FACULDADE DE COMPUTAÇÃO E INFORMÁTICA TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS



UNIVERSIDADE PRESBITERIANA MACKENZIE

CEDaD - Centro de Educação a Distância







Reitor: Benedito Guimarães Aguiar Neto

Vice-Reitor: Marco Tullio de Castro Vasconcelos

Chanceler: Davi Charles Gomes

PRÓ-REITORIA DE GRADUAÇÃO E ASSUNTOS ACADÊMICOS

Pró-Reitor: Cleverson Pereira de Almeida

CENTRO DE EDUCAÇÃO A DISTÂNCIA

Coordenadora Geral: Esmeralda Rizzo

Coordenadora de Apoio Técnico-Administrativo: Jussara Cristina Paulon

Coordenadora de Apoio Didático-Pedagógico: Ana Lúcia de Souza Lopes

Coordenadores da Produção de Materiais Didáticos:

Solange Palma de Sá Barros

Ubirajara Carnevale de Moraes

COMISSÃO DE CONCEPÇÃO E ACOMPANHAMENTO PEDAGÓGICO

Ana Lúcia de Souza Lopes

Esmeralda Rizzo

Marili Moreira da Silva Vieira

Solange Duarte Palma de Sá Barros

Ubirajara Carnevale de Moraes

© 2016 Universidade Presbiteriana Mackenzie (UPM).

Todos os direitos reservados à Universidade Presbiteriana Mackenzie (UPM). Nenhuma parte desta publicação poderá ser reproduzida em qualquer meio ou forma sem a prévia autorização.

Dados Internacionais de Catalogação na Publicação (CIP) (Câmara Brasileira do Livro, SP, Brasil)

> Universidade Presbiteriana Mackenzie Rua da Consolação, 930 São Paulo - SP - CEP 01302-907 Tel.: (11) 2114-8000 www.mackenzie.br

SUMÁRIO

Apresentação da Disciplina	5
Everton Knihs	
Unidade 1 - Segurança e Mecanismos de Segurança	6
Unidade 2 - Direito Digital	22
Unidade 3 - Forense Computacional	48
Unidade 4 - Aspectos do Direito Relacionados com o Profissional de Informática	62







APRESENTAÇÃO DA DISCIPLINA

Segurança e direito digital é uma disciplina que trata de aspectos importantes da área de tecnologia. Ela se comporta como conteúdo transversal e extremamente fundamental para a atuação profissional. O que estudaremos não possui uma disciplina como pré-requisito. A abordagem do conteúdo será dividida a seguir para que você compreenda e acompanhe as unidades.

Na unidade um, você estudará os conceitos pertinentes à segurança da informação, análise de riscos, *malwares*, política de segurança e *cloud computing*. Será uma apresentação das estruturas fundamentais e dos conceitos de segurança em meios computacionais.

Na unidade dois, você estudará o Direito Digital e o Marco Civil da *Internet*. Você conhecerá os aspectos da Propriedade Intelectual e Privacidade, que ajudarão a compreender os aspectos relacionados à Segurança e ao Direito Digital e conhecimentos de fato, relação e norma jurídica.

A unidade três aborda a Forense Computacional, Perícia e os Atos ilícitos e crimes eletrônicos. Você identificará as normas relacionadas aos profissionais de Tecnologia da Informação e conhecerá o porquê de elas não poderem ser desobedecidas.

Na unidade quatro, você estudará os aspectos do direito relacionados ao profissional de informática, como o direito do trabalho, as relações de trabalho e o comércio eletrônico, que conceituarão os temas do direito com a atuação profissional na área de tecnologia da informação.

5

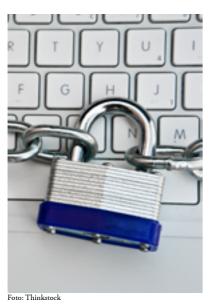


SEGURANÇA E MECANISMOS DE SEGURANÇA

A popularização e o avanço tecnológico proporcionaram uma nova e extraordinária maneira das pessoas se comunicarem, motivando a democratização da informação e oferendo novas formas de relações profissionais, de consumo e de serviços.

O comércio eletrônico, as transações bancárias, as notícias jornalísticas ou as informações econômicas, científicas, médicas, culturais etc. são exemplos de uma dinâmica na sociedade moderna que necessita cada vez mais de acesso rápido e eficiente aos meios informáticos. A segurança da informação surge nesse contexto. O desenvolvimento tecnológico avança juntamente com a necessidade de privacidade em sistemas computacionais.

A internet e os sistemas computacionais podem sofrer invasões ou ataques indesejados por pessoas desautorizadas, com programas de computador ou conhecimentos técnicos de acesso aos dados individuais ou corporativos, evidenciando problemas na segurança e caracterizando alguns crimes ou delitos informáticos, como fraudes, violação e invasão de dispositivos informáticos ou instalação de vulnerabilidades sem prévia autorização.



Nesta unidade, discutiremos o tema segurança, apresentando problemas e respectivas soluções para proteção em sistemas informáticos. Você estudará os conceitos pertinentes à segurança da informação, à análise de riscos, aos malwares, à política de segurança e ao cloud computing, que introduzirão a caracterização de segurança sobre informações pessoais ou corporativas, indicando uma atenção para exposições ao risco inerente ao uso da tecnologia como meio de comunicação.



OBJETIVOS DE APRENDIZAGEM

FATOS E CONCEITOS

- Apresentar as estruturas fundamentais e conceitos de segurança.
- Entender os aspectos relacionados a Segurança e ao Direito Digital e suas noções de fato, relação e norma jurídica.
- Reconhecer as fontes do direito e entender como funciona a hierarquia das leis no ordenamento jurídico.
- Conhecer os principais ramos do Direito Digital e políticas de segurança.

2 PROCEDIMENTOS E HABILIDADES

- Conceituar os temas fundamentais de Segurança na tecnologia.
- Compreender os conceitos e a estrutura do Direito Digital.
- Conhecer os aspectos de propriedade intelectual, privacidade e computação forense.
- Identificar as normas que obrigam os profissionais de Tecnologia da
- Informação e por que não podem ser desobedecidas.

3 ATITUDES, NORMAS E VALORES

- Dominar os conceitos de Segurança em meios computacionais.
- Planejar a segurança e proteção dos sistemas e reconhecer os elementos relacionados ao direito digital.
- Reconhecer os seus direitos para que se possa exercê-los.
- Tomar as providências cabíveis ao caso concreto sempre que for necessário.
- Respeitar a lei ao tomar decisões no exercício da sua atividade profissional.



EXPLORANDO OS CONCEITOS



Fórum: Durante toda abordagem dos conceitos apresentados nesta unidade, caso tenha alguma dúvida ou queira apresentar um caso prático, você poderá questionar e discutir no fórum específico

"Fórum – Unidade 1" – o canal de interação entre os participantes desta disciplina no Ambiente Virtual.

O uso da tecnologia é essencial nos tempos modernos, mas pode gerar conflitos e contratempos, como a possibilidade de envio de um e-mail não autorizado, troca de informações ou invasão e captura de dados de forma não autorizada.

A segurança em meios informáticos torna-se necessária em um mundo cada vez mais tecnológico. Abordaremos os diversos riscos envolvidos no uso da *internet* e seus métodos de prevenção e discutiremos as formas que podem aumentar a segurança de um computador. Os riscos e medidas preventivas para o uso de sistemas computadorizados são temas importantes para o conhecimento do profissional da área de tecnologia da informação, auxiliando na segurança de programas de troca de mensagens, de distribuição e compartilhamento de arquivos. Você perceberá a importância da realização de cópias de segurança, *backups*, baseadas em uma política de segurança, de controle e de direito de acesso.



Assista: o vídeo "Os Profissionais 27 – Tecnologia no Cotidiano, Mercado de Trabalho e Startup Weekend" (até 8:01 min), que trata do crescimento de informações no campo cibernético e da profissão

na área de informática.

