrato social é uma ideia fundamental na teoria política e jurídica. Ele representa um acordo implícito ou explícito entre os membros de uma sociedade, no qual as pessoas concordam em obedecer a certas regras e autoridades em troca de proteção e benefícios. Dentro desse contexto, a solução de conflitos é um dos principais serviços que o Estado se compromete a fornecer em troca da obediência dos cidadãos às leis e às autoridades.

Os conflitos podem surgir de várias fontes, como disputas contratuais, danos pessoais, disputas de propriedade, entre outros. Para resolver esses conflitos, as partes envolvidas geralmente recorrem à jurisdição, buscando a intervenção do Estado para obter uma solução justa e imparcial. O sistema judiciário é projetado para fornecer uma estrutura legal na qual essas disputas possam ser resolvidas.

O contrato social estabelece a base para a intervenção estatal na resolução de conflitos, e o sistema judiciário brasileiro fornece uma estrutura para as partes buscarem soluções legais para seus interesses individuais ou coletivos.

Lide e a intervenção do Estado

Lide é o termo jurídico que se refere a uma disputa ou um litígio entre duas partes que buscam uma solução legal. As partes envolvidas podem ingressar com uma ação em juízo para que o Estado intervenha e decida a questão. A ação em juízo é o processo pelo qual as partes apresentam seus argumentos, evidências e reivindicações perante um tribunal, a fim de obter uma decisão judicial.

Estrutura do sistema judiciário brasileiro

O sistema judiciário brasileiro é composto de três instâncias principais:

- **Primeira instância**: nesta fase, os casos são julgados por um juiz de primeira instância ou, em alguns casos, por um júri. Os tribunais de primeira instância estão localizados em fóruns regionais ou locais, onde a maioria dos casos começa a ser tratada.

- **Segunda instância**: quando uma das partes não concorda com a decisão da primeira instância, ela pode recorrer a uma instância superior, que é composta de desembargadores em tribunais estaduais (TJ – Tribunal de Justiça). Os tribunais de segunda instância revisam as decisões da primeira instância e, muitas vezes, aprofundam a análise jurídica dos casos.

- **Terceira instância**: é composta do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF). Esses tribunais lidam com casos que envolvem questões constitucionais e legais complexas. O STJ é responsável por questões infraconstitucionais, e o STF é a mais alta corte do país e lida com questões constitucionais.

A progressão da primeira instância para a segunda e a terceira instâncias permite que casos sejam revisados e decididos por diferentes níveis de autoridade judicial, garantindo um sistema de justiça robusto e imparcial.

Resolução de conflitos

A resolução de conflitos pode ocorrer de duas maneiras principais: por meio da solução consensual ou da solução litigiosa. Cada abordagem tem suas próprias características, vantagens e desvantagens, e a escolha entre elas depende das circunstâncias e preferências das partes envolvidas.

Na solução consensual, as partes em conflito chegam a um acordo por meio de negociação, mediação ou conciliação, sem a necessidade de um julgamento formal perante um tribunal. Nesse processo, as partes trabalham juntas para encontrar uma solução que seja mutuamente aceitável, muitas vezes com a ajuda de um terceiro imparcial, como um mediador.

As principais características da solução consensual são:

- **rapidez**: normalmente, a solução consensual é mais rápida do que a solução litigiosa, que pode envolver procedimentos legais demorados;
- **eficácia**: uma vez que as partes concordam voluntariamente com os termos do acordo, a solução consensual tende a ser mais eficaz na resolução do conflito e na restauração das relações entre as partes;
- **vantagens mútuas**: as partes têm a oportunidade de participar ativamente na criação de uma solução que atenda a seus interesses e necessidades específicas, muitas vezes resultando em um acordo mais vantajoso para ambos;
- **economia**: a solução consensual geralmente é mais econômica do que a solução litigiosa, uma vez que evita custos associados a litígios, como taxas legais, despesas de tribunal e tempo gasto em procedimentos judiciais.

A solução litigiosa envolve a resolução de conflitos por meio de um processo legal formal, em que as partes apresentam suas reivindicações perante um tribunal e aguardam a decisão do juiz. Isso pode ser necessário quando as partes não conseguem chegar a um acordo consensual ou quando há questões legais complexas que exigem a interpretação e aplicação da lei por um tribunal.

As principais características da solução litigiosa são:

- **formalidade**: a solução litigiosa segue procedimentos legais formais, incluindo a apresentação de petições, a realização de audiências e a produção de provas, tornando-a um processo mais demorado e caro;
- **decisão do tribunal**: em última instância, a solução litigiosa resulta em uma decisão imposta pelo tribunal, independentemente das preferências das partes envolvidas;
- **conflito público**: os detalhes do litígio são geralmente públicos e acessíveis a terceiros, o que pode afetar a privacidade das partes e as relações interpessoais.

Ambas as abordagens têm seu lugar e utilidade, dependendo da natureza do conflito, das necessidades das partes e das circunstâncias. Muitas vezes, a solução consensual é preferida devido à rapidez, à eficácia e à capacidade de promover relacionamentos positivos entre as partes envolvidas. No entanto, em alguns casos, a solução litigiosa pode ser necessária para resolver disputas complexas ou quando as partes não conseguem chegar a um acordo de boa-fé.

Fontes do direito

A palavra fonte significa lugar de onde a água surge, nasce ou jorra.

Figura 5 – Fonte de água em um jardim

Disponível em: https://tinyurl.com/3zvc9kcz. Acesso em: 6 fev. 2024.

As principais fontes do direito são os meios pelos quais as normas jurídicas são criadas, estabelecidas e reconhecidas em um sistema jurídico. Essas fontes servem de base para a formação do ordenamento jurídico de um país ou de uma jurisdição específica. Elas podem variar de acordo com o sistema jurídico de cada país; algumas das fontes são:

- **Lei**: as leis são um dos pilares fundamentais do direito em muitos sistemas jurídicos. Elas são normas escritas vigentes em um país e formalmente promulgadas pelo poder legislativo (parlamento ou congresso), e têm autoridade legal para regular uma ampla gama de questões. As leis podem ser codificadas, como códigos civis e penais, ou não codificadas, como leis específicas ou estatutos. A vigência de uma lei é de, geralmente, 45 dias depois de publicadas no DOU; as leis estabelecem, no próprio texto, o prazo inicial de sua vigência.

- **Constituição**: é a lei fundamental de um país e estabelece a estrutura do governo, os direitos fundamentais dos cidadãos e os princípios gerais que regem a nação. Ela tem precedência sobre outras leis e é a norma suprema em um sistema jurídico.

- **Costumes**: são práticas tradicionais e repetidas na sociedade que são reconhecidas como normas jurídicas. Em alguns sistemas jurídicos, os costumes desempenham um papel importante na formação do direito, especialmente quando não há leis escritas sobre determinados assuntos. Exemplo: a fila.

- **Princípios gerais de direito**: inspiram o sistema jurídico na elaboração das leis ou na decisão que deverá ser tomada em um conflito de interesses. Exemplo: princípio da boa-fé, presente em todas as relações de negócios; honestidade e transparência nas relações pessoais e profissionais.

- **Jurisprudência**: refere-se às decisões de tribunais em casos anteriores. As decisões judiciais podem criar precedentes legais que servem de orientação para casos futuros e ajudam a interpretar a lei.

- **Doutrina**: inclui escritos de juristas, acadêmicos e comentaristas legais que analisam e interpretam as leis e a jurisprudência. Embora a doutrina em si não tenha força legal, ela pode influenciar a interpretação e a aplicação das leis pelos tribunais e legisladores.

Figura 6

Disponível em: https://tinyurl.com/c4f6fnmm. Acesso em: 6 fev. 2024.

- **Tratados internacionais**: em sistemas jurídicos que reconhecem o direito internacional, os tratados celebrados entre países podem ser fontes importantes do direito, desde que sejam ratificados e promulgados em conformidade com as leis nacionais.

Essas são algumas das principais fontes do direito, e a importância de cada fonte pode variar de acordo com o sistema jurídico do país e a natureza do assunto em questão. Além disso, é importante observar que as fontes do direito podem interagir e influenciar umas às outras no processo de formação e aplicação das normas jurídicas.

Princípios jurídicos

Os princípios jurídicos são conceitos fundamentais e diretrizes gerais que informam a interpretação, aplicação e desenvolvimento do Direito. Eles desempenham um papel importante na construção e na coerência do, orientando os juízes, advogados e legisladores na tomada de decisões legais e na resolução de casos complexos. Os princípios jurídicos são uma parte essencial do Direito, pois contribuem para a justiça, a equidade e a previsibilidade das decisões legais.

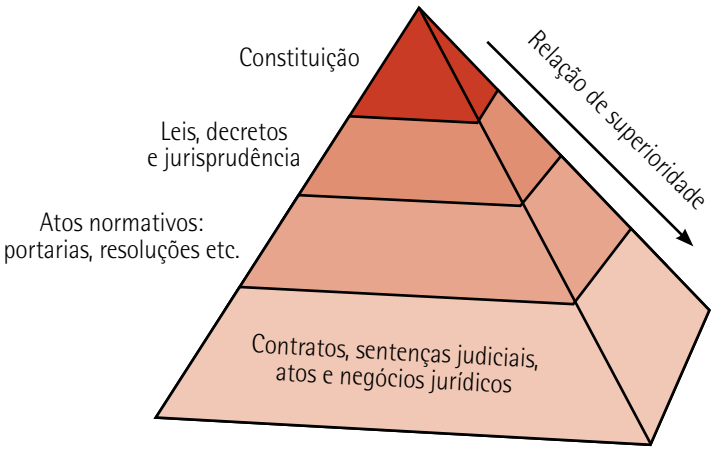

Figura 7 – Ordenamento jurídico

Podemos listar algumas características e aspectos importantes dos princípios jurídicos:

- **Abstração e generalidade**: são formulados de maneira geral e abstrata, o que significa que eles não são regras específicas e detalhadas, mas sim diretrizes amplas que se aplicam a uma variedade de situações legais. Isso permite que eles sejam flexíveis e adaptáveis a diferentes contextos.

- **Hierarquia**: alguns podem ter uma posição hierárquica superior em relação a outros no sistema jurídico. Por exemplo, a Constituição de um país pode estabelecer princípios fundamentais que têm precedência sobre leis ordinárias.

- **Fontes de interpretação**: desempenham um papel importante na interpretação da lei. Quando a lei é ambígua ou lacunosa, os tribunais podem recorrer aos princípios para ajudar a esclarecer o significado e a aplicação da norma legal.

- **Coerência e integração**: contribuem para a coesão e a consistência do sistema jurídico. Eles ajudam a evitar contradições e conflitos entre as normas legais e a garantir que o Direito seja aplicado de maneira justa e equitativa.

- **Orientação moral e ética**: muitos refletem valores morais e éticos, como a justiça, a equidade, a liberdade, a igualdade e a dignidade humana. Eles servem de guias para a tomada de decisões legais que estejam em conformidade com os valores fundamentais da sociedade.

- **Evolução e adaptação**: podem evoluir ao longo do tempo para refletir as mudanças na sociedade, na moral e na cultura. Isso permite que o direito seja relevante e responsivo às necessidades em constante mudança.

Exemplos de princípios jurídicos comuns incluem o devido processo legal, a presunção de inocência, o direito à igualdade perante a lei, a proteção dos direitos humanos, o princípio da legalidade e muitos

outros. Esses princípios desempenham um papel vital na defesa dos direitos e das liberdades dos indivíduos e na garantia de um sistema jurídico justo e equitativo.

É importante notar que a interpretação e a aplicação dos princípios jurídicos podem variar entre jurisdições e ao longo do tempo, e muitas vezes são objeto de debates jurídicos e filosóficos.

Princípio da legalidade

O princípio da legalidade é um dos princípios jurídicos fundamentais em muitos sistemas legais, incluindo o sistema legal brasileiro e diversos outros em todo o mundo. Esse princípio estabelece que o exercício do poder estatal, seja ele legislativo, executivo ou judiciário, está limitado e condicionado pela lei. Em resumo, significa que ninguém pode ser obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei.

Figura 8 – A importância do princípio da legalidade reside na garantia de que o Estado e seus agentes só podem agir dentro dos limites estabelecidos pela lei

Disponível em: https://tinyurl.com/mvkjevkr. Acesso em: 15 fev. 2024.

O princípio da legalidade garante que as normas e regras que regulam a conduta dos cidadãos e a atuação do Estado sejam claras, acessíveis e previsíveis. Isso promove a segurança jurídica, permitindo que as pessoas conheçam seus direitos e obrigações de acordo com a lei.

Este princípio atua como um freio ao poder do Estado. Isso significa que o governo e suas autoridades somente podem agir quando a lei expressamente os autoriza. Qualquer ação governamental que não esteja em conformidade com a lei pode ser contestada e anulada. O princípio da legalidade impede que o Estado e seus agentes ajam de forma arbitrária, ou seja, sem base legal sólida. Isso protege os cidadãos contra abusos de poder e garante que a atuação do Estado seja justa e equitativa.

