

UNIDADE I

Legislação Computacional e Ética

Profa. Ma. Irene Kim

Noções introdutórias

- 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 trouxe consigo 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.

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.
- Profissionais são responsáveis por suas ações no desempenho de suas 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.

A legislação profissional aplicada à internet

- A legislação profissional aplicada à internet é um campo em constante evolução que lida com as 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.

Legislação internacional – Lei Sabanes-Oxley

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. Esta 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.

Aspectos gerais no contexto histórico, social e econômico do Brasil

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

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. As soluções para interesses individuais ou coletivos muitas vezes envolvem a intervenção do Estado por meio da jurisdição.
- 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 autoridades.

Fontes do Direito

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 como base para a formação do ordenamento jurídico de um país ou de uma jurisdição específica. Dentre as fontes do Direito, merecem destaque as seguintes:

- Lei.
- Constituição.
- Costumes.
- Jurisprudência.
- Doutrina.

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.

Marco Civil da Internet e crimes cibernéticos

- O Marco Civil da Internet é uma lei brasileira que estabelece princípios, garantias, direitos e deveres relacionados ao uso da internet no Brasil. Foi sancionado em abril de 2014 e é conhecido formalmente como Lei n. 12.965/2014. O Marco Civil da Internet é 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.
- Crimes cibernéticos são atividades ilegais que ocorrem no ambiente digital, muitas vezes explorando vulnerabilidades na tecnologia e na internet.

Interatividade

As partes que estiverem diante de conflito de interesses podem ingressar com uma ação em juízo para que o Estado intervenha e decida uma controvérsia. O termo jurídico que se refere a uma disputa judicial ou litígio entre duas partes que buscam uma solução jurídica, amparada pela lei é:

- a) Perícia.
- b) Mediação.
- c) Arbitragem.
- d) Lide.
- e) Inventário.

Resposta

As partes que estiverem diante de conflito de interesses podem ingressar com uma ação em juízo para que o Estado intervenha e decida uma controvérsia. O termo jurídico que se refere a uma disputa judicial ou litígio entre duas partes que buscam uma solução jurídica, amparada pela lei é:

- a) Perícia.
- b) Mediação.
- c) Arbitragem.
- d) Lide.
- e) Inventário.

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.

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.

- Social: enganar usuários para revelar informações confidenciais, como senhas, através de técnicas enganosas.
- Infiltração de redes: acesso não autorizado a sistemas, redes e servidores para coleta de dados.
- Os governos podem conduzir 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, as empresas e indústrias para roubo de propriedade intelectual, planos de negócios e estratégias. Os ativistas e indivíduos com foco no monitoramento de atividades *online* e *off-line*.
- 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 acompanharem.

- A espionagem digital pode apresentar diversas consequências, como os ataques cibernéticos visando governos, e podem ter implicações significativas para a segurança nacional. Empresas que são alvo de espionagem digital podem sofrer 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, podem prevenir ou mitigar esse crime. Outra ação pode ser 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 pela espionagem digital 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.

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 a 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 toda cópia não autorizada, isto é, a obtenção, instalação ou distribuição de cópias de software sem a devida autorização do detentor dos direitos autorais. Ativação fraudulenta quando se utiliza de manipulação de métodos de ativação ou uso de chaves de licença falsas para contornar os mecanismos de proteção.

Uso ilícito de softwares

Quais são 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.

Interatividade

Diferentemente da espionagem tradicional, a espionagem digital ocorre no ciberespaço e muitas vezes envolve métodos altamente sofisticados. A espionagem digital, também conhecida como ciberespionagem, refere-se ao uso de tecnologias da informação e comunicação para coletar:

- a) Informações confidenciais.
- b) Segredos industriais.
- c) Dados estratégicos.
- d) Outras informações sensíveis.
- e) Todas as alternativas anteriores.