SEGURANÇA E CUIDADOS BÁSICOS EM MEIOS INFORMÁTICOS

A atuação profissional em diversas áreas econômicas utiliza, maciçamente, recursos para armazenar e processar informações das atividades desenvolvidas. Esta questão também é válida na esfera pessoal da utilização dos recursos informáticos.



Foto: Thinksto

A internet está cada vez mais presente no seu cotidiano, facilitando o acesso a informações. Você pode acessar sites de entretenimento, de esportes e de notícias, pode jogar, fazer compras, consultar serviços bancários, pode estudar e frequentar cursos educacionais, conversar com amigos e familiares. Todos estes acessos devem ser de forma segura. Com algumas medidas preventivas, você evitará riscos de exposição.

Alguns riscos devem ser analisados para a criação de uma cultura de segurança:

Cuidado com o Controle de Acesso – O acesso a conteúdos impróprios ou ofensivos, contatos com pessoas mal-intencionadas, dificuldades de manter sigilo, divulgação de boatos, uso excessivo, invasão de privacidade, plágio ou violação de direitos autorais são alguns exemplos de acesso indiscriminado, que afetam a segurança em sistemas informáticos. A falta de controle nos acessos caracteriza um problema decorrente de falha humana, não informática. O controle de acesso deve existir em sistemas computacionais, evitando consequências negativas, coibindo e restringindo irregularidades. O acesso não autorizado poderá surgir em um ambiente com falta de controle. Entre os acessos não autorizados estão os *hackers*, vírus, cavalo de Troia, *cookies*, janelas de *pop-up*, *banners* de propaganda, *links*, entre outros.

Cuidado na Retenção e na Concentração de Informações ou Funções – Concentrar dados em um único equipamento computacional, com acesso restrito de um único usuário, bem como a retenção de informações por um único usuário, torna-se um risco devido a possibilidade de ataque ao equipamento, que além de furtar informações, poderá apagá-las ou impossibilitar seu acesso futuro. A concentração de funções torna uma organização vulnerável, aumentando o risco de violações de informações, que poderão passar desapercebidas.

Cuidado com Informações Imprecisas — As informações imprecisas ou obscuras tornam-se um problema relacionado com a maioria dos acessos e compartilhamento de dados e informações, pois não saber a origem ou o conteúdo das informações inseridas ou acopladas é, algo comum na transferência e recebimento de dados; isso pode trazer códigos maliciosos, *malwares*, que poderão invadir ou comprometer o sistema computacional. A introdução de erros, dados ou programas que induzem a interpretação ou informação inválidas podem processar e propagar dados que, em grande escala serão difíceis de eliminar.

Você poderá adotar algumas formas de prevenção e proteção em casos de insegurança ou falta de cuidado com os sistemas computacionais que ajudarão nos aspectos de controle e segurança, como a utilização de senhas individuais e de acesso autorizado, controle dos acessos dos usuários, organização do conteúdo informatizado, identificação e responsabilização de ações danosas por meio da fiscalização contínua.



Fórum: A partir dos conceitos elencados, vá até o fórum de discussão "Fórum – Unidade 1" no Ambiente Virtual e apresente um caso prático ou um exemplo de cuidado em meios informáticos

que aumente a segurança.



Assista: o vídeo "Segurança da Informação: por onde eu começo?", uma Palestra do Professor Adriano Mauro Cansian (Unesp) ministrada no Campus Party em 2014, que trata sobre Segurança da Informação.

CÓDIGOS MALICIOSOS – MALWARES

Os códigos maliciosos são conhecidos *malwares* em sistemas informáticos. Esses códigos são programas que possuem o intuito de executar ações impróprias, danosas, visando prejudicar e interferir no funcionamento dos sistemas computacionais. As atividades maliciosas passam a ter acesso ao sistema computacional, executando ações indesejadas. O acesso a dados armazenados por códigos maliciosos interfere e opõe-se diretamente no conceito de segurança, pois o objetivo é obter informações sigilosas, confidenciais e pessoais, acessar informações financeiras ou praticar vandalismo, prejudicando o funcionamento ou comprometendo os dados armazenados.

Entre as diversas formas de infestação de *malwares*, as mais comuns formas de contato são por meio de programas em mídias removíveis, como o *pendrive*, ao acessar *sites* que contenham anexos arquivos executáveis maliciosos, mensagens infectadas em *e-mails*, entre outros.

Os *malwares* podem ser classificados ou divididos entre vírus, *spyware*, cavalo de Troia, *worm*, *bot*, alçapão ou *backdoor*.

Vírus – O vírus é um código ou parte de um código malicioso que é instalado sem autorização. Ele se propaga pelo sistema computacional, tornando-se parte de arquivos e programas, que podem permanecer ocultos, mas infectando arquivos e executando atividades não autorizadas sem que os usuários do sistema computacional percebam; fazendo autocópias, ou seja, multiplicando-se e infectando outros arquivos ou contatos que possam acontecer, por e-mails, mensagens, transferência de dados, anexos, ou mídias removíveis.

Spyware – O spyware é um programa de computador que monitora informações de um sistema computacional e as fornece a terceiros. Este programa poderá ser utilizado de forma legítima como forma de controle, mas geralmente funciona de maneira não autorizada e maliciosa. O spyware executa ações no

sistema computacional de maneira indesejada, altera configurações, páginas iniciais de web; monitora sites durante a navegação captura informações tecladas ou acessadas, vasculha dados e arquivos, inclusive localização e monitoramento do mouse e teclado durante a visita a uma página web.

Cavalo de Troia – O cavalo de Troia é um programa de computador que executa funções aparentes e maliciosas, esta de forma oculta, sem autorização ou conhecimento do usuário. Geralmente, o cavalo de Troia pode estar associado a programas ou a arquivos anexados, como jogos, fotos, protetores de tela, cartões virtuais etc. Entre as ações maliciosas do *malware*, pode-se citar a captura e o envio de senhas e dados financeiros para terceiros ou para o invasor, destruição ou alteração de arquivos, instalação de outros *malwares*. O cavalo de Troia se diferencia do vírus e do *worm* pois não se propaga instantaneamente e não realiza autocópias. Este *malware* geralmente possui um único arquivo que poderá ser executado, de forma programada, podendo ficar inativo por algum tempo e executar atividades maliciosas conforme seu objetivo prévio.

O termo cavalo de Troia surgiu na mitologia grega. Durante a guerra de Troia, os gregos enviaram uma grande estátua em forma de cavalo à cidade. A estátua do cavalo continha soldados gregos em seu interior. Eles esperaram os troianos festejarem a "vitória" e, à noite, abriram os portões da cidade de Troia para o exército grego, que acabou por dominar a cidade. Assim, surgiram as expressões "cavalo de Troia", simbolizando uma ação oculta esperando o momento oportuno para sua execução, e "presente de grego", que determina um presente no qual não se pode confiar.



Worm – O worm é um programa de propagação automática entre sistemas computacionais, enviando cópias desse mesmo programa entre os computadores. Ele é diferente do vírus, pois – ao se propagar e infectar novos sistemas computacionais – o worm executa sua cópia nos novos sistemas, buscando vulnerabilidades para esta execução.

Bot – O bot é um programa de computador destinado a propagação automática, similar ao worm, buscando falhas e vulnerabilidades em softwares e configurações. Diferencia-se dele, pois envia informações ao invasor, permitindo que este controle o sistema computacional a distância. Quando vários computadores são invadidos por bots, eles formam uma rede controlada remotamente, chamada de botnet, que controla os computadores infectados a distância.

Alçapão ou *Backdoor* – O termo alçapão ou *backdoor* tem origem na associação entre passagens secretas ou passagens para entrada no sistema computacional. São caminhos de acesso ao computador utilizados por invasores experientes, pois o usuário não percebe a falha na segurança Este *malware* é uma maneira de retornar ao sistema computacional sem ser notado, ou precisar de novos métodos para invasão; é uma forma de deixar o caminho de acesso sempre disponível para o invasor. A instalação desta ação maliciosa se dá por um cavalo de Troia e determina o controle e acesso remoto dos invasores.