O devido processo legal é uma extensão do princípio da legalidade e garante que qualquer pessoa que esteja sujeita a um processo legal tenha seus direitos respeitados e seja tratada de acordo com a lei. Isso inclui o direito a um julgamento justo e imparcial. O princípio da legalidade também se aplica ao direito penal, estabelecendo que ninguém pode ser condenado ou punido criminalmente senão em virtude de lei. Isso significa que a lei deve definir claramente quais comportamentos são considerados crimes e estabelecer as penas correspondentes.

Embora o princípio da legalidade exija que o Estado aja de acordo com a lei, ele não impede que as leis sejam alteradas e adaptadas ao longo do tempo para refletir as mudanças na sociedade. A alteração da lei deve ser feita de acordo com procedimentos legais estabelecidos.

O princípio da legalidade é um dos pilares do Estado de direito e desenvolve um papel fundamental na garantia dos direitos e liberdades dos indivíduos e na limitação do poder estatal. Ele assegura que o Estado atue de forma justa, equitativa e dentro dos limites estabelecidos pela lei.

Princípio da moralidade

O princípio da moralidade é um dos princípios fundamentais do direito administrativo, um ramo do direito que trata da organização, do funcionamento e da atuação da administração pública. Esse princípio estabelece que a administração pública deve pautar suas ações e decisões não apenas pela legalidade, mas também pela moral e pela ética. Em outras palavras, a administração pública deve agir de acordo com padrões éticos e morais elevados, além de cumprir as leis.

O princípio da moralidade não está em oposição à legalidade, mas é complementar a ela. Enquanto a legalidade se concentra na conformidade estrita com as leis e regulamentos, a moralidade vai além, exigindo que a administração pública aja de maneira justa, honesta e ética, mesmo quando as ações estejam dentro dos limites legais.

O princípio da moralidade desempenha um papel importante no combate à corrupção e ao nepotismo. Ele impede que agentes públicos utilizem sua posição para obter benefícios pessoais indevidos ou favorecer amigos e familiares em detrimento do interesse público.

A moralidade na administração pública está ligada à transparência e à responsabilização. As ações e decisões da administração pública devem ser transparentes e sujeitas à fiscalização, de modo que a sociedade possa avaliar se os princípios éticos estão sendo respeitados.

O princípio da moralidade visa garantir que as ações da administração pública estejam alinhadas ao interesse público e não sejam prejudiciais à sociedade como um todo. Tal princípio limita a discricionariedade dos agentes públicos, impedindo que eles tomem decisões arbitrárias ou injustas, mesmo quando a lei lhes confere margem de manobra. Também enfatiza a necessidade de que a administração pública seja conduzida de acordo com princípios éticos, respeitando os direitos e interesses dos cidadãos, evitando práticas discriminatórias e promovendo a igualdade.

Embora o princípio da moralidade seja essencial no contexto do direito administrativo, sua interpretação e aplicação podem ser subjetivas e variar de acordo com a cultura e os valores da sociedade em questão. O equilíbrio entre a legalidade e a moralidade na administração pública é uma questão complexa, e muitas vezes é objeto de debates e discussões na esfera jurídica e política. No entanto, a observância desse princípio é fundamental para promover a integridade, a justiça e a confiança na administração pública.

Peter Ferdinand Drucker (1909-2005) foi um influente escritor, consultor de gestão e educador austríaco-americano, considerado o pai da administração moderna e um dos pensadores mais importantes no campo da gestão e administração de empresas no século XX. Ele é conhecido por suas contribuições significativas para o desenvolvimento das teorias de administração e por sua influência na prática de gestão em organizações em todo o mundo. Drucker escreveu mais de 30 livros sobre administração, gestão de organizações e temas relacionados. Sua obra mais famosa é provavelmente o livro *The Practice of Management* (A prática da administração), publicado em 1954. Ele também escreveu sobre liderança, inovação, eficácia organizacional e responsabilidade social das empresas.

Uma de suas frases mais famosas é: "O que os administradores precisam, para serem aceitos como autoridade legítima, é um princípio de moralidade" (Drucker *apud* Villamarín, 2002, p. 24).

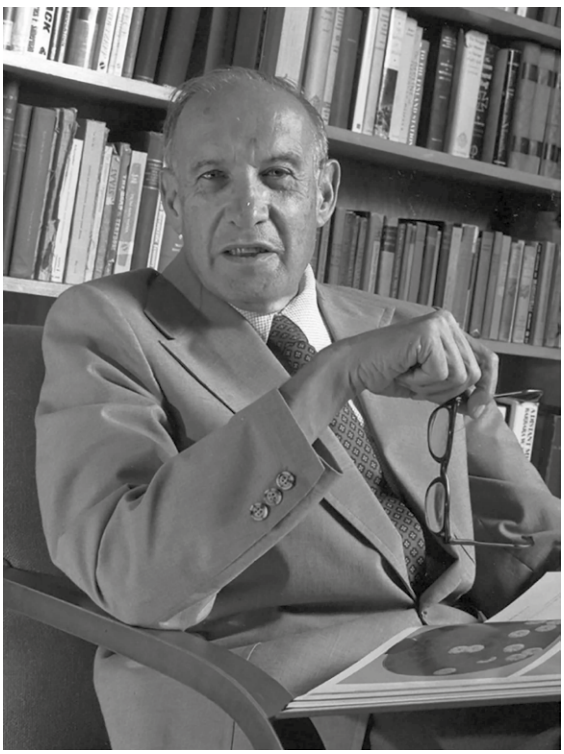

Figura 9 – Peter Drucker, pai da administração moderna

Disponível em: https://tinyurl.com/ynw4f2cd. Acesso em: 16 fev. 2024.

Saiba mais

Recomendamos assistir aos filmes:

ANON. Direção: Andrew Niccol. Reino Unido/Canadá/Alemanha/Estados Unidos: Netflix, 2018. 100 min.

Como você lidaria com a ideia de saber que alguém está vigiando você o tempo todo? Essa é a sociedade distópica do filme *Anon*. Por um lado, isso garante que nenhum crime aconteça. Por outro, a privacidade deixa de existir.

O filme narra a história de Sal Frieland, um detetive que investiga o caso de uma moça que conseguiu burlar todo o sistema e se manter em anonimato.

Essa é uma ótima obra para refletir sobre os limites do desenvolvimento e da segurança digital, além da necessidade de privacidade de dados.

JOBS. Direção: Joshua Michael Stern. Estados Unidos: Open Road Films, 2013. 129 min.

Que tal conhecer um pouco mais da história da personalidade que olhou para o futuro e deu início a uma das empresas mais conhecidas da atualidade? Estamos falando de Steve Jobs, fundador da Apple e um dos maiores CEOs da história.

Estrelado por Ashton Kutcher, o filme conta a trajetória do empreendedor que deu início ao negócio na garagem de casa. Além disso, a obra dirigida por Joshua Michael Stern apresenta os contratempos encontrados pelo protagonista para conciliar a vida pessoal e a profissional.

No filme, é possível ver também a relação de Jobs com o amigo e primeiro sócio, Steve Wozniak, interpretado por Josh Gad.

Princípio da publicidade

O princípio da publicidade, no contexto do direito e da administração pública, refere-se à obrigação de que os atos e decisões dos órgãos e entidades governamentais sejam transparentes e acessíveis ao público. Em outras palavras, esse princípio estabelece que a administração pública deve conduzir suas ações de forma aberta e disponibilizar informações sobre suas atividades, decisões e processos para que os cidadãos tenham acesso e possam fiscalizar o governo.

Figura 10 – A Lei de Acesso à Informação brasileira foi criada em 2012

Disponível em: https://tinyurl.com/6mum3kmv. Acesso em: 16 fev. 2024.

A publicidade visa promover a transparência na administração pública, permitindo que os cidadãos, a sociedade civil e a mídia tenham conhecimento das ações, gastos e políticas governamentais. Isso ajuda a prevenir a corrupção, a falta de responsabilidade e o abuso de poder. O princípio da publicidade está relacionado ao direito dos cidadãos de ter acesso a informações relevantes sobre a atuação do governo. Muitos países têm leis de acesso à informação que garantem esse direito e estabelecem procedimentos para solicitar informações públicas.

A publicidade é uma ferramenta fundamental para a responsabilização (*accountability*) dos agentes públicos. Quando as ações do governo são públicas, torna-se mais fácil para os cidadãos e órgãos de controle avaliarem se os agentes públicos estão atuando de maneira ética e de acordo com os interesses públicos. A publicidade ajuda a legitimar as decisões do governo, uma vez que o público pode entender o processo decisório e os motivos por trás das políticas públicas. Isso contribui para a aceitação das decisões governamentais pela sociedade.

Embora a publicidade seja um princípio importante, existem limites em relação à divulgação de informações governamentais. Por exemplo, questões de segurança nacional, privacidade e sigilo podem justificar restrições à publicidade em certos casos. Conforme a Constituição Federal (CF), no artigo 5º, incisos X e XXXIII, algumas informações não são acessíveis, encontrando-se em segredo por duas razões: em caso de violação da intimidade das pessoas e quando imprescindíveis para a segurança da sociedade ou do Estado.

[...]

X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

[...]

XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado [...] (Brasil, 1988).

Figura 11 – As informações relacionadas à intimidade de pessoas e à segurança nacional não podem ser divulgadas

Disponível em: https://tinyurl.com/533nxbbz. Acesso em: 16 fev. 2024.

A publicidade pode ser alcançada por meio de diferentes meios de comunicação, como sites governamentais, relatórios anuais, audiências públicas, redes sociais e divulgação de informações em órgãos de imprensa. A escolha dos meios varia de acordo com a jurisdição e a natureza das informações a serem divulgadas.

O princípio da publicidade desempenha um papel fundamental na promoção da democracia, na garantia dos direitos dos cidadãos e na construção da confiança na administração pública. Ele é parte integrante do Estado de direito e ajuda a equilibrar o poder do governo, assegurando que as ações do Estado estejam sujeitas à supervisão pública e ao escrutínio.

Sociedade digital

A sociedade digital refere-se à transformação da sociedade e da vida cotidiana impulsionada pelo uso crescente das tecnologias digitais, principalmente a internet. Esse fenômeno tem se intensificado nas últimas décadas, à medida que a conectividade online se tornou mais ubíqua e acessível. A sociedade

digital tem impactos significativos em diversas áreas, incluindo comunicação, economia, educação, política, cultura e privacidade.

A internet e as redes sociais têm permitido que as pessoas estejam conectadas em tempo real, independentemente de sua localização geográfica. Isso facilita a comunicação, a colaboração e o compartilhamento de informações em escala global.

Vivemos em uma era de dados, onde a sociedade digital gera enormes quantidades de informações todos os dias, que são coletadas, armazenadas e analisadas. Esses dados têm grande valor para empresas, governos e instituições, ajudando a moldar decisões e estratégias.

O acesso a tantos dados pessoais levanta questões sobre privacidade e segurança. Por exemplo, muitas vezes os usuários precisam ceder informações pessoais para usar serviços online. Isso gera preocupações.

Figura 12 – Os dados que compartilhamos na internet deixam rastros, que podem ser usados por pessoas mal-intencionadas

Disponível em: https://tinyurl.com/2bhk48ru. Acesso em: 16 fev. 2024.

Quando utilizamos o WhatsApp e aceitamos os termos de uso, damos acesso ao histórico do aplicativo e do dispositivo, à localização, aos contatos etc. Ao aceitarmos os termos de uso de um aplicativo, realizamos uma contratação eletrônica, assinando um contrato de adesão, que aborda questões de segurança e privacidade dos dados. Dessa forma, estamos sujeitos, por exemplo, às leis brasileiras, como o Código de Defesa do Consumidor (CDC), o Código Civil (CC), o Código Penal (CP), o direito internacional privado, entre outros.

A sociedade digital impulsionou o crescimento de indústrias relacionadas à tecnologia, como o comércio eletrônico, a publicidade online, a tecnologia financeira (fintech) e a economia de compartilhamento. Essas indústrias têm transformado a economia global. A tecnologia digital tem mudado a forma como as pessoas adquirem conhecimento e acessam informações. Plataformas de ensino online, tutoriais em vídeo e recursos digitais estão disponíveis.

Empresas como o Facebook têm planos de conectar 4 bilhões de pessoas até 2026. O uso de tecnologias de IA se torna cada vez mais frequente na análise e processamento de dados, e as redes sociais geram oportunidades como:

- novos métodos de trabalho;
- agilidade dos processos;
- aumento de negócios;
- maior interação com consumidores;
- facilidade de comunicação com clientes;
- acesso irrestrito à informação.

A sociedade digital também tem papel nas esferas política e cívica. As redes sociais e as plataformas online têm sido usadas para mobilização social, conscientização política e engajamento cívico. Embora a sociedade digital tenha trazido benefícios, também aprofundou as desigualdades digitais. Nem todos têm acesso igual às tecnologias digitais, criando divisões sociais, econômicas e educacionais.

Com a sociedade digital, surgem questões éticas, como a disseminação de notícias falsas, a manipulação de informações, o cyberbullying e a responsabilidade das empresas de tecnologia em relação ao conteúdo em suas plataformas. A sociedade digital é caracterizada pela constante inovação tecnológica. Novas tecnologias, como inteligência artificial, blockchain e realidade virtual, continuam a moldar a maneira como vivemos, trabalhamos e nos relacionamos.