Resposta

Diferentemente da espionagem tradicional, a espionagem digital ocorre no ciberespaço e muitas vezes envolve métodos altamente sofisticados. A espionagem digital, também conhecida como ciberespionagem, refere-se ao uso de tecnologias da informação e comunicação para coletar:

- a) Informações confidenciais.
- b) Segredos industriais.
- c) Dados estratégicos.
- d) Outras informações sensíveis.
- e) Todas as alternativas anteriores.

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.

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 direito à intimidade na internet

- 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.

Noções gerais e aspectos da Lei n. 12.737/12

- A Lei n. 12.737/2012, popularmente conhecida como "Lei Carolina Dieckmann", foi criada em resposta a um caso de grande repercussão no Brasil envolvendo 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 Carolina Dieckmann introduziu mudanças no Código Penal, incluindo a tipificação de crimes específicos relacionados a invasões de dispositivos informáticos e a divulgação não autorizada de conteúdo íntimo.

Noções gerais e aspectos da Lei n. 12.737/12

- A lei estabelece penalidades para quem invade dispositivos informáticos alheios, seja 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.
- Um dos principais aspectos da lei é a criminalização da divulgação não autorizada de conteúdo íntimo. 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 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. Este 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 e rápida propagação nas redes sociais

- 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.
- 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.
 - Fake news pode 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.

Impacto na opinião pública e motivações por trás da criação de fake news

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

Responsabilidade das plataformas digitais e educação e alfabetização digital

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

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

Interatividade

As consequências de não lidar efetivamente com *fake news* podem minar a confiança na informação, comprometer a democracia e criar desafios duradouros para a sociedade. Enfrentar *fake news* na internet exige uma abordagem complexa, abrangendo:

- a) Educação.
- b) Regulamentação.
- c) Tecnologia.
- d) Colaboração global.
- e) Todas as alternativas anteriores.

Resposta

As consequências de não lidar efetivamente com *fake news* podem minar a confiança na informação, comprometer a democracia e criar desafios duradouros para a sociedade. Enfrentar *fake news* na internet exige uma abordagem complexa, abrangendo:

- a) Educação.
- b) Regulamentação.
- c) Tecnologia.
- d) Colaboração global.
- e) Todas as alternativas anteriores.

As novas tecnologias e a internet das coisas

- As novas 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, cada vez mais, os atos relativos ao Judiciário estão sendo realizados por meio eletrônico.
- A internet impulsionou um expressivo mercado de consumo virtual, no qual as trocas e compras são realizadas por meio eletrônico.

Legislação

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 5°, 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:"

Legislação

A regra da responsabilidade subjetiva está prevista nos artigos 186 e 927 do Código Civil de 2002 (Lei n. 10.406/02), conforme segue:

- "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."

Legislação

- 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.

Bens digitais

- 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."

- Segundo Paesani (2014), o termo informática é um neologismo de origem francesa, extraído da expressão 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, dentre outros.

- Os termos informática, telemática, informática jurídica e direito da informática não são sinônimos, uma vez que possuem 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. É a técnica que trata da 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. Informática jurídica 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 destes 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. Direito na informática 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. A Carta Maior, no seu artigo 5º estabelece que:

"Art. 5°. 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 à 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;"
- O digital como um componente curricular apresenta-se cada vez mais relevante.

Interatividade

O Código de Defesa do Consumidor define o que é o fornecedor. De acordo com o Código, **não** pode ser fornecedor:

- a) Pessoa física.
- b) Pessoa jurídica.
- c) Pessoa política.
- d) Pessoa pública.
- e) Pessoa privada.

Resposta

O Código de Defesa do Consumidor define o que é o fornecedor. De acordo com o Código, **não** pode ser fornecedor:

- a) Pessoa física.
- b) Pessoa jurídica.
- c) Pessoa política.
- d) Pessoa pública.
- e) Pessoa privada.

Referências

- CÓDIGO CIVIL. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm
- CÓDIGO DE DEFESA DO CONSUMIDOR.
 https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm
- CÓDIGO PENAL. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.
- CONSTITUIÇÃO FEDERAL. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm.
 - LEI N. 12.965 de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
 - LEI N. 12.737 de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

ATÉ A PRÓXIMA!