Para saber mais: Código Malicioso foi adaptado para o português; em inglês é designado como *Malware*, que deriva da junção de *Malicious Sofware*.

VULNERABILIDADE

A vulnerabilidade é uma falha de projeto, no processo, na configuração ou na fase implementada de aplicação e uso de *sofwtares* ou sistemas computacionais e operacionais. Esta falha é uma ameaça à segurança. Sistemas operacionais

ou *softwares* desatualizados, instalações defeituosas, acesso e autorizações inadequadas, falhas na configuração da rede de acesso, ausência de equipamentos necessários, entre outros exemplos, podem ser considerados falhas e, assim, determinam o conceito de vulnerabilidade que ameaça a segurança do sistema computacional e dos recursos envolvidos.

Vulnerabilidades podem ser encontradas desde o aspecto estrutural, como instalações suscetíveis a perigos físicos (incêndios, depreciação material, vazamentos de líquidos ou material químico), até o aspecto natural, como desastres naturais, aumento de temperatura ou umidade. Outros aspectos sobre as vulnerabilidades seriam os relacionados a falhas tecnológica, de instalação ou de configuração dos *softwares*, aos acessos indesejados ou desautorizados e à usabilidade, devido a falhas humanas por desconhecimento ou mau uso de sistemas ou de equipamentos, de forma intencional ou não.

Estas falhas ou vulnerabilidades precisam ser revistas e identificadas para sanar todo o risco envolvido. As vulnerabilidades são a porta de entrada dos *malwares*.

ENGENHARIA SOCIAL

Engenharia Social é considerada a habilidade de persuasão, a habilidade de conseguir dados confidenciais por meio do trato social. É considerado um método de invasão, uma forma de ataque à segurança com o uso da persuasão para obter acesso não autorizado a informações ou a sistemas computacionais. Esta habilidade é um risco à segurança da informação, induzindo um usuário a executar tarefas ou fornecer informações sigilosas. Este método de ataque pode ocorrer por diversos meios, como e-mails, ligações telefônicas, sites que induzem fraudes no comércio eletrônico, entre outros.

Para se proteger deste tipo de ataque e diminuir o risco, você não deve fornecer dados importantes, como senhas ou informações financeiras, não deve executar programas recebidos ou clicar em *links* contidos em e-mails. Informe-se sobre a procedência da mensagem ou das ligações telefônicas, verificando a veracidade

das solicitações e dos diálogos estabelecidos. No caso de atividades corporativas, treinamentos de funcionários e alertas sobre essa forma de abordagem que compromete a segurança deverá ser detalhada, como forma de prevenção.

POLÍTICA E MECANISMOS DE SEGURANÇA

A política e os mecanismos adotados para a segurança em sistemas computacionais são medidas a serem tomadas com o intuito de proteção e diminuição de riscos de ataques e de invasões de programas maliciosos. Para diminuir o risco de ataque ao seu computador, além de deixar seu sistema computacional sempre atualizado, sugere-se a instalação de mecanismos de segurança como *firewalls* e *antimalwares*.

Outra medida importante é o cuidado no recebimento de arquivos anexos em *e-mails* e comunicações gerais, no *download* de arquivos desconhecidos e no acesso a *sites* não confiáveis.

•

Assista: o vídeo "Tratamento de Incidentes de Segurança na Internet, explicado pelo NIC.br" (2014), do Núcleo de Informação e Coordenação do Ponto BR e do Centro de Estudos, Respostas e

Tratamento de Incidentes de Segurança no Brasil. Ele relata a temática abordada até o momento, o que poderá auxiliá-lo na compreensão do conteúdo.

Adotar uma política de segurança é uma ação importante para estabelecer e manter um sistema computacional seguro, restringindo as possibilidades de danos e diminuindo os riscos inerentes à tecnologia.

A política de segurança é uma medida fundamental para determinar as responsabilidades e os direitos dos usuários sobre os aspectos envolvidos com a segurança da informação e com os recursos computacionais. Este mecanismo de segurança envolverá formas de tratamento e condução de ações sobre os cuidados a serem observados: senhas e acessos, *backups* de dados e arquivos, informações pessoais ou institucionais. Formalizar esta política de segurança na

forma documental é outra medida importante, estabelecendo os termos de uso de sistemas computacionais e atitudes dos usuários.

Adotar sistemas seguros e menos vulneráveis, controlar o acesso a informações, instalar softwares que detectam malwares, manter os sistemas computacionais sempre atualizados e ser cauteloso com a engenharia social, tomando medidas de prevenção aos diversos tipos de riscos e ataques, fazem parte de uma política de segurança e são considerados mecanismos importantes de combate a fraudes relacionadas a sistemas computacionais. O desenvolvimento de sistemas computacionais também requer atenção para a construção de aplicações seguras, que atendam políticas e mecanismos de segurança.

CRIPTOGRAFIA



A criptografia é uma técnica de escrever mensagens de maneira cifrada ou por meio de códigos. Essa técnica utiliza uma comunicação codificada, secreta, e auxilia na transferência de dados e informações que não devem ser interceptadas ou acessadas.

Uma informação criptografada autentica a identidade dos usuários, protege os dados e informações pessoais, auxiliando na integridade das informações acessadas e comunicadas. As informações criptografadas podem identificar o remetente e, desse modo, são caracterizadas como informações privadas, de remetente para destinatário, somente acessadas por estes dois usuários.

A criptografia auxilia na segurança dos dados, considerado um método seguro para transmissão e acesso de informações privadas. Você pode usar a criptografia para proteger arquivos e senhas, proteger uma área específica no seu computador (criada para armazenar informações), criptografar dados financeiros, backups, e-mails ou mensagens.



APROFUNDANDO CONCEITOS

Você poderá aprofundar os conceitos estudados com as sugestões a seguir, visitando alguns sites ou lendo livros que tratam a respeito de segurança, de criptografia, que dão dicas e informações gerais sobre o tema, como também assistir aos vídeos destacados que apresentam uma palestra sobre o tema Segurança da Informação e sobre três profissionais relacionados à área de segurança e tecnologia.

- Criptografia e segurança de redes: princípios e práticas, de Willian Stallings (2010).
- Dicas de segurança (2005) do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (Cert.br).
- Computer Security Incident Response Team (CSIRT). FAQ do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil.
- Tratamento de Incidentes de Segurança na Internet, explicado pelo NIC.br. Núcleo de Informação e Coordenação do Ponto BR. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil.
- Segurança da Informação: por onde eu começo? Palestra do Professor Adriano Mauro Cansian - UNESP - no Campus Party 2014 sobre Segurança da Informação.
- Assista ao vídeo Tecnologia no cotidiano do Programa Os profissionais (0:00 - 8:01).



Nesta unidade, estudamos aspectos importantes da segurança em recursos computacionais e mecanismos de segurança para proteção e precaução sobre possíveis riscos relacionados à informática.

Compreendemos que é necessário adotar medidas de segurança e aplicar uma política preventiva relacionada a riscos que envolvem os sistemas informáticos e de navegação web.

Tais medidas nos protegem completamente de ataques? E se pensarmos em sistemas computacionais seguros, o comportamento humano influencia uma possível falha na segurança? Uma simples configuração de data e hora no computador, atualização de softwares ou sistemas operacionais, falta de senhas de acesso ou falta de instalação de detectores de malwares podem ser considerados como riscos. No entanto, essas atitudes são consideradas falha do usuário ou da política de segurança?

Para auxiliá-lo nesse processo de síntese, responda a estas questões, partindo dos conceitos apresentados e das situações do cotidiano.