À medida que a sociedade digital continua a evoluir, é importante que indivíduos, empresas e governos estejam cientes dos desafios e das oportunidades. A proteção da privacidade, a promoção da igualdade de acesso à tecnologia e a responsabilidade digital são questões importantes que merecem atenção na era da sociedade digital.

Quais são os impactos do mundo digital?

O mundo digital tem impactado profundamente várias esferas da sociedade. Esses impactos podem ser tanto positivos quanto desafiadores, e refletem a transformação contínua que a tecnologia digital trouxe à forma como vivemos, trabalhamos e nos relacionamos. Alguns dos principais impactos da era digital são:

- **Vazamento de informações**: a facilidade de compartilhar informações online torna as empresas mais suscetíveis a vazamentos de dados. Isso pode prejudicar a confiança dos clientes e causar danos financeiros.

- **Falta de ética dos colaboradores no acesso aos dados**: o acesso a dados sensíveis pode levar a problemas de ética se os colaboradores abusarem dessa autorização. A implementação de políticas rigorosas de segurança da informação é fundamental para minimizar esse risco.

- **Dificuldade de gerenciamento das informações**: a crescente quantidade de dados digitais pode tornar desafiador para as organizações gerenciar, armazenar e acessar informações de maneira eficaz. A gestão de dados se tornou uma preocupação crítica nas empresas.

- **Atendimento ao consumidor exigindo respostas rápidas**: na era digital, os consumidores esperam respostas rápidas e eficazes às suas interações. Isso exige que as empresas adotem estratégias de atendimento ao cliente que integrem canais online e offline.

- **Questões relacionadas à privacidade dos dados**: o aumento da coleta e do compartilhamento de dados pessoais levanta questões sobre a privacidade. Regulamentações, como a LGPD, foram implementadas para proteger a privacidade dos indivíduos.

- **Segurança das informações**: a segurança das informações se tornou uma prioridade, uma vez que ciberataques e ameaças cibernéticas representam riscos significativos para empresas e governos. A proteção de sistemas e redes é fundamental para evitar violações de segurança.

- **Direito de imagem**: a disseminação de conteúdo visual online levanta questões sobre o direito de imagem, especialmente em relação à divulgação de fotos e vídeos de pessoas sem seu consentimento. O uso indevido de imagens pode resultar em violações legais.

- **Propriedade intelectual**: a facilidade de compartilhamento online também tornou a propriedade intelectual mais vulnerável à violação de direitos autorais e à pirataria. Isso afeta a indústria criativa, como música, cinema e publicações.

A era digital trouxe consigo benefícios significativos, mas também desafios complexos, especialmente no que diz respeito à segurança, ética e privacidade. Lidar com esses desafios requer a implementação de políticas adequadas, regulamentações eficazes e a conscientização tanto dos indivíduos quanto das organizações sobre as responsabilidades associadas ao uso de tecnologia e à gestão de informações.

1.4 Estudos de caso

Smart city

Uma *smart city* (ou cidade inteligente) utiliza tecnologia e inovação para melhorar a qualidade de vida de seus habitantes, promover o desenvolvimento sustentável e aumentar a eficiência na prestação de serviços públicos. *Smart cities* buscam utilizar dados e tecnologia para enfrentar desafios urbanos, como congestionamento de tráfego, poluição, uso ineficiente de recursos e serviços públicos ineficientes.

Prefeitura de Londres

A Prefeitura de Londres proibiu a empresa Renew de coletar informações de smartphones por meio de suas lixeiras inteligentes, um incidente que lançou luz sobre questões de privacidade e vigilância nas cidades modernas.

Figura 13 – Exemplo de lixeira inteligente

Disponível em: http://tinyurl.com/2vhx62s2. Acesso em: 19 fev. 2024.

As latas de lixo inteligentes, que foram instaladas antes das Olimpíadas de 2012, foram projetadas para coletar informações dos dispositivos móveis de pedestres que estivessem com o Wi-Fi ligado. A empresa Renew afirmava que essa coleta de dados tinha o propósito de ajudar parceiros a produzir publicidade direcionada, visando oferecer aos cidadãos anúncios mais relevantes.

No entanto, o que gerou grande controvérsia foi que as pessoas que passavam perto das lixeiras inteligentes não tinham conhecimento da finalidade desses dispositivos e, portanto, não davam seu consentimento para que seus dados fossem coletados para fins publicitários e de marketing. Isso levantou questões significativas relacionadas à privacidade, ao consentimento e à transparência no uso de tecnologia de coleta de dados nas cidades.

A coleta de dados sem o consentimento dos cidadãos levanta preocupações éticas e legais sobre a vigilância em ambientes urbanos. A privacidade dos cidadãos deve ser protegida, e eles precisam ser informados sobre como seus dados serão usados e ter a opção de consentir ou recusar a coleta.

O incidente também destaca a importância de regulamentações e políticas claras relacionadas ao uso de tecnologias de vigilância e coleta de dados em espaços públicos. Cidades inteligentes podem

se beneficiar de soluções inovadoras, mas devem garantir que essas soluções respeitem os direitos e a privacidade dos cidadãos.

Em resposta a essas preocupações, a Prefeitura de Londres agiu de forma proativa, proibindo a prática de coleta de dados por meio de lixeiras inteligentes. Esse episódio serve de lembrete da necessidade de equilibrar a inovação tecnológica com a proteção da privacidade e dos direitos dos cidadãos em ambientes urbanos cada vez mais conectados.

Telemarketing, e-mails promocionais e videovigilância

O registro de queixas relacionadas a telemarketing, e-mails promocionais e videovigilância destaca as crescentes preocupações dos cidadãos com a privacidade e o uso de suas informações pessoais.

- **Telemarketing**: as queixas relacionadas ao telemarketing geralmente se referem a chamadas não solicitadas de empresas que tentam vender produtos ou serviços. Muitos cidadãos optam por se inscrever em listas de "não perturbe" ou "não ligue" para evitar esse tipo de abordagem intrusiva. A falta de conformidade com as regulamentações de telemarketing, como a obrigação de obter consentimento prévio para fazer chamadas de marketing, pode levar a um aumento nas queixas.

- **E-mails promocionais**: o envio de e-mails promocionais não solicitados, também conhecidos como spam, é uma fonte constante de irritação para os consumidores. Regulamentações, como a LGPD, estabelecem diretrizes estritas sobre o uso de informações pessoais para fins de marketing por e-mail. A falta de transparência, a ausência de opções de cancelamento de inscrição e o compartilhamento de dados sem consentimento são questões comuns que podem resultar em queixas.

- **Videovigilância**: a videovigilância em locais públicos é uma ferramenta importante para a segurança, mas também levanta questões sobre privacidade. A instalação de câmeras de vigilância em espaços públicos deve ser realizada com transparência e de acordo com regulamentações específicas. Queixas relacionadas à videovigilância geralmente se concentram na coleta excessiva de imagens e na falta de divulgação adequada.

Os cidadãos têm o direito de serem informados sobre como seus dados serão usados, dar consentimento explícito para o uso de suas informações e ter a capacidade de retirar esse consentimento a qualquer momento. Além disso, têm o direito de solicitar o acesso às informações que as organizações mantêm sobre eles e o direito de serem esquecidos, ou seja, terem seus dados excluídos.

Essas queixas destacam a importância da proteção da privacidade e do controle sobre informações pessoais em um mundo cada vez mais digital. As regulamentações de privacidade são essenciais para garantir que as empresas e organizações respeitem os direitos dos cidadãos e usem dados pessoais de maneira responsável. Além disso, evidenciam a necessidade de conscientização e educação contínuas para que os cidadãos entendam seus direitos e como exercê-los em um ambiente digital em constante evolução.

2 MARCO CIVIL DA INTERNET

No Brasil, o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Ele aborda questões como neutralidade da rede, privacidade e responsabilidade dos provedores de serviços.

Leis de propriedade intelectual

Profissionais de TI frequentemente lidam com a criação e implementação de software. Portanto, é crucial compreender as leis de propriedade intelectual, que incluem direitos autorais, patentes e marcas registradas, para proteger o trabalho desenvolvido.

Segurança da informação e cibercrimes

A segurança da informação é uma área crítica para profissionais de TI. As leis relacionadas a cibercrimes e segurança cibernética variam, mas é essencial conhecer regulamentações específicas para denunciar incidentes e adotar práticas que garantam a proteção contra ameaças digitais.

Contratos de trabalho e terceirização

Aspectos legais relacionados a contratos de trabalho, terceirização e direitos trabalhistas são fundamentais para os profissionais de TI. Contratos devem definir claramente as responsabilidades e direitos das partes envolvidas.

Ética profissional

Embora não seja uma legislação específica, a ética profissional é um aspecto legal implícito. Profissionais de TI devem aderir a padrões éticos, evitando práticas antiéticas que possam resultar em consequências legais.

Conformidade com padrões e certificações

A conformidade com padrões da indústria e certificações específicas, como ISO 27001 para segurança da informação, não apenas promove boas práticas, mas também pode ser requisito legal em alguns setores.

Desafios atuais

Profissionais de TI enfrentam desafios para manter-se atualizados com as rápidas mudanças nas leis e regulamentações, especialmente em um ambiente globalizado onde as práticas de governança de dados e segurança variam.

A compreensão e a conformidade com os aspectos legais são cruciais para o profissional de TI, pois garantem a integridade, a segurança e a legalidade de suas atividades. Manter-se informado sobre as leis pertinentes e buscar atualizações regulares são práticas essenciais para o sucesso nesse campo dinâmico e altamente regulamentado.

O Marco Civil da Internet é uma lei brasileira que estabelece princípios, garantias, direitos e deveres relacionados ao uso da internet no país. Foi sancionado em abril de 2014 e é conhecido formalmente como Lei n. 12.965/2014. Trata-se de uma das legislações mais importantes do mundo em termos de regulamentação da internet e serve como um marco regulatório para a governança da rede no Brasil.

Figura 14 – Sessão de votação do Marco Civil da Internet na Câmara dos Deputados

Disponível em: https://tinyurl.com/3tfsj2ht. Acesso em: 19 fev. 2024.

2.1 Noções sobre a Lei n. 12.965/2014

A Lei n. 12.965/2014 estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

> [...]
>
> Art. 5º Para os efeitos desta Lei, considera-se:
>
> I – internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
>
> [...]
>
> VII – aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;
>
> [...]
>
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

[...]

VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

[...]

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (Brasil, 2014).

Decreto n. 8.771, de 11 de maio de 2016

O Decreto n. 8.771, de 11 de maio de 2016, é um ato normativo que regulamenta partes do Marco Civil da Internet (Lei n. 12.965/2014) relacionadas à neutralidade da rede, o princípio que garante que todos os dados trafegados na internet devem ser tratados de forma igualitária, sem discriminação, priorização ou bloqueio injustificado.

A regulamentação do Marco Civil da Internet era aguardada para fornecer diretrizes mais específicas sobre a aplicação do princípio da neutralidade da rede, bem como outros aspectos da lei. O Decreto n. 8.771/2016 estabelece diversas regras e princípios relacionados à neutralidade da rede e à proteção dos direitos dos usuários da internet.

O decreto reforça a proibição de discriminação de tráfego na internet, garantindo que os provedores de acesso à internet tratem todos os pacotes de dados da mesma forma, independentemente de seu conteúdo, origem, destino ou serviço. Os provedores são autorizados a gerenciar o tráfego em suas redes para garantir sua estabilidade e segurança, desde que isso seja feito de maneira transparente, proporcional e sem discriminação.

O decreto permite que os provedores de acesso à internet ofereçam diferentes planos e serviços com base na velocidade de conexão, franquia de dados e outros critérios comerciais, desde que isso seja feito de maneira transparente e não viole os princípios da neutralidade da rede.

Os provedores de acesso à internet são obrigados a fornecer informações claras e transparentes sobre as características dos serviços oferecidos, incluindo velocidade de conexão, franquias de dados, termos de uso e políticas de gerenciamento de rede. O decreto proíbe o bloqueio de aplicativos e conteúdo de forma arbitrária, garantindo que os usuários possam acessar os serviços e aplicativos de sua escolha, desde que estejam em conformidade com a lei.

O decreto reforça a importância da proteção da privacidade dos usuários, especialmente no que diz respeito a coleta, uso e armazenamento de dados pessoais.

O Decreto n. 8.771/2016 tem como objetivo fornecer diretrizes mais detalhadas e claras sobre como a neutralidade da rede e outros princípios do Marco Civil da Internet devem ser aplicados na prática. Ele desempenha um papel fundamental na regulamentação da internet no Brasil, promovendo a liberdade, a igualdade e a proteção dos direitos dos usuários da rede:

> [...]
>
> Art. 2º O disposto neste Decreto se destina aos responsáveis pela transmissão, pela comutação ou pelo roteamento e aos provedores de conexão e de aplicações de internet, definida nos termos do inciso I do caput do art. 5º da Lei n. 12.965, de 2014.
>
> [...]

> Capítulo III
>
> DA PROTEÇÃO AOS REGISTROS, AOS DADOS PESSOAIS E ÀS COMUNICAÇÕES PRIVADAS
>
> [...]
>
> Art. 11. [...]
>
> § 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.
>
> [...]
>
> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
>
> I – o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas [...];
>
> II – a previsão de mecanismos de autenticação de acesso aos registros [...];
>
> III – a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações [...]; e
>
> IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. [...] (Brasil, 2016).

2.2 Aspectos objetivos e subjetivos

O Marco Civil da Internet aborda tanto aspectos objetivos quanto subjetivos para estabelecer um conjunto abrangente de regras e princípios que regem o uso da internet no país. Vamos explorar esses aspectos.

Aspectos objetivos

Neutralidade da rede: um dos aspectos objetivos mais notáveis do Marco Civil da Internet é a garantia da neutralidade da rede. Isso significa que os provedores de acesso à internet são proibidos de discriminar ou priorizar o tráfego com base no conteúdo, aplicação, serviço ou protocolo. Isso assegura que todos os dados em trânsito na internet sejam tratados de maneira igualitária.

Privacidade e proteção de dados: o Marco Civil objetiva proteger a privacidade dos usuários, estabelecendo diretrizes para a coleta e o uso de dados pessoais. Isso inclui a necessidade de consentimento prévio do usuário e regras para retenção de dados. A lei também exige ordens judiciais para acessar informações pessoais.

Responsabilidade dos provedores de serviços: a lei define os direitos e deveres dos provedores de serviços online, estabelecendo que eles não são responsáveis pelo conteúdo gerado pelos usuários, a menos que não cumpram ordens judiciais para a remoção de conteúdo ilegal após notificação.

Aspectos subjetivos

Liberdade de expressão: o Marco Civil da Internet protege a liberdade de expressão dos usuários online. Isso é um aspecto subjetivo da lei, uma vez que busca equilibrar o direito à liberdade de expressão com limites estabelecidos pela legislação, como a proibição de conteúdo ilegal.

Princípios de governança aberta: a lei promove princípios subjetivos de governança aberta, transparência e participação dos cidadãos no processo de tomada de decisão relacionado à internet. Isso incentiva a colaboração entre governo, sociedade civil e setor privado.

Proteção de direitos autorais: outro aspecto subjetivo do Marco Civil é a proteção de direitos autorais na internet, estabelecendo regras para notificação e retirada de conteúdo protegido. Isso equilibra os interesses dos titulares de direitos autorais e dos usuários da internet.

Garantia de neutralidade e acessibilidade: o aspecto subjetivo da garantia da neutralidade da rede busca garantir que a internet permaneça acessível a todos, sem discriminação ou bloqueio de conteúdo com base em interesses comerciais.

O Marco Civil da Internet combina aspectos objetivos, como a neutralidade da rede, a proteção da privacidade e a responsabilidade dos provedores, com aspectos subjetivos, como a promoção da liberdade de expressão, a governança aberta e a proteção de direitos autorais. Essa abordagem equilibrada visa proteger os direitos dos usuários, promover a inovação e garantir a governança democrática da internet no país.

2.3 Tipificação penal: exemplos aplicados

A tipificação penal refere-se à definição de condutas criminosas e à aplicação de penas para tais atos. No contexto do Marco Civil da Internet no Brasil, a tipificação penal é importante na regulamentação das atividades online, buscando combater práticas ilegais que possam prejudicar a segurança e a privacidade dos usuários. A seguir, discutiremos alguns exemplos de tipificação penal aplicada ao contexto do Marco Civil da Internet.

- **Cyberbullying**: o Marco Civil da Internet estabelece que a prática do cyberbullying, que envolve a divulgação de mensagens ofensivas, ameaçadoras ou difamatórias online, pode ser tipificada como crime, sujeitando os perpetradores a penalidades legais. Isso visa proteger os usuários da internet contra abusos e danos à sua reputação.

- **Divulgação não autorizada de dados pessoais**: a disseminação não autorizada de dados pessoais, como fotos ou informações privadas, pode ser tipificada como crime sob o Marco Civil da Internet. Isso se alinha com a proteção da privacidade e a prevenção de violações de dados.

- **Acessos não autorizados (hackeamento)**: a invasão de sistemas de computador, o acesso não autorizado a contas online e o roubo de informações confidenciais são práticas que podem ser tipificadas como crimes cibernéticos de acordo com a legislação do Marco Civil. Tais ações violam a segurança online e a integridade dos sistemas.

- **Assédio virtual**: o assédio online, que inclui ameaças, perseguições e abuso verbal, pode ser tipificado como crime, visando proteger as vítimas contra danos emocionais e psicológicos.

- **Compartilhamento ilegal de conteúdo protegido por direitos autorais**: o Marco Civil da Internet estabelece regras para a proteção dos direitos autorais online. O compartilhamento ilegal de conteúdo protegido por direitos autorais, como músicas, filmes e software, pode resultar em penalidades legais.

- **Ataques cibernéticos à infraestrutura crítica**: ataques cibernéticos contra infraestruturas críticas, como sistemas de energia e comunicações, podem ser tipificados como crimes graves, devido ao potencial impacto na segurança nacional e na infraestrutura do país.

- **Violação de direitos de propriedade intelectual**: a violação de direitos de propriedade intelectual, como patentes e marcas registradas, também pode ser considerada uma tipificação penal sob a legislação do Marco Civil da Internet.

É importante observar que a tipificação penal no contexto do Marco Civil da Internet é uma ferramenta para garantir a aplicação da lei e a proteção dos direitos dos usuários da internet. A eficácia da tipificação penal depende da capacidade das autoridades e do sistema judicial de investigar e processar violações de maneira justa e eficaz. Além disso, é crucial equilibrar a repressão de crimes online com a proteção dos direitos individuais e a liberdade de expressão na internet.

Saiba mais

Recomendamos assistir ao filme:

MINORITY report: a nova lei. Direção: Steven Spielberg. Estados Unidos: DreamWorks Pictures, 2002. 145 min.

O filme se passa em 2054, época na qual a tecnologia está tão avançada que os policiais conseguem identificar crimes antes mesmo que eles surjam. Dessa maneira, é possível agir de modo preventivo e evitar graves consequências.

Por ter sido lançado em 2002, o título mostra algumas tecnologias que, na época, ainda não existiam, mas que hoje já fazem parte do dia a dia de muitas pessoas, como a realidade aumentada. Por esse motivo, é bastante interessante fazer uma comparação do desenvolvimento tecnológico que a sociedade teve em cerca de 20 anos.

3 DIREITO DIGITAL

O direito digital é uma área do direito que lida com questões legais relacionadas à tecnologia da informação, à internet e ao uso de dispositivos eletrônicos. É uma disciplina em constante evolução devido ao rápido desenvolvimento da tecnologia e à crescente dependência da sociedade em relação à internet e à tecnologia digital.

Uma das áreas mais proeminentes do direito digital é a proteção de dados pessoais. Isso envolve regulamentações para garantir que as informações pessoais sejam coletadas, armazenadas e tratadas de maneira segura e em conformidade com as leis de privacidade. A legislação – como o GDPR, na União Europeia, e a LGPD, no Brasil – estabelece diretrizes claras para a coleta e o uso de dados pessoais.

Questões de propriedade intelectual, como direitos autorais, marcas registradas e patentes, são fundamentais no direito digital. Isso abrange a proteção de conteúdo digital, de softwares e de inovações tecnológicas.

A cibersegurança é uma preocupação crescente, e as leis de cibersegurança são fundamentais para proteger sistemas e dados contra ameaças cibernéticas. Elas envolvem regulamentações para proteção contra ataques, notificação de violações de dados e medidas para garantir a segurança da informação.

O direito digital abrange regulamentações para comércio eletrônico, incluindo contratos online, regulamentos fiscais e direitos do consumidor no ambiente digital.

A criação, validação e execução de contratos digitais são temas relevantes no direito digital. Isso inclui acordos feitos online, como termos de serviço, contratos de software e transações financeiras digitais.

O equilíbrio entre a liberdade de expressão na internet e a necessidade de regulamentação para prevenir discurso de ódio, desinformação e outras formas de conteúdo prejudicial é uma questão fundamental no direito digital.

A resolução de disputas online envolve procedimentos para resolver litígios que surgem no ambiente digital, incluindo arbitragem, mediação e ações judiciais.

Questões éticas e de privacidade também são centrais no direito digital. Isso inclui preocupações com a coleta de dados, o rastreamento de usuários e a necessidade de consentimento informado.

Visto que as redes sociais desempenham um papel significativo na comunicação e interação online, a regulação das práticas de redes sociais e o combate à desinformação são tópicos importantes no direito digital.

Questões de jurisdição, cooperação internacional e extraterritorialidade são desafios no cenário global do direito digital, especialmente quando se trata de crimes cibernéticos e proteção de dados em contextos transfronteiriços.

O direito digital é uma disciplina multifacetada que requer adaptação constante para acompanhar o rápido avanço da tecnologia e os desafios emergentes no mundo digital. É fundamental para proteger os direitos individuais, a segurança da informação e a integridade da sociedade em um ambiente cada vez mais digital.

3.1 Crimes cibernéticos

Crimes cibernéticos são atividades ilegais que ocorrem no ambiente digital, muitas vezes explorando vulnerabilidades na tecnologia e na internet. Aqui estão alguns exemplos de crimes cibernéticos, incluindo os mais comuns:

- **Furto de identidade (*identity theft*)**: envolve o uso não autorizado de informações pessoais de outra pessoa para cometer fraudes, abrir contas bancárias, obter crédito e outros atos fraudulentos em nome da vítima.

- **Fraude eletrônica (dados bancários ou cartão de crédito)**: compreende atividades como a clonagem de cartões de crédito, roubo de informações bancárias e transações fraudulentas com o objetivo de obter ganhos financeiros ilícitos.

- **Estelionato digital (com uso de golpes)**: inclui uma variedade de golpes online, nos quais os criminosos enganam as vítimas para obter vantagens financeiras. Isso envolve golpes de investimento, leilões falsos, falsos serviços de caridade e muito mais.

- **Golpe de loja online fantasma**: cria lojas online falsas para vender produtos que não existem ou que nunca serão entregues, enganando os compradores.

- **Golpe de boleto falso**: envolve a criação de boletos falsos para pagamento de produtos ou serviços, com os fundos sendo direcionados para contas controladas pelo criminoso.

- **Golpe de aplicativo falso**: desenvolve aplicativos falsos que parecem legítimos, mas, na realidade, são projetados para roubar informações pessoais ou financeiras dos usuários.

- **Pedofilia e pornografia infantil**: compartilha, distribui ou cria conteúdo na internet relacionado à exploração sexual de crianças.

- **Invasão**: envolve a intrusão não autorizada em sistemas de computador, redes ou contas online. Os invasores podem roubar informações, prejudicar a integridade dos sistemas ou realizar ações maliciosas.

- **Furto de dados (vazamento)**: rouba informações confidenciais, como dados pessoais, informações comerciais ou segredos de empresas, e as divulgam de maneira não autorizada.

- **Crimes contra honra (difamação)**: inclui difamação, calúnia e injúria cometidas online, como publicação de informações falsas ou prejudiciais sobre uma pessoa.

- **Racismo**: promove discurso de ódio racial, discriminação e incitação ao ódio com base em raça, etnia ou nacionalidade.

- **Ameaça**: ameaça ou assedia indivíduos ou grupos, incluindo ameaças de violência física, difamação ou chantagem.

Esses foram alguns dos mais comuns crimes cibernéticos, mas a natureza da criminalidade digital evolui constantemente à medida que a tecnologia avança. A prevenção e a resposta a esses crimes requerem uma combinação de medidas legais, segurança cibernética robusta e conscientização dos usuários. As autoridades, empresas e indivíduos devem estar vigilantes para enfrentar essas ameaças online.

Saiba mais

Recomendamos assistir ao filme:

O JOGO da imitação. Direção: Morten Tyldum. Estados Unidos: The Weinstein Company, 2014. 115 min.

O filme conta a história de Alan Turing (Benedict Cumberbatch), um matemático e cientista da computação.

Durante a Segunda Guerra Mundial, o grande projeto de Turing foi construir uma máquina para decodificar o código que a frota alemã usava, chamado enigma. Assim, os ingleses poderiam decifrar as ordens dos alemães antes que elas fossem executadas. A máquina deu origem aos computadores que usamos hoje, criando uma revolução na informática.

3.2 Ciberterrorismo e conflitos digitais

O ciberterrorismo refere-se ao uso da tecnologia da informação e comunicação para realizar atividades terroristas. Ao contrário do terrorismo convencional, que muitas vezes envolve ataques físicos, o ciberterrorismo se concentra em explorar vulnerabilidades em sistemas de computadores e redes para causar danos, disseminar o medo e atingir objetivos políticos ou ideológicos.

Objetivos do ciberterrorismo

- **Desestabilização**: ciberterroristas buscam desestabilizar governos, organizações ou sociedades ao comprometer infraestruturas críticas, como energia, comunicações, transporte e serviços financeiros.
- **Propagação de ideologias**: muitas vezes envolve a disseminação de mensagens ideológicas extremistas por meio da internet, recrutamento online e radicalização.