REFERÊNCIAS

- ▶ BOSWORTH, S.; KABAY, E. M.; WHYNE, E. Computer security handbook. Nova York: Willey, 2014.
- CARUSO, C. A. A.; STEFFEN, F. D. Segurança em informática e de informações. São Paulo: Senac, 1999.
- CSIRT FAQ. Cert.br, 19 mar. 2012. Disponível em: http://moodle.mackenzie.br/link/1ag>. Acesso em: 4 abr. 2016.
- FARMER, D.; VENEMA, W. Perícia forense computacional: teoria e prática aplicada. São Paulo: Pearson Prentice Hall, 2007.
- ▶ LIMA, P. M. F. Crimes de computador e segurança computacional. 2. ed. São Paulo: Atlas, 2011.
- MARTINS, S. P. Instituições de direito público e privado. 3. ed. São Paulo: Atlas, 2003.
- MEDHI, D.; RAMASAMY, K. Network routing: algoritms, protocols, and architectures. Amsterdam: Elsevier; Boston: Morgan Kaufmann Publishers, 2007.
- NAKAMURA, E. T.; GEUS, P. L. Segurança de redes em ambientes cooperativos. São Paulo: Novatec, 2012.
- NG, R. Forense computacional corporativa. Rio de Janeiro: Brasport, 2007.

- OS PROFISSIONAIS 27 TECNOLOGIA NO COTIDIANO, MERCADO DE TRABALHO E STARTUP WEEKEND. Direção e produção: TV Mackenzie. São Paulo: Universidade Presbiteriana Mackenzie, 4 dez. 2015. Disponível em: http://moodle.mackenzie.br/link/lao. Acesso em: 6 jul. 2016.
- REIS, H. M.; REIS, C. N. P. Direito para administradores. São Paulo: Thomson, 2006. 1 v.
- STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. São Paulo: Pearson Education do Brasil, 2010.
- SÊMOLA, M. Gestão da segurança da informação: visão executiva da segurança da informação. Rio de Janeiro: Campus, 2003.
- SOMMERVILLE, I. Engenharia de software. 8. ed. São Paulo: Pearson: Addison Wesley, 2011.
- TRATAMENTO DE INCIDENTES DE SEGURANÇA NA INTERNET, EXPLICADO PELO NIC.BR. Produção: Antônio Marcos Moreira. São Paulo: Nic.br, 10 nov. 2014. Disponível em: http://moodle.mackenzie.br/link/1am>. Acesso em: 7 jul. 2016.
- TANENBAUM, A.; WETHERALL, D. Redes de computadores. 5. ed. São Paulo: Pearson, 2011.
- TURBAN, E.; RAINER, R. K.; POTTER, R. E. Introdução a sistemas de informação: uma abordagem gerencial. Rio de Janeiro: Campus, 2007.

UNIDADE 2

DIREITO DIGITAL

Nesta unidade você estudará os conceitos e especialidades de Direito relacionados com o mundo Digital, bem como os princípios desta matéria.

Para introdução temática do direito digital, reflita, primeiramente, sobre os questionamentos a seguir: O que é o Direito? O que entendemos como Direito?

O conceito de direito é complexo, podemos defini-lo como "[...] a ordenação ética coercível, heterônoma e bilateral atributiva das relações sociais, na medida do bem comum. Sua definição, portanto, apresenta a soma das características gerais e distintivas das normas éticas" (REALE, 2003, p. xx).

Para Miguel Reale, o direito poderá ser divido a partir da tridimensionalidade ética, chamados fato, valor e norma. Esses três elementos congregam a distinção de um simples fato, verificando que o valor está relacionado ao bem comum por meio do surgimento de normas consideradas éticas, que limitam os fatos de forma coercível conforme sua atribuição. Nesta visão, o fato social decorre do valor humano de forma anterior a norma imposta, distinguindo os fatos conforme a valoração atribuída, que resultará em uma norma específica.

Para Vicente Rao (1991, p. xx):

é o direito um sistema de disciplina social fundado na natureza humana que, estabelecendo nas relações entre os homens uma proporção de reciprocidade nos poderes e deveres que lhes atribui, regula as condições existenciais dos indivíduos e dos grupos sociais e, em consequência, da sociedade, mediante normas coercitivamente impostas pelo poder público.

A imposição da norma, pelo Estado, aos atos praticados pelo ser humano durante as relações e atividades sociais, independe da especialidade jurídica, ou seja, da norma trabalhista penal, civil, constitucional, entre outras. Deste modo, o direito digital também possui definições inerentes ao direito e à necessidade de sua observação para cumprimento das normas vinculadas.

Mas por que temos a necessidade de regulação, pela norma, do uso da informática?

O desenvolvimento tecnológico modifica a forma pela qual todos se relacionam e se comunicam, encurta distâncias, otimiza processos, auxilia tratamentos e cuidados com a saúde, organiza e simplifica finanças e economias. É nesse aspecto que a necessidade de normas claras se apresenta. Com todas as modificações que a informática trouxe, torna-se imprescindível para o relacionamento humano, bem como para as regulamentações de comportamento no ambiente virtual, a definição de parâmetros a fim de dirimir conflitos.

O direito digital encontra respaldo em diversas normas. No âmbito da Constituição Federal (BRASIL, 1988), também chamada de Carta Magna, temos o artigo Art. 5°, incisos IX, X, XII, XIV, o Art. 22, inciso IV e o Art. 220, § 1º, que se referem a esta matéria. Veja, em detalhes, o que a legislação aponta.

O dispositivo legal constitucional serve como base técnica e fundamento para a evolução da legislação, com a edição de novas leis infraconstitucionais.



A qualquer momento, caso tenha alguma dúvida ou queira discutir sobre o tema em estudo, você poderá apresentar os questionamentos no fórum específico desta unidade, chamado "Fórum – Unidade

2", um canal de interação entre os participantes desta disciplina.





EXPLORANDO OS CONCEITOS

Você entenderá, neste momento, uma parte importante do direito digital que assegura direitos e estabelece uma base de princípios para o uso da Internet no Brasil, a lei chamada de Marco Civil da Internet. Também será apresentado o conteúdo sobre Propriedade Intelectual, matéria importante e necessário para o conhecimento do profissional de informática.

Durante toda abordagem dos conceitos apresentados nesta unidade, caso tenha alguma dúvida ou queira apresentar alguma experiência, você poderá apresentar e discutir no fórum específico "Fórum – Unidade 2", um canal de interação entre os participantes desta disciplina.



Assista ao vídeo "Documentário – A Verdadeira História da Internet – 01 – A Guerra dos Navegadores – Discovery Channel" (2013).

Ele trata sobre a história da internet, um documentário que ajudará a entender a contemporaneidade da rede e a navegação em rede.

MARCO CIVIL DA INTERNET: O USO DA INTERNET, A LIBERDADE, A PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS E A NEUTRALIDADE DA REDE

O Marco Civil da Internet, Lei nº 12.965/2014, é uma lei infraconstitucional que estabelece a norma para o uso da Internet, parâmetro primordial para dirimir conflitos e orientar provedores e usuários sobre a conduta que devem adotar. Esta lei não esgota a matéria, mas torna-se um referencial para interpretações jurisprudenciais.

O Brasil foi considerado inovador com a publicação de uma legislação sobre a Internet. Considerado o quarto país a adotar uma lei sobre esta matéria, depois da Eslovênia, Holanda e Chile, pioneiros na publicação de lei respectiva.

Visite a Lei nº 12.965, procure se inteirar sobre o conteúdo disposto.

No artigo Art. 1º do Marco Civil da internet, você encontra orientações sobre o que a lei estabelece: os "[...] princípios, garantias, direitos e deveres para o uso da internet no Brasil e [a determinação das] diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria" (BRASIL, 2014).

Os direitos definidos na Lei n. 12.965/14 podem ser elencados como a liberdade de expressão nos termos da Constituição Federal, que considera a Internet um ambiente democrático, aberto, livre, preservando a intimidade e a vida privada. Outro direito encontrado é o da proteção da privacidade e dos dados pessoais, que somente serão repassados a terceiros se autorizado pelo usuário ou por decisões judiciais.

A guarda de informações dos provedores se dará pelo prazo que a lei fixar e serão utilizados somente com autorização do usuário ou decisão judicial, que poderá solicitar, também, a retirada do conteúdo do ar. A neutralidade da rede, após amplo debate legislativo, entrou como um direito definido pelo Marco Civil da Internet, determinando que os provedores de acesso devem tratar todos da mesma forma, sem distinção do conteúdo, origem, destino ou serviço.