Ataques cibernéticos

- **Ataques de negação de serviço (DoS/DDoS)**: sobrecarregam os servidores-alvo, tornando os serviços inacessíveis.
- **Ataques de malware:** inserção de software malicioso para roubo de informações, espionagem ou destruição de dados.
- ***Hacking* de infraestrutura crítica:** alvos incluem redes elétricas, sistemas de água, transporte e serviços de emergência.

Ameaças à segurança nacional

- **Espionagem cibernética**: estados ou grupos terroristas podem usar ciberespionagem para coletar informações sensíveis.
- **Manipulação de eleições**: ciberataques podem ser usados com o objetivo de influenciar processos democráticos, comprometendo a integridade das eleições.

Atores envolvidos

- **Estados-nação**: alguns governos podem patrocinar ou apoiar atividades cibernéticas para atingir objetivos políticos.
- **Grupos terroristas**: organizações terroristas podem empregar especialistas em tecnologia para realizar ataques cibernéticos.
- **Hacktivistas**: indivíduos ou grupos que buscam promover causas políticas ou sociais por meio de atividades de *hacking*.

Desafios para combater o ciberterrorismo

- **Anonimato na internet**: a capacidade de operar de forma anônima torna difícil rastrear e responsabilizar os perpetradores.
- **Rápida evolução tecnológica**: as ameaças cibernéticas evoluem rapidamente, desafiando os esforços de segurança para acompanhar o ritmo.
- **Coordenação internacional**: o ciberterrorismo muitas vezes atravessa fronteiras, exigindo cooperação global para enfrentar efetivamente o problema.

Medidas de prevenção e mitigação

- **Segurança cibernética reforçada**: implementação de medidas robustas de segurança em sistemas críticos.
- **Cooperação internacional**: colaboração entre países para compartilhar informações e coordenar esforços.
- **Conscientização e educação**: educação pública sobre práticas seguras online e conscientização sobre ameaças cibernéticas.

O ciberterrorismo representa uma ameaça significativa no mundo digital atual. Enfrentar esse desafio requer uma abordagem multifacetada, combinando medidas técnicas avançadas, cooperação

internacional e consciência pública. À medida que a tecnologia continua a evoluir, é essencial que os esforços para combater o ciberterrorismo também se adaptem e se fortaleçam.

Conflitos digitais

Os conflitos digitais referem-se a disputas e confrontos que ocorrem no ciberespaço, envolvendo o uso de tecnologias da informação e comunicação. Esses conflitos podem assumir diversas formas, desde ataques cibernéticos entre nações até ações de grupos ativistas ou criminosos.

Tipos de conflito digital

- **Ciberataques estatais:** nações podem conduzir operações cibernéticas para espionagem, sabotagem ou desestabilização de outros países.
- **Cibercrime**: atividades criminosas, como roubo de dados, fraudes e extorsão, realizadas por meio de recursos digitais.
- **Guerra da informação**: uso de meios digitais para influenciar a opinião pública, disseminar desinformação ou manipular eventos.

Ciberespionagem

- **Roubo de propriedade intelectual**: nações e entidades corporativas podem buscar informações confidenciais para ganho estratégico ou econômico.
- **Monitoramento de comunicações**: agências de inteligência podem interceptar e analisar comunicações eletrônicas para obter informações sensíveis.

Ataques cibernéticos

- **Infiltração de redes**: hackers podem entrar em sistemas para roubar dados, interromper operações ou implantar malware.
- **Ataques de negação de serviço (DoS/DDoS)**: sobrecarga de servidores para tornar serviços indisponíveis.

Desafios éticos e legais

- **Atribuição**: a identificação dos responsáveis por ataques cibernéticos pode ser desafiadora, dada a capacidade de ocultação online.
- **Normas internacionais**: a falta de consenso sobre normas e leis internacionais relacionadas a conflitos cibernéticos cria desafios para a governança.

Guerra cibernética e defesa

- **Desenvolvimento de capacidades**: países investem em desenvolver capacidades ofensivas e defensivas no ciberespaço.

- **Estratégias de resposta**: estabelecimento de políticas e estratégias para responder a ameaças cibernéticas, incluindo medidas de retaliação.

Consequências e impacto

- **Impacto econômico**: ataques cibernéticos podem causar danos significativos à economia, interrompendo operações e resultando em perda de dados valiosos.

- **Riscos para a segurança nacional**: a segurança nacional pode ser comprometida se infraestruturas críticas, como energia e serviços públicos, forem alvo de ataques.

Ciberpaz e diplomacia

- **Normas e acordos**: necessidade de desenvolver normas e acordos internacionais para governar o comportamento no ciberespaço.

- **Diplomacia cibernética**: diálogo entre nações para reduzir tensões e promover a cooperação no ciberespaço.

Os conflitos digitais tornaram-se uma parte inevitável da paisagem geopolítica contemporânea. A rápida evolução da tecnologia exige que as nações e as organizações desenvolvam estratégias eficazes para prevenir, detectar e responder a ameaças cibernéticas. A colaboração internacional e a construção de normas éticas são cruciais para lidar com os desafios cada vez mais complexos apresentados pelos conflitos no ciberespaço.

3.3 Espionagem digital

A espionagem digital, também conhecida como ciberespionagem, refere-se ao uso de tecnologias da informação e comunicação para coletar informações confidenciais, segredos industriais, dados estratégicos ou outras informações sensíveis. Diferentemente da espionagem tradicional, a espionagem digital ocorre no ciberespaço e muitas vezes envolve métodos altamente sofisticados.

Objetivos da espionagem digital são a coleta de inteligência, obtendo informações estratégicas sobre governos, organizações, ou indivíduos para ganho político, militar ou econômico; e o roubo de propriedade intelectual, adquirindo segredos comerciais, planos de produtos ou outras informações valiosas para adquirir vantagem competitiva.

As principais atividades de ciberespionagem são:

- **malware e ataques persistentes avançados (APTs)**: uso de software malicioso para infiltrar sistemas e coletar dados ao longo do tempo;

- ***phishing* e engenharia social**: engano de usuários para revelar informações confidenciais, como senhas, por meio de técnicas enganosas;

- **infiltração de redes**: acesso não autorizado a sistemas, redes e servidores para coleta de dados.

Os governos conduzem atividades de espionagem digital para obter vantagens estratégicas e de segurança, assim como os hacktivistas, que são grupos ou indivíduos que conduzem ciberespionagem em apoio a causas políticas ou sociais. As empresas também podem se envolver em espionagem digital para obter informações sobre concorrentes.

Os alvos da espionagem digital são os governos e as instituições estatais, com o objetivo de coletar informações políticas, militares e econômicas, e as empresas e indústrias, para roubo de propriedade intelectual, planos de negócios e estratégias. Os ativistas são indivíduos com foco no monitoramento de atividades online e offline.

Os desafios na detecção desse crime são a atribuição e a evolução tecnológica. Identificar os responsáveis pela espionagem digital pode ser difícil, pois os atacantes frequentemente usam técnicas para esconder sua verdadeira origem. As táticas de espionagem digital evoluem rapidamente, desafiando as ferramentas de segurança a as acompanharem.

A espionagem digital apresenta diversas consequências; por exemplo, os ataques cibernéticos a governos podem ter implicações significativas para a segurança nacional. Empresas que são alvo de espionagem digital sofrem perdas financeiras e danos à reputação.

Pensar em segurança cibernética, como a implementação de medidas robustas de segurança, incluindo firewalls, antivírus e detecção de intrusão, pode prevenir ou mitigar esse crime. Outra ação envolve a conscientização com educação sobre práticas seguras online e treinamento para identificar ameaças de engenharia social.

A espionagem digital representa uma ameaça significativa na era da informação. A rápida expansão das capacidades tecnológicas exige um foco contínuo na segurança cibernética e na colaboração internacional para enfrentar os desafios apresentados, que muitas vezes transcende fronteiras e setores. As organizações e os governos precisam adotar abordagens proativas para proteger informações sensíveis e mitigar os riscos associados à ciberespionagem.

3.4 Uso ilícito de softwares

O uso ilícito de softwares, também conhecido como pirataria de software, refere-se à prática de adquirir, instalar ou distribuir software de maneira que viole os termos de licenciamento ou os direitos autorais. Essa atividade envolve a obtenção e utilização de programas de computador de maneira não autorizada, geralmente sem pagar as taxas ou aderir aos termos estabelecidos pelos desenvolvedores do software.

Classifica-se como pirataria de software as cópias não autorizadas, isto é a obtenção, instalação ou distribuição de cópias de software sem a devida autorização do detentor dos direitos autorais. A ativação fraudulenta quando se utiliza de manipulação de métodos de ativação ou uso de chaves de licença falsas para contornar os mecanismos de proteção.

Quais as motivações para a pirataria de software?

- **Econômicas**: a busca por economizar dinheiro, evitando os custos associados à compra legal de software.
- **Facilidade de acesso**: disponibilidade facilitada de cópias ilegais na internet e em redes de compartilhamento de arquivos.
- **Ignorância ou desconsideração**: falta de conhecimento sobre as leis de direitos autorais ou desconsideração deliberada por parte do usuário.

Os desenvolvedores de software perdem receita devido à distribuição não autorizada. Quem utiliza software pirata também pode ser prejudicado, pois os softwares piratas frequentemente não recebem atualizações de segurança, tornando os sistemas vulneráveis a ameaças.

Algumas medidas técnicas podem ser aplicadas para evitar a pirataria, como chaves de licença, autenticação online e criptografia. Também recomenda-se informar os usuários sobre os riscos associados à pirataria e promover a ética no uso de software.

A pirataria de software é muitas vezes considerada uma violação das leis de direitos autorais, sujeita a penalidades legais. Desenvolvedores e organizações buscam ações legais contra usuários envolvidos em pirataria de software, como multas e processos judiciais.

Uma alternativa à pirataria são os softwares livres e de código aberto, que são alternativas legais e gratuitas que respeitam os princípios de código aberto. Muitas empresas agora oferecem modelos de assinatura para tornar o acesso legal ao software mais acessível.

O uso ilícito de softwares não apenas prejudica financeiramente os desenvolvedores, mas também representa uma ameaça à segurança dos sistemas. A conscientização sobre os riscos associados à pirataria, a implementação de práticas de segurança e a promoção de alternativas legais são cruciais para combater essa prática e garantir um ambiente digital ético e sustentável. As empresas, os usuários e os governos são importantes na prevenção e repressão à pirataria de software.

3.5 Aspectos legais e tipificação penal

Os aspectos legais e a tipificação penal no âmbito do direito digital são de extrema importância para regulamentar e punir condutas relacionadas a crimes cibernéticos. À medida que a sociedade se torna mais dependente da tecnologia, as leis precisam evoluir para abordar questões específicas do mundo digital.

Legislação específica

- **Leis de cibercrimes**: muitos países têm desenvolvido leis específicas para lidar com crimes digitais, abordando questões como *hacking*, roubo de identidade, fraude eletrônica e difamação online.

- **Proteção de dados**: leis que regulamentam a coleta, armazenamento e uso de dados pessoais, como a LGPD no Brasil.

Tipificação penal no ciberespaço

- **Acesso não autorizado**: *hacking*, invasão de sistemas e acesso não autorizado a dados são frequentemente criminalizados.

- **Fraude eletrônica**: atividades fraudulentas online, como *phishing*, esquemas de pirâmide e manipulação de transações eletrônicas.

- **Ciberterrorismo**: atos que visam causar danos sérios por meio de ataques cibernéticos, muitas vezes com motivações políticas ou ideológicas.

Proteção à propriedade intelectual

- **Violação de direitos autorais:** penalização para a distribuição não autorizada de software, música, filmes e outros conteúdos protegidos por direitos autorais.

- **Pirataria de software**: leis específicas para coibir a reprodução e distribuição não autorizadas de softwares.

Crime organizado no ciberespaço

- **Ataques coordenados**: penalização para grupos que coordenam ataques cibernéticos para obter ganhos financeiros, políticos ou ideológicos.

- **Tráfico de dados roubados**: leis que abordam o comércio ilegal de informações pessoais roubadas.

Jurisdição e cooperação internacional

- **Jurisdição transnacional**: crimes cibernéticos muitas vezes transcendem fronteiras, exigindo cooperação internacional na persecução legal.

- **Convenções internacionais**: acordos entre países para combater crimes cibernéticos e compartilhar informações.

Responsabilidade das plataformas online

- **Leis de responsabilidade civil**: plataformas online podem ser responsabilizadas por conteúdos ilegais ou prejudiciais veiculados em suas redes.

- **Combate à desinformação**: leis que visam mitigar a disseminação de notícias falsas e desinformação online.

Desafios legais no mundo digital

- **Anonimato e atribuição**: identificar os perpetradores em um ambiente digital pode ser desafiador devido ao anonimato.

- **Rapidez das mudanças tecnológicas**: a legislação muitas vezes luta para acompanhar o ritmo das inovações tecnológicas.

O desenvolvimento e a aplicação eficaz das leis no âmbito do direito digital são cruciais para garantir a segurança e a ordem no ciberespaço. À medida que as ameaças cibernéticas evoluem, as legislações precisam ser adaptadas para abordar novas formas de crimes digitais. A cooperação internacional e a harmonização das leis são essenciais para enfrentar os desafios transnacionais apresentados pelo mundo digital.

4 DIREITO À INTIMIDADE E DIVULGAÇÃO DE NOTÍCIAS FALSAS

O direito à intimidade é um pilar fundamental dos direitos humanos, garantindo a proteção da esfera pessoal de indivíduos contra interferências injustificadas. No entanto, a disseminação de notícias falsas na era digital levanta questões complexas, muitas vezes desafiando esse direito e criando um equilíbrio delicado entre liberdade de expressão, informação verdadeira e respeito à privacidade.

Direito à intimidade

O direito à intimidade protege a vida privada das pessoas, resguardando informações pessoais, relações familiares, correspondências e outras áreas sensíveis da vida cotidiana. Esse direito é consagrado em diversas legislações nacionais e tratados internacionais de direitos humanos.

Divulgação de notícias falsas

As notícias falsas, ou fake news, são informações deliberadamente fabricadas para enganar ou distorcer a realidade. A disseminação rápida e massiva dessas notícias, impulsionada pela era digital e pelas redes sociais, pode causar danos significativos à reputação das pessoas e à sociedade.

Desafios éticos

A divulgação de notícias falsas muitas vezes entra em conflito com o direito à intimidade. Informações falsas podem ser difundidas com o intuito de difamar ou prejudicar a reputação de indivíduos, invadindo sua esfera privada e gerando consequências adversas.

Liberdade de expressão e responsabilidade

A liberdade de expressão é um direito fundamental, mas não absoluto. A disseminação irresponsável de informações falsas ultrapassa os limites dessa liberdade, especialmente quando compromete a reputação ou a segurança de indivíduos. Há uma crescente necessidade de responsabilização por informações enganosas.

O direito à liberdade de expressão é um dos princípios fundamentais assegurados pela Constituição Federal de 1988 no Brasil. Esse direito está consagrado no artigo 5º, inciso IV, que estabelece que "é livre a manifestação do pensamento, sendo vedado o anonimato". A redação desse dispositivo reflete a importância atribuída pelos constituintes à liberdade de expressão como um dos pilares da democracia e dos direitos individuais.

O reconhecimento da liberdade de expressão na Constituição Federal de 1988 é um reflexo do comprometimento do legislador brasileiro com os princípios democráticos e com a proteção dos direitos humanos. Esse direito não se limita apenas à expressão verbal, mas abrange também a liberdade de imprensa, de comunicação e de manifestação em geral, respeitando-se os limites estabelecidos pela própria Constituição.

No entanto, é importante ressaltar que a liberdade de expressão não é absoluta, e a Constituição prevê alguns limites e restrições para proteger outros direitos e interesses fundamentais. Por exemplo, a lei estabelece que a manifestação do pensamento não pode ser utilizada para a prática de crimes, como calúnia, difamação e injúria, além de vedar o discurso de ódio e a apologia à violência.

Observação

É importante destacar que o direito à liberdade de expressão não isenta os indivíduos de responsabilidade pelas consequências de suas palavras. Se uma manifestação ultrapassa os limites legais e prejudica a honra de terceiros, por exemplo, a pessoa responsável pode ser responsabilizada civil e criminalmente.

Regulação e ética digital

Governos, plataformas de mídia social e sociedade civil estão buscando estratégias para enfrentar o fenômeno das notícias falsas. A regulação eficaz e as práticas éticas na esfera digital tornam-se essenciais para preservar a integridade da informação, sem violar os direitos individuais.

Educação, conscientização e desafios jurídicos

Educar o público sobre a identificação de notícias falsas é uma abordagem preventiva crucial. Promover a alfabetização digital e a conscientização sobre os perigos das informações enganosas contribui para a criação de uma sociedade mais informada e resistente a manipulações.

Encontrar um equilíbrio legal entre a proteção da intimidade e a liberdade de expressão é desafiador. Leis de privacidade e legislações relacionadas à difamação precisam ser atualizadas para abordar os desafios específicos apresentados pela era digital.

As plataformas digitais são importantes na disseminação de notícias falsas. Exigir responsabilidade delas na identificação e remoção de conteúdo falso é um aspecto crucial para mitigar danos.

Em última análise, encontrar um equilíbrio entre o direito à intimidade e a luta contra notícias falsas requer uma abordagem multifacetada, envolvendo educação, regulamentação eficaz e responsabilidade por parte das plataformas e indivíduos. A proteção da liberdade de expressão e a preservação da integridade da informação devem coexistir, respeitando os direitos fundamentais de cada indivíduo na sociedade digital.

Responsabilidade civil e penal

A responsabilidade, no contexto jurídico, é um conceito amplo que abrange diversas áreas e implicações. Duas das principais categorias de responsabilidade são as responsabilidades civil e penal, cada uma delas relacionada a diferentes aspectos do sistema legal.

A responsabilidade civil refere-se às obrigações que uma pessoa tem de reparar danos causados a outra. Isso pode ocorrer devido a atos ilícitos, negligência, imprudência ou violação de deveres contratuais. O objetivo principal da responsabilidade civil é compensar a vítima pelos prejuízos sofridos.

No âmbito civil, a reparação dos danos geralmente envolve o pagamento de indenizações monetárias, destinadas a restabelecer a situação da vítima ao estado anterior ao dano. Essa compensação pode incluir danos materiais, morais, estéticos, entre outros.

A responsabilidade penal está relacionada à prática de crimes e violações das normas penais. Quando alguém comete uma conduta considerada criminosa, está sujeito a sanções previstas no sistema penal, como prisão, multas, penas alternativas, entre outras.

Diferentemente da responsabilidade civil, a responsabilidade penal visa punir o autor da conduta ilícita em nome do interesse público e da ordem social. Além disso, as penas no âmbito penal têm caráter retributivo e preventivo, buscando retribuir o mal causado e prevenir a prática de novos delitos.

Observação

É importante notar que uma mesma conduta pode gerar responsabilidade tanto civil quanto penal. Por exemplo, em um acidente de trânsito causado por negligência, o responsável pode ser processado civilmente para indenizar a vítima pelos danos materiais e morais, e enfrentar ação penal por imprudência no trânsito.

As esferas civil e penal operam de forma independente, e o resultado de um processo em uma área não determina automaticamente o resultado na outra. O objetivo principal da responsabilidade civil é a reparação, enquanto a responsabilidade penal busca a punição do infrator.

4.1 O direito à intimidade na internet

O direito à intimidade, que historicamente protege a esfera pessoal dos indivíduos, enfrenta novos desafios na era da internet. A constante interconexão online, a proliferação de redes sociais e a coleta massiva de dados desafiam a privacidade de maneiras antes inimagináveis. Vamos explorar como esse direito se manifesta no contexto digital e os desafios associados.

A atividade online deixa rastros digitais, desde buscas na web até interações em redes sociais. O direito à intimidade na internet confronta a capacidade de indivíduos controlarem o que é conhecido sobre eles, exigindo uma reflexão sobre a coleta e o uso de dados pessoais. O uso generalizado de redes sociais levanta questões sobre a exposição voluntária. Muitos usuários compartilham detalhes íntimos de suas vidas online, desafiando a linha entre a escolha pessoal de divulgar informações e a necessidade de proteger a privacidade.

Empresas online frequentemente coletam dados para personalizar experiências e direcionar publicidade. O desafio está em equilibrar a personalização desejada pelos usuários com a preservação de sua privacidade, especialmente diante de práticas invasivas.

A crescente sofisticação de hackers e ciberataques representa uma ameaça constante à intimidade online. Proteger informações pessoais contra violações torna-se uma prioridade, envolvendo medidas robustas de cibersegurança. Muitas regiões implementaram legislação de proteção de dados, como a LGPD no Brasil. Essas leis visam dar aos usuários maior controle sobre seus dados pessoais, estabelecendo limites claros sobre sua coleta e uso.

Frequentemente, os usuários concordam com termos e condições sem compreender completamente as ramificações, destacando a necessidade de transparência e simplificação desses documentos. A obtenção de consentimento informado torna-se um desafio. Alguns países reconhecem o direito ao esquecimento, permitindo que os indivíduos solicitem a remoção de informações pessoais irrelevantes ou desatualizadas. Essa medida visa equilibrar o direito à privacidade com a permanência de informações online.

A promoção da educação digital é fundamental para capacitar os usuários a entenderem e protegerem sua própria privacidade online. Isso inclui conscientização sobre configurações de privacidade, uso seguro de senhas e reconhecimento de ameaças online.

Proteger o direito à intimidade na internet requer uma abordagem holística, envolvendo ações individuais, regulamentações eficazes e práticas éticas por parte das empresas. À medida que a tecnologia avança, a sociedade precisa continuar a adaptar suas abordagens para garantir que os direitos fundamentais não se percam no labirinto digital.

A proteção à intimidade é uma manifestação do respeito à esfera privada das pessoas, resguardando-as de intromissões indevidas por parte do Estado ou de terceiros. Esse direito abrange aspectos variados da vida pessoal, como segredos, correspondências, dados pessoais, e outras informações que dizem respeito à individualidade e à privacidade do cidadão.

Dentre as principais manifestações do direito à intimidade, podemos destacar:

- **Sigilo de comunicações**: garante a inviolabilidade das comunicações telefônicas, correspondências e comunicações eletrônicas, protegendo a privacidade das conversas e trocas de mensagens.
- **Proteção de dados pessoais**: abrange a proteção dos dados pessoais, assegurando que informações sensíveis sobre a vida de uma pessoa não sejam utilizadas de forma indevida.
- **Respeito à vida privada**: envolve a preservação da vida privada das pessoas em seus lares, relações familiares, e demais contextos nos quais se espera que a intimidade seja respeitada.
- **Imagem e honra**: assegura que a imagem e a honra das pessoas são garantidas, certificando que não sejam expostas de maneira indevida ou difamadas.

É importante ressaltar que, embora o direito à intimidade seja fundamental, ele não é absoluto e pode ser relativizado em situações específicas, como em investigações criminais ou para a preservação de interesses públicos relevantes.

Lembrete

O direito à intimidade é um dos itens fundamentais garantidos pela Constituição Federal de 1988 no Brasil. Esse direito está consagrado no artigo 5º, inciso X, que estabelece que "são 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".

Assim, caso ocorra uma violação desse direito, a pessoa afetada tem o respaldo legal para buscar reparação pelos danos sofridos.

4.2 A Lei n. 12.737/12: noções gerais e aspectos

A Lei n. 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, foi criada em resposta a um caso de grande repercussão no Brasil que envolveu a atriz Carolina Dieckmann, que teve suas fotos pessoais íntimas divulgadas sem sua autorização. Essa legislação introduziu alterações no Código Penal brasileiro para tipificar crimes virtuais, especialmente aqueles relacionados à invasão de dispositivos informáticos e à divulgação não autorizada de conteúdo íntimo.

A lei estabelece penalidades para quem invade dispositivos informáticos alheios para obter, adulterar ou destruir dados sem autorização. A invasão de dispositivos para obter conteúdo privado configura crime, com penas que podem variar de detenção de três meses a um ano, além de multa. Caso alguém obtenha, transmita ou divulgue, sem consentimento, material que revele cenas de nudez ou ato sexual de caráter privado, a pena pode variar de um a cinco anos de prisão, além de multa.

A legislação destaca a importância do consentimento explícito para a divulgação de imagens íntimas. A ausência de autorização prévia e expressa do titular do conteúdo configura a prática criminosa. As penas podem ser agravadas em determinadas circunstâncias, como quando o crime for cometido por pessoa que manteve relação íntima de afeto com a vítima, visando aumentar o constrangimento dela.

A lei estabelece a responsabilização criminal tanto para invasões de dispositivos quanto para a divulgação não autorizada de conteúdo íntimo, buscando coibir práticas que causem danos à privacidade e à dignidade das pessoas. A legislação visa proteger a vítima desses crimes, reconhecendo a gravidade do impacto emocional e psicológico causado pela exposição não consensual de conteúdo íntimo.

A Lei Carolina Dieckmann representou um avanço significativo na proteção digital e no reconhecimento da necessidade de legislação específica para lidar com crimes cibernéticos, destacando a importância de adequar as leis à realidade digital.

A Lei n. 12.737/2012 desempenhou um papel importante na proteção da privacidade e na criminalização de práticas danosas na esfera digital, refletindo a necessidade de adaptação da legislação diante dos desafios emergentes no mundo digital.

4.3 Tipificação

A tipificação é um conceito fundamental no campo jurídico e refere-se à descrição e classificação de condutas delitivas de acordo com as normas legais. Trata-se da definição precisa e específica dos elementos que caracterizam um crime, estabelecendo os parâmetros para a identificação e punição de determinadas ações.

Principais aspectos da tipificação

- **Descrição detalhada**: requer uma descrição detalhada e clara das condutas consideradas ilícitas. Essa descrição deve incluir elementos essenciais que distinguem o crime em questão de outras atividades legais.

- **Elementos constitutivos**: cada tipo penal tem elementos constitutivos que precisam estar presentes para que a conduta seja considerada criminosa. Esses elementos podem incluir ações, omissões, resultado danoso, entre outros.

- **Código Penal**: geralmente, ocorre no Código Penal de uma jurisdição. Esse código contém uma lista de crimes, cada um deles devidamente tipificado, indicando as penas associadas a esses delitos.