A Responsabilização pelo conteúdo postado na internet será dos usuários, definindo que a empresa de conexão não será responsabilizada pelo conteúdo postado por clientes.

Outras normas, como o Código de Defesa do Consumidor –CDC (BRASIL, 1990) compõem a interpretação do ordenamento jurídico nacional sobre a Internet e o comportamento dos provedores e usuários no mundo virtual. Para eventuais conflitos entre o Marco Civil da Internet e outros diplomas legais, deverão ser buscadas soluções, para estes conflitos, na jurisprudência dos tribunais superiores.

Alguns princípios encontrados no Marco Civil da Internet, Lei nº 12.965/2014, conforme o Art. 3º a seguir:

- garantia da liberdade de expressão, comunicação e manifestação do pensamento, nos termos da Constituição Federal;
- proteção da privacidade;
- proteção dos dados pessoais, na forma da lei;
- preservação e garantia da neutralidade da rede,
- preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- responsabilização dos agentes de acordo com suas atividades, nos termos da lei:
- preservação da natureza participativa da rede;
- liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei nº 12.965 (BRASIL, 2014).

Os princípios auxiliam na interpretação do conteúdo existente na lei e na associação ao caso concreto para suprimir eventuais conflitos.



O uso da internet, a luz do marco civil, objetiva o direito de acesso de todos à rede, o direito do acesso à informação, ao conhecimento e à participação na vida cultural e na condução de assuntos públicos, o direito da inovação e do fomento

à ampla difusão de novas tecnologias e modelos de uso e acesso e ao direito da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Para melhor entendimento, a Lei nº12.965/2014, no seu Art. 5º, define alguns aspectos relacionados a tecnologia, considerando:

- 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;
- terminal: o computador ou qualquer dispositivo que se conecte à internet;
- endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
- administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
- conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
- registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
- aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;
- registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. Lei nº 12.965 (BRASIL, 2014).

A interpretação do Marco Civil levará em conta não somente os fundamentos e princípios, mas também a natureza da internet, a forma de uso e os costumes, observando a importância que possui para o desenvolvimento humano, econômico, social e cultural.

Art. 70 O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

...]

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;

[...]

X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei nº 12.965 (BRASIL, 2014);

De acordo com o Art.7°, incisos VII e X fica vedada a utilização comercial dos dados pessoais dos internautas, salvo consentimento expresso, formalizando que a utilização de dados pessoais só poderá ocorrer por meio da manifestação da vontade, do consentimento livre, expresso e informado, que poderá ser revisado e revogado a qualquer tempo pelo próprio usuário, possuidor do direito de exclusão definitiva de todos dados pessoais que o provedor tiver cadastrado.



Este artigo esclarece, por exemplo, que propagandas de produtos ou serviços não poderão aparecer para o internauta, baseados no histórico de navegação, sem autorização prévia, ou seja, os registros de acesso a aplicações

incluídos no histórico de navegação não podem ser utilizados sem a mesma autorização expressa.

Os direitos e garantias dos usuários da internet estão previstos na lei e dispostos como forma essencial ao exercício da cidadania, baseados no uso e contrato de serviços, como você pode ver a seguir:

- não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
- manutenção da qualidade contratada da conexão à internet;
- informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão, aos registros de acesso a aplicações da Internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
- publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
- acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
- aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (BRASIL, 2014).

A privacidade e a proteção dos dados pessoais dos usuários estão assegurados conforme as garantias e direitos a seguir:

- inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
- inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
- inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
- 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;
- informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, não sejam vedadas

- pela legislação; e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
- consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
- exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei. (BRASIL, 2014).

A privacidade e a liberdade de expressão foram incluídas no dispositivo legal, condicionando o pleno exercício do direito de acesso à internet como garantia e direito do usuário. Deste modo, as cláusulas contratuais que violem esta garantia serão nulas, tais como as cláusulas que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet ou em contrato de adesão, que não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil, assim, os provedores deverão ter representantes no território nacional para anular conflitos.

O contrato de adesão é aquele em que uma das partes adere às cláusulas já estabelecidas pela outra parte sem discussão igualitária, não podem ser impressos com letras miúdas ou redação confusa e ambígua, e na dúvida, adota-se a interpretação mais favorável ao aderente. Um exemplo é o contrato de adesão disposto em sites de compra pela internet, estes contratos são "aceitos" pelo consumidor para efetivar a compra.

Até o momento, apresentamos os direitos à privacidade e a proteção dos dados e as garantias dos usuários na internet. Agora, entendamos um pouco mais a respeito de um tema extremamente importante: a Neutralidade da Rede.

A garantia da neutralidade significa que os provedores de acesso devem tratar todos os dados que circulam pela Internet da mesma forma, sem distinção de conteúdo, origem, destino, serviço, terminal ou aplicação. O provedor não poderá beneficiar o fluxo de tráfego de sites ou de serviços em detrimento de outro, desse modo, a lei garante a liberdade de expressão, a escolha do conteúdo pelo usuário conforme seu desejo, a livre concorrência na internet e o desenvolvimento da inovação.

A neutralidade da rede trata, de forma isonômica, quaisquer pacotes de dados, sem distinção de acessos ou envio. A regulamentação da lei sobre priorização de serviços de emergência e requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações será efetuada no futuro e compete ao Presidente da República e ao Comitê Gestor da Internet.

A proteção dos Registros, Dados Pessoais e Comunicações Privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas na conexão e no acesso à internet. O provedor é responsável pela guarda e somente disponibilizará os registros ou dados de usuários, associados ou terminais, mediante ordem judicial.

Sobre este aspecto, usuários e provedores, obrigatoriamente, devem respeitar a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, desde que pelo menos um dos terminais esteja localizado no Brasil.

A guarda de registros de conexão de internet cabe ao administrador do sistema autônomo respetivo dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, não poderá transferir a terceiros e somente disponibilizar o acesso a estes registros de conexão precedida por decisão judicial.



Neste momento, você teve contato com o marco civil da internet e seus conceitos principais. Assista ao vídeo "Aberto debate público sobre regulamentação do marco civil da

internet" (2015) e apresente, no fórum destinado a esta unidade "Fórum – Unidade 2", sua opinião sobre privacidade e registro de informações na

internet, conforme a temática do vídeo e os assuntos que devem ser regulamentados na lei do marco civil.

PROPRIEDADE INTELECTUAL

Agora você estudará um tema muito importante para o profissional da área de informática, a Propriedade Intelectual. Tal estudo surge devido a formalização do direito no intuito de proteção aos bens intelectuais provenientes do direito autoral, da propriedade industrial e direito sui generis. A proteção, ou direito positivo, desses direitos não se referem somente ao ramo do direito patrimonial, mas englobam os direitos inerentes à obra, criação, novidade e à originalidade, bem como, aos direitos morais do autor, esta definição é dada pela Organização Mundial de Propriedade Intelectual (Ompi).

A Ompi é vinculada a Organização das Nações Unidas (ONU) e um organismo internacional responsável pelo estudo da propriedade intelectual, com o intuito de proteger não somente os direitos econômicos envolvidos no direito autoral, mas também aqueles relacionados ao trabalho, à criação, inovação, originalidade e aos direitos morais do autor.

Encontramos em nossa Constituição Federal, Art. 5°, incisos XXVII e XXVII, as referências e indicações sobre a propriedade intelectual:

XXVII – aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar,

XXVIII – são assegurados, nos termos da lei:

- a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas;
- b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de que participarem aos criadores, aos intérpretes e às respectivas representações sindicais e associativas; [...]. (BRASIL, 1988).

Do mesmo modo, a Constituição Federal, em seu art. 5°, inciso XXIX, estabelece proteção à propriedade industrial, conforme vemos em

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

Você teve contato com o conceito de propriedade intelectual, verificando que organismos internacionais influenciaram a legislação interna, ou seja, o âmbito internacional, com as convenções e tratados sobre propriedade intelectual, os quais o Brasil tornou-se signatário, ratificado pelo congresso nacional, determinaram parâmetros e influenciaram na legislação interna, com a Lei de Direitos Autorais, Lei do Software, Lei da Propriedade Industrial.

A Lei de Direitos Autorais, nº 9609/98, trata sobre obras intelectuais protegidas, expressas por qualquer meio ou fixadas em qualquer suporte, tangíveis ou intangíveis, conhecidas ou inventadas futuramente.

O direito autoral é um aspecto do contexto legal que envolve uma obra e deve ser observado, como matéria relevante na criação e inovação.

No Brasil, o sistema de direitos autorais baseia-se na tradição jurídica latina, e esta tem sua origem no direito romano-francês. Em tais legislações, ao contrário dos sistemas anglo-saxônicos, considera-se a trabalhar como uma emanação da personalidade do autor, de modo a distinguir os direitos econômicos e os direitos morais, conforme Garcia (2013). Diferente da legislação latina, os sistemas de common law não consideram os direitos morais inseridos nas leis de direitos autorais, abordando principalmente os direitos patrimoniais, transformando o direito autoral como bens de consumo comercializáveis, caracterizando-os da mesma forma que bens físicos.

Nos sistemas jurídicos latinos, a proteção jurídica torna-se mais complexa, devido ao direito autoral envolvido que se configura como um direito da personalidade e direitos humanos, que somente o autor da obra poderá exercê-los. Neste contexto, existe uma fronteira política, jurídica e cultural entre diferentes países. Em uma tentativa de abordar esta questão de forma internacional, Convenção de Berna a surge como principal tratado internacional sobre direitos autorais e uma tentativa de harmonização legal para as diferentes concepções sobre o tema. Outra forma de harmonizar as diferentes legislações foi a Ompi.

Os direitos do autor são formados pelos direitos morais e patrimoniais Os direitos morais do autor são considerados direitos da personalidade, portanto, inalienáveis e intransferíveis. Assim, mesmo que haja cessão dos direitos patrimoniais sobre a obra, o direito moral do autor é indisponível e imprescritível.

A criação de uma obra emana da personalidade do autor, assim surgem seus direitos morais: os componentes que unem o autor a sua obra, produzindo efeitos por toda sua existência, mesmo após sua morte. Desta maneira, os direitos morais, que se referem aos bens jurídicos tutelados, são de ordem incorpórea, imaterial e intelectual, preservam a integridade da obra.

Este é um direito personalíssimo e visa proteger o criador da obra. Ele possui reflexos da personalidade do autor e é, assim, protegido pelas características intrínsecas dos direitos da personalidade (imprescritível, impenhorável, irrenunciável e inalienável). Também se relaciona com a elaboração, a divulgação e a titulação da obra. Contrário aos direitos patrimoniais, que consistem na exploração econômica das obras protegidas (PARANAGUÁ; BRANCO, 2009).



Assista ao vídeo "Direitos Autorais na Era Digital" (2013), um debate que exemplifica situações desta temática. Após assisti-lo, acesse o "Fórum – Unidade 2" e insira sua opinião sobre o caso do

YouTube comentado no debate.

Diferente do que você analisou sobre direito moral do autor, o direito patrimonial, também chamado de direito econômico da obra, é aquele que autoriza seu titular a explorar a obra economicamente (PARANAGUÁ; BRANCO, 2009).

Considera-se direito patrimonial todo bem apreciável economicamente, que esteja em comércio ou que possa ser alienado ou apropriado (PAESANI, 2012).

Os direitos patrimoniais do autor nascem no momento que ele divulga a obra, comunicando-se com o público. Eles são considerados bens móveis, cessíveis, transferíveis (por morte ou em vida) e temporários; reservam ao autor vantagens de ordem econômica, derivadas da exploração da obra. Estas vantagens impõem-se na autorização expressa ao legitimado, pelo autor, para qualquer uso econômico.

A criação de uma obra requer atenção em seu contexto autoral e, com base na discussão vista sobre direitos autorais, surgem novas formas de autoria, por exemplo, a adoção de licenças, que determinam no nascimento da obra, como ela será organizada no aspecto autoral.

LICENÇA

Uma licença é um contrato que exprime uma autorização para o uso, ou uso e fruição de direitos de propriedade intelectual, que pode ser onerosa ou gratuita, exclusiva ou limitada, tomando o caráter de uma locação, caso for onerosa, ou comodato, caso for gratuita. A retribuição financeira é designada por royalty, calculado em percentual sobre a obtenção de qualquer ganho econômico de propriedade intelectual (PIMENTEL, 2010).

A licença é a matéria que regulamenta como será a circulação dos direitos autorais; dessa forma, alguns direitos do autor podem ser transferidos a terceiros, sendo de continuidade e circulação previamente estabelecidas conforme o desejo e a autorização prévia do autor da obra original, que se dará por meio da

escolha de uma licença específica. Na Lei de Direitos Autorais (BRASIL, 1998), no Art. 49, encontra-se a indicação do direito de o autor transferir alguns direitos, mediante o licenciamento.

A cessão de direitos também existe na transferência da titularidade da obra intelectual, conforme o mesmo artigo, mas se diferencia da licença. Na cessão, a transferência da titularidade da obra intelectual, com exclusividade para o cessionário, assemelhando-se a uma compra e venda, se onerosa, ou a uma doação, se gratuita; já a licença é uma autorização dada pelo autor para que um terceiro se valha da obra, com exclusividade ou não, nos termos da autorização concedida, assemelhando-se a uma locação, se onerosa, ou a um comodato, se gratuita (PARANAGUÁ; BRANCO, 2009).

Neste momento, o estudo abordará o contexto de licenças abertas, que surgem como fundamento legal, expresso pelos próprios criadores, titulares do direito de autoral de uma obra. Essas produções possibilitam um movimento social em torno de uma obra, formalizando a proteção legal e autorizando previa e expressamente suas condições de uso. Caracterizadas como uma alternativa para que o direito autoral seja preservado de acordo com os critérios de uso e derivação que o autor da obra original escolheu, baseada na adoção da licença a qual a obra será regida.

Conforme Paesani (2012), como consequência do copylef, movimento destinado à democratização dos direitos, foram introduzidas as licenças CC (Creative Commons), licenças públicas gerais, específicas para cada obra autoral, destinadas a viabilizar a livre redistribuição de obras fonográficas, científicas e literárias de acordo com a vontade do seu titular.

Outra forma de contrato jurídico de aspecto aberto é o GNU-GPL (General Public License) e o GNU-LGPL (Lesser General Public License). GNU é uma sigla de língua inglesa que consiste em um sistema operacional de software livre, ou seja, respeita a liberdade dos usuários e que são livres para executar, copiar, distribuir, estudar, mudar e melhorar o software.

GNU é um sistema operacional Unix, ou seja, uma coleção de muitos programas: aplicações, bibliotecas, ferramentas de desenvolvimento e até mesmo jogos. O desenvolvimento do GNU, lançado em janeiro de 1984, é conhecido como Projeto GNU e o nome "GNU" remete a uma expressão em inglês "GNU's Not Unix" conforme disponibilizado no site oficial (www.gnu.org).

A Licença Pública Geral GNU, ou GNU General Public Licencse em inglês, é frequentemente chamada abreviadamente de GNU-GPL e objetiva a formação de redes de contratos, ou de contratos de licenciamento em rede. Conforme Segundo Paranaguá e Branco (2009), aquele que se vale da licença precisa necessariamente permitir o uso de seus eventuais aperfeiçoamentos e modificações.

A GNU-LGPL (GNU-Lesser General Public License em inglês) diferenciase da GNU-GPL no aspecto que permite também a associação com programas que não estejam sob as licenças GPL ou LGPL, incluindo softwares que não sejam "livres".