- **Garantia da legalidade**: é uma garantia fundamental no princípio da legalidade, assegurando que apenas condutas previamente definidas por lei como crimes podem ser objeto de punição. Ninguém pode ser punido por algo que não seja expressamente proibido por lei.

- **Clareza e precisão**: para garantir justiça e segurança jurídica, a tipificação deve ser redigida com clareza e precisão. Isso evita interpretações vagas que poderiam levar a aplicações arbitrárias da lei.

- **Adaptação às mudanças sociais**: também precisa ser flexível o suficiente para se adaptar às mudanças sociais e tecnológicas. Novas leis e atualizações frequentes são necessárias para abordar crimes emergentes e evoluir conforme a sociedade evolui.

Importância da tipificação

- **Previsibilidade jurídica**: proporciona previsibilidade jurídica, permitindo que os cidadãos compreendam claramente quais comportamentos são considerados criminosos.

- **Garantia dos direitos individuais**: estabelece os limites legais para o que constitui um crime, a tipificação protege os direitos individuais, garantindo que as pessoas sejam tratadas de acordo com a lei e não arbitrariamente.

- **Atuação do sistema de justiça**: facilita a atuação do sistema de justiça, fornecendo orientações claras para investigadores, promotores e juízes, permitindo uma aplicação consistente e justa da lei.

- **Dissuasão e prevenção**: serve de instrumento de dissuasão, desencorajando a prática de condutas criminosas. Além disso, fornece a base para estratégias de prevenção criminal.

- **Responsabilidade penal**: é essencial para estabelecer a responsabilidade penal. Ela define os limites entre a conduta permitida e proibida, estabelecendo as consequências legais para quem viola esses limites.

A tipificação é um elemento essencial do sistema jurídico, fornecendo os alicerces para a aplicação justa e consistente da lei em sociedades democráticas. Ela desempenha um papel importante na definição dos limites do que é aceitável e proibido, assegurando a harmonia entre a ordem legal e os direitos individuais.

4.4 A divulgação de notícias falsas (fake news) na internet

A disseminação de notícias falsas na internet emergiu como um fenômeno global com implicações significativas para a sociedade, a política e a confiança na informação. Esse fenômeno, conhecido como fake news, destaca desafios complexos e aponta para a necessidade urgente de estratégias eficazes para enfrentar esse problema. Vamos explorar os principais aspectos relacionados à divulgação de notícias falsas na internet:

Definição de fake news

Fake news refere-se a informações deliberadamente falsas ou enganosas apresentadas como notícias legítimas. Elas podem ser criadas para distorcer a realidade, influenciar opiniões públicas, prejudicar reputações ou obter ganhos financeiros.

Rápida propagação nas redes sociais

As redes sociais desempenham um papel central na disseminação de notícias falsas. A velocidade com que as informações circulam nas plataformas online pode resultar na rápida propagação de conteúdos enganosos antes que a veracidade seja verificada.

Impacto na opinião pública

As fake news podem moldar a opinião pública, influenciar eleições, criar pânico e contribuir para a polarização. A capacidade de manipular as percepções das pessoas destaca a gravidade do problema.

Desafios na verificação de informações

A verificação de informações na internet tornou-se um desafio, especialmente dada a quantidade massiva de conteúdo gerado a cada minuto. Isso exige esforços coordenados para validar e classificar a credibilidade das fontes.

Motivações por trás da criação de fake news

As motivações para a criação e disseminação de notícias falsas variam, incluindo interesses políticos, econômicos e sociais ou simplesmente o desejo de enganar. Compreender essas motivações é crucial para desenvolver estratégias eficazes de combate.

Responsabilidade das plataformas digitais

As plataformas digitais têm um papel crucial na mitigação da disseminação de fake news. Elas enfrentam desafios para equilibrar a liberdade de expressão com a responsabilidade de combater informações enganosas em suas plataformas.

Lembrete

O direito à liberdade de expressão é um dos alicerces da democracia e está garantido na Constituição Federal de 1988. No entanto, é necessário equilibrar essa liberdade com a responsabilidade social, evitando abusos que possam prejudicar outros direitos e interesses fundamentais.

Educação e alfabetização digital

A promoção da alfabetização digital e da educação midiática é essencial. Capacitar as pessoas para reconhecerem e questionarem fontes duvidosas contribui para a construção de uma sociedade mais resiliente contra a desinformação.

Regulamentação e ética jornalística

A regulamentação eficaz, alinhada a princípios éticos jornalísticos, é necessária para responsabilizar aqueles que deliberadamente espalham informações falsas. Isso exige uma abordagem equilibrada para evitar a censura excessiva.

Colaboração global

A disseminação de fake news é um desafio global que requer esforços colaborativos entre governos, organizações, sociedade civil e empresas de tecnologia. A cooperação internacional é essencial para abordar esse fenômeno de maneira abrangente.

Verificação independente

A promoção de organizações de verificação de fatos independentes é crucial. Essas entidades desempenham um papel vital na avaliação da veracidade das informações e na correção de desinformações disseminadas.

Enfrentar o problema das notícias falsas na internet exige uma abordagem complexa, abrangendo educação, regulamentação, tecnologia e colaboração global. As consequências de não lidar efetivamente com esse fenômeno podem minar a confiança na informação, comprometer a democracia e criar desafios duradouros para a sociedade.

4.5 Contexto histórico e tendências atuais

Contexto histórico

O século XX testemunhou uma revolução tecnológica sem precedentes, desde a industrialização até a ascensão da era digital. A criação do computador, o desenvolvimento da internet e a proliferação de dispositivos móveis marcaram transformações fundamentais na sociedade.

O avanço dos meios de transporte e comunicação facilitou a globalização. As fronteiras tornaram-se mais permeáveis, impulsionando o comércio internacional, a interconexão cultural e a disseminação de ideias em uma escala nunca experimentada.

Movimentos sociais, como o dos direitos civis, o feminista e o LGBTQIA+, influenciaram de modo profundo as dinâmicas sociais. Mudanças culturais significativas moldaram a forma como as pessoas percebem a identidade, a igualdade e a diversidade.

O final do século XX e início do século XXI foram marcados pela revolução digital. A ascensão da internet, o desenvolvimento de dispositivos móveis e a computação em nuvem transformaram radicalmente a forma como as pessoas interagem, comunicam-se e acessam informações.

Tendências atuais

A inteligência artificial (IA) e a automatização estão redefinindo a natureza do trabalho e da produção. Desde chatbots até carros autônomos, a integração de sistemas inteligentes está moldando indústrias e criando oportunidades, mas também desafios éticos.

A preocupação com a sustentabilidade tornou-se central. As mudanças climáticas e a escassez de recursos estão impulsionando esforços em direção a práticas mais sustentáveis, desde a produção de energia até a gestão de resíduos.

A transformação digital redefine os modelos de negócios. A implementação de tecnologias como big data, internet das coisas (IoT) e blockchain está otimizando processos, melhorando a eficiência e criando oportunidades de inovação.

A saúde experimenta uma revolução tecnológica. Telemedicina, *wearables*, análise de dados de saúde e pesquisas genômicas estão moldando a forma como os serviços de saúde são entregues e personalizados.

O aumento da interconexão digital trouxe preocupações sobre cibersegurança e privacidade. Ataques cibernéticos e debates sobre o equilíbrio entre segurança e privacidade são temas de relevância crescente.

A pandemia global acelerou a adoção de métodos de educação online e trabalho remoto. Essas tendências estão impactando a forma como as pessoas aprendem, trabalham e colaboram, desafiando modelos tradicionais.

O avanço tecnológico levanta questões éticas, desde o uso de algoritmos de IA até dilemas éticos na engenharia genética. A sociedade está confrontando desafios relacionados à responsabilidade, equidade e justiça em meio às inovações tecnológicas.

O contexto histórico e as tendências atuais refletem a dinâmica constante de mudança e inovação. A interconexão global e a rápida evolução tecnológica moldam não apenas a forma como vivemos e trabalhamos, mas também colocam desafios importantes que exigem respostas colaborativas e reflexão ética. O século XXI continua a ser uma era de transformações, exigindo adaptação contínua e abordagens responsáveis para enfrentar os desafios emergentes.

4.6 As novas tecnologias e a internet das coisas (IoT)

As tecnologias que surgiram com a chegada do computador e da internet mudaram a sociedade e, em especial, o direito. As ciências jurídicas sofrem influência dessas novas tecnologias. O processo físico passou a ser virtual e os atos relativos ao Judiciário estão cada vez mais sendo realizados por meio eletrônico.

A internet impulsionou um expressivo mercado de consumo virtual, no qual trocas e compras são realizadas por meio eletrônico.

Nos termos do artigo 3º, §1º, do Código de Defesa do Consumidor, os bens digitais são espécies de bens incorpóreos sobre os quais recai a titularidade e a possibilidade de sua disposição, oferta e venda.

> [...]
>
> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
>
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial [...] (Brasil, 1990).

São exemplos de bens digitais: software, fotos, livros, músicas, mensagens de correio eletrônico e moeda eletrônica.

A IoT, segundo Bruno Miragem (2019), é a técnica que permite conexão física ou virtual entre bens e serviços, por intermédio da internet.

O Decreto n. 9.854, de 25 de junho de 2019, instituiu o Plano Nacional da Internet das Coisas. O artigo 2º, inciso I, do referido Decreto define que internet das coisas é a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com

dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade.

Um dos principais aspectos discutidos acerca da IoT é a perda do conceito tradicional de propriedade, tendo em vista os novos fenômenos trazidos pela tecnologia. Os livros virtuais são exemplos do degaste do conceito de propriedade: o consumidor adquire a licença de uso, mas não sua propriedade.

De acordo com o artigo 2º do Decreto n. 9.854/2019, coisas são objetos do mundo físico ou do mundo digital, capazes de serem identificados e integrados pelas redes de comunicação. Dispositivos são equipamentos ou subconjuntos de equipamentos com capacidade mandatória de comunicação e capacidade opcional de sensoriamento, de atuação, de coleta, de armazenamento e de processamento de dados.

Segundo Bruno Miragem (2019), o desenvolvimento da tecnologia da informação ultrapassou uma fronteira sensível que separa o ser humano das suas invenções, e tal fato se deve ao desenvolvimento da IA.

Um aspecto importante sobre a IA tem relação com o tratamento de dados, seja na concessão de crédito, seja no atendimento ao cliente. Sobre essa colocação, Bruno Miragem (2019) destaca que, em relação ao tratamento de dados, uma das principais questões diz respeito ao risco de, que, mediante o uso da IA, a decisão que dela resulte possa ser conflitante com a proibição de discriminação segundo critérios definidos pelo direito.

A utilização de IA em atendimentos ao consumidor permite uma redução de custos, mas nem sempre esse atendimento atende às demandas dos consumidores. O Decreto n. 7.962/2013, que disciplinou o comércio eletrônico, dispõe nos artigos 2º, 4º e 5º o que as empresas devem oferecer aos consumidores.

A publicidade é uma forma de oferta, que consiste no principal instrumento dos fornecedores para apresentarem ao mercado a sua produção. No Brasil, a publicidade é ferramenta obrigatória de informação.

O artigo 30 do Código de Defesa do Consumidor, Lei n. 8.078/1990, enfatiza a importância da informação e da publicidade:

> Art. 30. Toda informação ou publicidade, suficientemente precisa, veiculada por qualquer forma ou meio de comunicação com relação a produtos e serviços oferecidos ou apresentados, obriga o fornecedor que a fizer veicular ou dela se utilizar e integra o contrato que vier a ser celebrado (Brasil, 1990).

A Constituição Federal determina que compete à lei federal estabelecer os meios legais que garantam à pessoa e à família a possibilidade de se defenderem de programas ou programações de rádio e televisão que propaguem propaganda de produtos, práticas e serviços que possam ser nocivos à saúde e ao meio ambiente:

> [...]
>
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
>
> § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
>
> § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.
>
> § 3º Compete à lei federal:
>
> I – regular as diversões e espetáculos públicos, cabendo ao Poder Público informar sobre a natureza deles, as faixas etárias a que não se recomendem, locais e horários em que sua apresentação se mostre inadequada;
>
> II – estabelecer os meios legais que garantam à pessoa e à família a possibilidade de se defenderem de programas ou programações de rádio e televisão que contrariem o disposto no art. 221, bem como da propaganda de produtos, práticas e serviços que possam ser nocivos à saúde e ao meio ambiente.
>
> § 4º A propaganda comercial de tabaco, bebidas alcoólicas, agrotóxicos, medicamentos e terapias estará sujeita a restrições legais, nos termos do inciso II do parágrafo anterior, e conterá, sempre que necessário, advertência sobre os malefícios decorrentes de seu uso.
>
> § 5º Os meios de comunicação social não podem, direta ou indiretamente, ser objeto de monopólio ou oligopólio.
>
> § 6º A publicação de veículo impresso de comunicação independe de licença de autoridade [...] (Brasil, 1988).

De acordo com os ensinamentos de Paesani (2014), com relação à responsabilidade civil na internet e no mercado informático, o Código de Defesa do Consumidor (Lei n. 8.078, de 1990) incorporou o instituto, e a Constituição Federal de 1988 abrigou o mesmo instituto no artigo 5º, nos incisos V e X:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]

> V – é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;
>
> [...]
>
> X – são 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).