Através Por meio destes conceitos, licenças para software livres, surgiu o projeto colaborativo criado pelo professor Lawrence Lessig, da Universidade de Harvard, que tem por objetivo objetiva expandir a quantidade de obras criativas disponíveis ao público, permitindo criar outras obras sobre elas, compartilhando-as e disponibilizando as licenças jurídicas que permitem o acesso às obras pelo público em condições mais flexíveis (PARANAGUÁ e; BRANCO, 2009).

Neste contexto, tempos como exemplo o licenciamento em Creative Commons, que implica uma renúncia dos direitos morais, o que seria ilegal nos sistemas jurídicos de tradição latina, como ocorre no Brasil. Os termos de licença referentes a tais direitos são interpretados como uma autorização para a reutilização, adaptação e redefinição das obras, desde que o trabalho derivado mantenha a mesma licença.

A diferença básica entre "renúncia" e "autorização" reside na possibilidade de os autores retirarem as licenças concedidas. Isso acontece porque, nos termos da licença escolhidos, incluem aspectos relacionados aos direitos morais e os sistemas jurídicos que se vinculam, tais direitos são inalienáveis.

A revogação da licença não será retroativa, para que não sejam afetadas as obras ou cópias de trabalho que começaram a circular, existentes na forma derivativa ou derivativas. Caso uma equipe de autores, no exercício de seus direitos morais, oponha-se a existência de uma obra derivada por entender que aquela prejudica sua honra ou reputação, esta deve remover todas as referências à obra original e aos autores que se sentiram lesados.

Todas as licenças Creative Commons contêm uma cláusula de "separabilidade", que permite, em caso de incompatibilidade de alguns de seus termos com as leis de qualquer país, eliminar qualquer disposição considerada inaplicável nas demais disposições aplicadas.

A licença Creative Commons permite que o autor tenha alguns direitos reservados, autorizando toda a sociedade a usar a sua obra segundo os termos das licenças públicas adotadas.

A seguir, apresenta-se as principais licenças Creative Commons (2016):

Atribuição CC BY: Esta licença permite que outros possam distribuir, remixa, aperfeiçoar e construir sobre o seu trabalho, até mesmo comercialmente, desde que seja dado crédito pela criação original. Este é o mais flexível de licenças oferecidas. Recomendado para o máximo de divulgação e utilização dos materiais licenciados.

Atribuição-Compartilhamento pela mesma licença CC BY-SA: Esta licença permite que outros remixem, adaptem, e criem obras até com fins comerciais, desde que seja dado crédito você e licenciem as

novas criações sob os mesmos parâmetros. Esta licença é geralmente comparada a licenças de software de código 'copyleft' livres e abertas. Todos os trabalhos futuros levarão a mesma licença, permitindo inclusive o uso comercial.

Atribuição-Não a obras derivadas CC BY-ND: Esta licença permite a redistribuição, comercial e não-comercial, desde que a obra se mantenha inalterada.

Atribuição-Uso Não Comercial CC BY-NC: Esta licença permite que terceiros remixem, adaptem e criem obras não-comercial, e dessa maneira, tem-se o acesso à obra mas não podem comercializá-la e as obras derivadas devem conter os mesmos termos da licença.

Atribuição-Uso Não Comercial-Compartilhamento pela mesma licença CC BY-NC-SA: Esta licença permite que outros remixem, adaptem, e criem obras não-comercial, desde que seja dado crédito você e licenciem as novas criações sob os mesmos parâmetros.

Atribuição-Uso Não comercial: Não a obras derivadas CC BY-NC-ND: Esta licença é a mais restritiva das seis licenças principais, permitindo que apenas os outros a fazer download das obras e compartilhá-las com outras pessoas, desde que creditá-la e sem alterá-las de qualquer forma ou usá-las comercialmente.

LEI DO SOFTWARE

Lei do Software, nº 9.609/98, em seu Art. 1º, define o que é um Software; para a legislação, no entanto, Software será chamado de Programa de Computador.

O Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos

periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. Uma situação importante para sua vida profissional e seus objetivos futuros como profissional da área de informática é conhecer o Art. 4º da Lei do Software que trata sobre a criação de um programa de computador quando este for desenvolvido e elaborado durante a vigência de contrato ou vínculo empregatício:

Art. 4º. Salvo estipulação em contrário, pertencerão exclusivamente ao empregador, contratante de serviços ou órgão público, os direitos relativos ao programa de computador, desenvolvido e elaborado durante a vigência de contrato ou de vínculo estatutário, expressamente destinado à pesquisa e desenvolvimento, ou em que a atividade do empregado, contratado de serviço ou servidor seja prevista, ou ainda, que decorra da própria natureza dos encargos concernentes a esses vínculos.

§ 1º Ressalvado ajuste em contrário, a compensação do trabalho ou serviço prestado limitar-se-á à remuneração ou ao salário convencionado.

§ 2º Pertencerão, com exclusividade, ao empregado, contratado de serviço ou servidor os direitos concernentes a programa de computador gerado sem relação com o contrato de trabalho, prestação de serviços ou vínculo estatutário, e sem a utilização de recursos, informações tecnológicas, segredos industriais e de negócios, materiais, instalações ou equipamentos do empregador, da empresa ou entidade com a qual o empregador mantenha contrato de prestação de serviços ou assemelhados, do contratante de serviços ou órgão público.(BRASIL, 1998).

O Software poderá ser registrado no Instituto Nacional da Propriedade Industrial (INPI) e possui uma lei específica o que caracteriza a necessidade de mais atenção e análise sobre seus aspectos particulares, pois no que tange a questão autoral, a legislação específica para o Software é a Lei do Software, mas a Lei de Direitos Autorais poderá ser aplicada conforme o Art. 7º, parágrafo 1º, e o registro do programa de computador será no INPI.

Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como:

[...]

§ 1º Os programas de computador são objeto de legislação específica, observadas as disposições desta Lei que lhes sejam aplicáveis.

Mas o software pode ser considerado um produto ou um serviço?

Para responder a esta questão, a análise sobre a criação dependerá da comercialização e do software. Poderá ser classificado como produto, cujo titular de direito receberá royalties, ou poderá ser classificado como serviço, incidindo tributos como o Imposto Sobre Serviços (ISS).



O Software, como produto ou mercadoria, poderá ser classificado como "software de prateleira", disponibilizado em um comércio, loja, supermercado etc., incidindo o Imposto sobre Circulação de Mercadorias e Serviços (ICMS) ou os tributos do Imposto sobre Produtos Industrializados (IPI) Imposto sobre Importação (II). Observar a forma de criação, comercialização, atualização e manutenção do Software irá caracterizá-lo como produto/mercadoria ou serviço.

Você acabou de estudar os conceitos relacionados com a Lei do Software e como sugestão para leitura complementar, leia o artigo "A propriedade intelectual na lei do software" (ORTIZ, 2012).



APROFUNDANDO CONCEITOS

Você poderá aprofundar os conceitos estudados com as sugestões a seguir, visitando alguns sites ou artigos que tratam desde o conceito de direito, até as convenções internacionais as quais o Brasil é signatário, como também o site do



Instituto Nacional de Propriedade Industrial (INPI), órgão estatal responsável pelo registro do programa de computador e de outras propriedades intelectuais.

Os vídeos apresentam a continuação do documentário sobre a história da internet.

"O conceito de direito" (MARTINS, 2011).

"Os valores de Miguel Reale" (MARTINS, 2008).

Marco Civil da Internet (BRASIL, 2014).

"Convenção de Berna" (UNESCO, 1886).

INPI (BRASIL – Ministério, 2016).

"Documentário – A Verdadeira História da Internet – 01 – A Guerra Dos Navegadores – Discovery Channel" (2013).

"Documentário – A Verdadeira História da Internet – 02 – A Pesquisa – Discovery Channel" (2013).

"Direitos Autorais na Era Digital" (2013).

"Direitos Autorais no Youtube" (2016).



SÍNTESE

Sintetizando essa unidade, você conheceu os aspectos importantes a respeito do Marco Civil da Internet, que assegura, entre outros aspectos, o direito de acesso à Internet, à informação, estabelece regras de responsabilidade civil para provedores e usuários, impõe medidas para preservar a liberdade de expressão e a privacidade, e, também, estabelece princípios e diretrizes para garantir o funcionamento da internet de forma isonômica, de igual tratamento para todos os usuários.