A regra da responsabilidade subjetiva prevista no artigo 159 do Código Civil de 1916 e igualmente prevista nos artigos 186 e 927 do Código Civil de 2002, que consiste na Lei n. 10.406/02:

> [...]
>
> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> [...]
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
>
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. [...] (Brasil, 2002).

Sobre atos ilícitos, a mesma lei disciplinou: "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

Lembrete

A lei civil positivou a responsabilidade objetiva no parágrafo único do artigo 927: "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".

Portanto, existindo dano relevante para a sociedade, e não sendo possível provar a culpa, a lei dispensa a prova, desde que seja comprovado o nexo causal.

4.7 Uso ético e seguro das tecnologias disponíveis

Segundo Paesani (2014), o termo informática tem origem na expressão francesa *information automatique*, adotada por Philippe Dreyfus em 1962, por analogia com o termo inglês *datamation*.

Informática é a ciência que tem por objetivo estudar o tratamento automático da informação, ou seja, o processamento, a coleta, o armazenamento e a difusão da informação pelos meios informáticos, utilizando aparelhos que têm tecnologia para o processamento de dados, como é o caso de notebooks, computadores, celulares, tablets, entre outros.

Os termos informática, telemática, informática jurídica e direito da informática não são sinônimos, uma vez que apresentam significados distintos.

Telemática consiste na ciência que estuda o procedimento para elaboração, utilização e circulação da informação por meio do uso combinado de aparelhos eletrônicos e meios de telecomunicação, ou rede de internet. Trata-se da técnica que aborda a comunicação de dados entre equipamentos informáticos distantes uns dos outros.

Informática jurídica consiste na disciplina que trata da utilização otimizada da informática pelos profissionais ou operadores do direito e nas atividades de natureza jurídica. Ela é a ciência que investiga as leis gerais dos sistemas de tratamento da informação para a utilização pelos juristas e estudiosos do direito, desenvolvendo o trabalho desses profissionais com maior agilidade e rapidez. A utilização dos bens informáticos conectados a um network para peticionar em uma plataforma eletrônica, em sites dos tribunais é um exemplo.

Direito da informática, conhecido como o conjunto de normas que regulam as relações jurídicas que surgem como consequência da aplicação e desenvolvimento da informática, consiste na disciplina que estuda as implicações e problemas jurídicos surgidos com a utilização das modernas tecnologias da informação. Ele pressupõe que a utilização da informática reflete no cotidiano das pessoas influenciando nas relações jurídicas dos usuários.

A Constituição Federal de 1988 tem dado proteção aos usuários das novas tecnologias, assegurando a liberdade informática, sem censura, mas impondo limites. O artigo 5º estabelece que:

> [...] Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

> X – são 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;
>
> [...]
>
> XII – 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).

Segundo Sandra Letícia Schroeder (2013), diante das recorrentes inovações tecnológicas, utilizar a internet e suas interfaces com segurança, conduzida pela conduta ética social e nos termos das leis vigentes, é de extrema importância.

A importância da educação digital como um componente curricular apresenta-se cada vez mais relevante.

Novos comportamentos na sociedade atual são atribuídos à presença das novas tecnologias, em especial, o uso da internet.

Diferentes formas de comunicação, como blog, chat, redes sociais e e-mail, que surgiram com o advento das novas tecnologias, têm cada vez mais relativizado as fronteiras existentes pelos limites geográficos, com especial destaque à crescente conectividade instantânea atribuída à globalização.

Resumo

Nesta unidade, abordamos as noções básicas de legislação profissional, o Marco Civil da Internet, o direito digital, o direito à intimidade, a divulgação de notícias falsas, o uso ético e seguro das tecnologias disponíveis, as novas tecnologias e a internet das coisas.

Com relação às noções básicas de legislação profissional, tratamos dos princípios fundamentais das leis que regulam o exercício de diversas profissões, estabelecendo direitos e deveres dos profissionais em suas respectivas áreas. A legislação profissional aplicada à internet explora as normativas e regulamentações específicas relacionadas ao uso da internet em diversas profissões, considerando questões como privacidade, segurança digital e responsabilidades legais. Apresentamos a legislação internacional, que enfoca as leis que transcendem fronteiras nacionais. Tratados, acordos e convenções buscam padronizar normas legais em contextos internacionais. Vimos aspectos gerais no contexto histórico, social e econômico do Brasil com uma análise da legislação, levando em conta fatores que moldaram o desenvolvimento do país, influenciando as leis ao longo do tempo. Apresentamos casos práticos e reais que exemplificam a aplicação da legislação em situações específicas, permitindo a análise de decisões judiciais e interpretação das leis em contextos concretos.

O Marco Civil da Internet, Lei n. 12.965/2014, estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Ele abrange questões como neutralidade da rede, privacidade, responsabilidade de provedores e liberdade de expressão. A referida Lei tem como objetivo estabelecer diretrizes para o uso da internet no Brasil, visando proteger a privacidade, garantir a liberdade de expressão e definir responsabilidades dos diversos atores no ambiente online. Os aspectos objetivos referem-se às normas e às regras estabelecidas pela lei, enquanto os aspectos subjetivos estão relacionados às interpretações individuais e aplicação prática dessas normas por diferentes agentes, considerando contextos específicos. A tipificação penal refere-se à classificação de condutas como crimes, estabelecendo penas e responsabilidades legais. No contexto do Marco Civil da Internet, a tipificação penal pode abranger atividades como invasão de sistemas, difamação online, entre outras.

Direito digital refere-se ao conjunto de normas e princípios jurídicos que regulam as atividades relacionadas à tecnologia da informação e comunicação, abrangendo questões como privacidade online, responsabilidade civil, propriedade intelectual e crimes digitais.

Vimos que os crimes cibernéticos são infrações cometidas no ambiente digital e incluem atividades como *hacking*, *phishing*, fraudes online e outros delitos que violam a segurança e a integridade de sistemas computacionais e redes. O ciberterrorismo refere-se ao uso de ataques cibernéticos com o objetivo de causar danos graves à infraestrutura de um país. Conflitos digitais envolvem disputas entre nações no ciberespaço, podendo incluir espionagem, sabotagem e outras ações hostis. A espionagem digital inclui a obtenção não autorizada de informações sensíveis, geralmente por governos, organizações ou indivíduos, por meios digitais para obter acesso a dados confidenciais. A prática de utilizar softwares de maneira não autorizada, como a pirataria de programas ou a manipulação de códigos para contornar licenças, é considerada uma infração legal.

Estudamos os limites do direito à intimidade em situações em que a divulgação de notícias falsas viola a privacidade das pessoas. Questões éticas e legais foram exploradas nesse contexto. O direito à intimidade na internet analisa como o direito à intimidade é aplicado no ambiente online, considerando os desafios e as peculiaridades da internet, onde a privacidade pode ser ameaçada de diversas formas. Apresentamos a Lei n. 12.737/12, conhecida como Lei Carolina Dieckmann, que trata de crimes cibernéticos, como invasão de dispositivos eletrônicos, e estabelece penas para essas práticas. Abordamos a tipificação que se refere à classificação e definição legal de condutas no contexto dessa lei, especificando quais atividades são consideradas crimes cibernéticos.

Examinamos a disseminação de informações falsas na internet, seus impactos na sociedade e como a legislação pode abordar esse fenômeno, visando à proteção da verdade e à prevenção de danos. Tratamos do contexto histórico que contextualiza a evolução da disseminação de notícias falsas ao longo do tempo, destacando tendências atuais e os desafios enfrentados na era digital.

Exploramos as implicações legais e éticas relacionadas ao uso crescente de novas tecnologias e à conectividade proporcionada pela internet das coisas (IoT). Por fim, abordamos considerações éticas e legais sobre o uso responsável e seguro das tecnologias, incentivando a adoção de práticas éticas no desenvolvimento e na utilização de novas tecnologias.

Exercícios

Questão 1. A Lei n. 12.965, de 23 de abril 2014, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para as atuações da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Entre os princípios tratados na referida lei, temos:

- a neutralidade da rede;
- a privacidade;
- a liberdade de expressão.

Em relação a esses princípios, avalie as afirmativas.

I – A neutralidade da rede nega o tratamento isonômico para qualquer tipo de dado que circule na rede. Ela garante o acesso somente a alguns conteúdos e desde que tenha ocorrido pagamento por eles.

II – A privacidade refere-se à inviolabilidade e ao sigilo do fluxo das comunicações e das comunicações privadas armazenadas.

III – A liberdade de expressão garante a comunicação e manifestação de pensamento, enfatizando que a decisão sobre a retirada de conteúdo fica condicionada a uma ordem judicial.

É correto o que se afirma em:

A) I, apenas.

B) II, apenas.

C) III, apenas.

D) II e III, apenas.

E) I, II e III.

Resposta correta: alternativa D.

Análise da questão

A Lei n. 12.965/2014 está descrita em 32 artigos, alguns dos quais já antecedem a LGPD quanto à proteção de dados pessoais, exigindo informações claras e completas sobre a coleta, o uso, o armazenamento e o tratamento de dados pessoais. Além disso, ela traz disposições transitórias que focam na "proteção integral da criança e do adolescente e a dignidade da pessoa humana".

Adaptado de: Ruiz (2023).

Em relação aos princípios da neutralidade da rede, da privacidade e da liberdade de expressão abordados na Lei n. 12.965/2014, temos o que segue.

A neutralidade da rede é um princípio que garante que todo tipo de dado seja tratado da mesma maneira, independentemente se é parte de um blog, de uma música ou de um anúncio publicitário. Essa neutralidade também implica "não enxergar" a origem e tampouco o destino do pacote de dados. Na época, esse princípio, tão sedimentado na atualidade, era um impasse entre duas grandes forças: por um lado, as empresas de telecomunicações (Vivo, Claro e TIM, entre outros), que já haviam cabeado as cidades e forneciam conexão à internet; e, por outro lado, os provedores de acesso e conteúdo (grandes veículos da mídia tradicional, além das redes sociais, blogs etc.). As teles pediam o direito de vender pacotes fechados de dados, limitando o acesso a alguns serviços, enquanto os provedores acreditavam que a internet deveria ser completamente neutra e não tolher a liberdade de escolha dos usuários.

Adaptado de: Ruiz (2023).

Em relação à privacidade,

A inviolabilidade e o sigilo do fluxo de comunicação, bem como as mensagens armazenadas, salvo por ordem judicial, na forma da lei, são garantias do Marco Civil da Internet. A inviolabilidade protege uma série de serviços e atendimentos, como dos profissionais da saúde e, claramente, dos profissionais de Direito.

Adaptado de: Ruiz (2023).

No que concerne à liberdade de expressão, o artigo 8º da Lei n. 12.965/2014 afirma que "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet". Vale destacar que o Marco Civil da Internet protege a liberdade de expressão dos usuários online. Isso é um aspecto subjetivo da lei, uma vez que busca equilibrar o direito à liberdade de expressão e os limites estabelecidos pela legislação, como a proibição de conteúdo ilegal.

Questão 2. Vimos que, no Brasil, não existe uma lei equivalente à Lei Sarbanes-Oxley (SOX) dos Estados Unidos, mas nosso país adotou medidas e regulamentações para melhorar a governança corporativa e a transparência das empresas listadas em bolsas de valores.

Alguns aspectos das práticas de governança corporativa no Brasil incluem:

- código de melhores práticas;
- regulamentações e agências;
- regras de contabilidade e auditoria;
- responsabilidade dos gestores.

Em relação a esse tema, avalie as afirmativas.

I – Código de melhores práticas refere-se ao que é estabelecido pela CVM, órgão regulador do mercado de capitais no Brasil que desempenha papel fundamental na regulamentação e na fiscalização das empresas listadas.

II – Regras de contabilidade e auditoria dizem respeito ao fato de as empresas no Brasil seguirem as normas contábeis internacionais (IFRS) e garantirem auditorias independentes das suas demonstrações financeiras.

III – Regulamentações e agências são relativas às legislações brasileiras que estabelecem regras de responsabilidade para gestores de empresas listadas em bolsas de valores.

É correto o que se afirma em:

A) III, apenas.

B) II, apenas.

C) I, apenas.

D) I e II, apenas.

E) I, II e III.

Resposta correta: alternativa B.

Análise da questão

Código de melhores práticas refere-se ao fato de o Brasil ter um Código Brasileiro de Governança Corporativa, que estabelece recomendações e diretrizes para empresas cotadas na Bolsa de Valores de São Paulo (B3).

Regulamentações e agências referem-se ao fato de a CVM ser o órgão regulador do mercado de capitais no Brasil e desempenhar papel fundamental na regulamentação e na fiscalização das empresas listadas. A CVM emitiu resoluções e regulamentações para promover a governança corporativa e a transparência.

Regras de contabilidade e auditoria referem-se ao fato de as empresas no Brasil seguirem as IFRS e garantirem auditorias independentes das suas demonstrações financeiras.

Responsabilidade dos gestores refere-se ao fato de a legislação brasileira estabelecer regras de responsabilidade para gestores de empresas listadas em bolsas de valores, sendo que eles devem prestar contas a acionistas e reguladores.