O marco civil estabeleceu normas para a conduta dos prestadores de serviço de internet e usuários, incentivando a adesão a padrões tecnológicos abertos, sem maiores restrições sobre a propriedade intelectual.

A respeito deste assunto, você encontrou informações importantes sobre direito do autor, direitos morais e patrimoniais, lei do software e seu instituto de registro.

A autora Paesani (2012, p. xx12) relata que os direitos sobre a Propriedade Intelectual:

são direitos exclusivos, ou seja, direitos de excluir terceiros, que não o titular, da fruição econômica do bem, a intervenção do Estado se faz necessária para coibir a cópia, restringir a concorrência desleal e proteger as inovações e as novas obras intelectuais. A propriedade intelectual nasce da lei, não é um direito natural e espelha o patrimônio cultural de um povo.

Para auxiliar e complementar esta síntese, faça um resumo do manual do usuário, com no máximo duas páginas, para o pedido do registro do programa de computador conforme determinações localizadas no site do INPI.



REFERÊNCIAS

- ABERTO DEBATE PÚBLICO SOBRE REGULAMENTAÇÃO DO MARCO CIVIL DA INTERNET. Direção e Produção: TVNBR. Brasília, DF: NBR Entrevista, 16 fev. 2015. Disponível em: http://moodle.mackenzie.br/link/1as. Acesso em: 28 jul. 2016.
- ▶ BRASIL. Constituição (1988). Constituição da República Federativa do Brasil, de 5 de outubro de 1988. Disponível em: http://moodle.mackenzie.br/link/1av. Acesso em: 4 abr. 2016.
- ▶ BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, DF, 19 set. 1990. Seção 1, p. 1. Disponível em: http://moodle.mackenzie.br/link/1at>. Acesso em: 28 jul. 2016.
- ▶ BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Diário Oficial da União, DF, 15 maio 1996. Seção 1, p. 8353. Disponível em: http://moodle.mackenzie.br/link/1au. Acesso em: 4 abr. 2016.
- ▶ BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da União, DF, 20 fev. 1998. Seção 1, p. 1. Disponível em: http://moodle.mackenzie.br/link/law>. Acesso em: 4 abr. 2016.
- ▶ BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, DF, 20 fev. 1998. Seção 1, p. 3. Disponível em: http://moodle.mackenzie.br/link/lay. Acesso em: 29 jul. 2016.

- ▶ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Seção 1, p. 1. Disponível em: http://moodle.mackenzie.br/link/1b2>. Acesso em: 4 abr. 2016.
- ▶ BRASIL. MINISTÉRIO da Indústria, Comércio Exterior e Serviços. Instituto Nacional da Propriedade Industrial. Disponível em: http://moodle.mackenzie.br/link/1b3>. Acesso em: 29 abr. 2016.
- CREATIVE Commons, 2016. Disponível em: http://moodle.mackenzie.br/link/1b4. Acesso em: 4 abr. 2016.
- DIREITOS AUTORAIS NA ERA DIGITAL. Direção: Guilherme Bacalhao. Produção: Danielle Araujo. Brasília: TV Câmara, 2 jan. 2013. Disponível em: http://moodle.mackenzie.br/link/1b5>. Acesso em: 25 maio 2016.
- DIREITOS AUTORAIS NO YOUTUBE. Produção e Direção: Youtube, 2016. Disponível em: http://moodle.mackenzie.br/link/1b6. Acesso em 16 maio 2016.
- DOCUMENTÁRIO A VERDADEIRA HISTÓRIA DA INTERNET 01 A GUERRA DOS NAVEGADORES DISCOVERY CHANNEL. Produção e Direção: Julian Jones. Londres: Oxford Scientific Films, 5 nov. 2013. Disponível em: http://moodle.mackenzie.br/link/1b7>. Acesso em: 9 maio 2016.
- DOCUMENTÁRIO A VERDADEIRA HISTORIA DA INTERNET 02 A PESQUISA DISCOVERY CHANNEL. Produção e Direção: Julian Jones. Londres: Oxford Scientific Films, 5 nov. 2013. Disponível em: http://moodle.mackenzie.br/link/1b8>. Acesso em: 9 maio 2016.

- SOU, 2016. Disponível em: http://moodle.mackenzie.br/link/1ba. Acesso em: 4 abr. 2016.
- NPI. Manual do Usuário Programa de Computador. Disponível em: http://moodle.mackenzie.br/link/1bb>. Acesso em: 29 jul. 2016.
- ORTIZ, L. R. A. A propriedade intelectual na lei do software. Revista Eletrônica da Faculdade de Direito de Franca, Franca, v. 6, n. 1, p. 304-309, dez. 2012. Disponível em: http://moodle.mackenzie.br/link/1bc. Acesso em: 18 maio 2016.
- MARTINS, D. C. O conceito de direito. Portal de e-governo, inclusão digital e sociedade do conhecimento, 7 dez. 2011. Disponível em: http://moodle.mackenzie.br/link/1bd>. Acesso em: 30 abr. 2016.
- MARTINS, A. M. S. Os valores de Miguel Reale. a. 45, Brasília, n.180, p. 263-277, out./dez. 2008. Disponível em:http://moodle.mackenzie.br/link/1be. Acesso em: 30 abr. 2016.
- PAESANI, L. M. Manual de Propriedade Intelectual: direito do autor, direito da propriedade industrial, direitos intelectuais sui generis. 1. ed. São Paulo: Atlas, 2012. 1 v.
- PARANAGUÁ, P.; BRANCO, S. Direitos Autorais. Rio de Janeiro: FGV, 2009.

- PIMENTEL, L. O. Manual básico de acordos e parceria de PD&I: aspectos jurídicos. Fórum Nacional de Gestores de Inovação e Transferência de Tecnologia. Porto Alegre: EDIPUCRS, 2010.
- RAO, V. O direito e a vida dos direitos. São Paulo: Revista dos Tribunais, 1991.
- REALE, M. Filosofia do Direito. 19. ed. São Paulo: Saraiva, 2003.
- UNSECO. Convenção de Berna. Convenção para a proteção das obras literárias e artísticas, de 09 de setembro de 1886. Disponível em: http://moodle.mackenzie.br/link/1bg>. Acesso em: 29 abr. 2016.

UNIDADE 3

FORENSE COMPUTACIONAL

Nesta unidade, abordaremos a Forense Computacional, os Crimes Eletrônicos, a Perícia e os Atos Ilícitos. Você identificará os aspectos relevantes do direito e da profissão na área de perícia em sistemas computacionais e as particularidades das normas relacionadas aos atos ilícitos cometidos com o uso da Tecnologia da Informação.

Por meio dos recursos computacionais e da internet, os relacionamentos entre usuários tornam-se virtuais. Isso fez com que surgissem atos considerados tipificados no código penal, sendo tais atos ilícitos enquadrados como crimes por meios eletrônicos. Para identificação e comprovação desses atos, faz-se necessária, em muitos casos, a perícia computacional. Ela identificará o conjunto probatório para comprovação dos atos ilícitos.

Você é responsável pelos seus atos cometidos no meio tecnológico e por isso precisa tomar cuidado para não ser vítima de fraudes ou crimes cometidos por atos ilícitos de terceiros.

Esse tema é atual e recorrente na área de informática, pois, com o aumento do uso da tecnologia, há o aumento do número de crimes no ambiente digital.



EXPLORANDO OS CONCEITOS



Nesta unidade temática, poderão surgir dúvidas sobre alguns dos conceitos. Deste modo, você poderá descrever sua dúvida ou apresentar uma discussão no fórum específico da unidade: "Fórum – Unidade 3". Para auxiliá-lo no estudo da unidade, leia

as matérias "Quais os crimes virtuais mais comuns?" (POZZEBON, 2015) e "Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação" (CARNEIRO, 2012) e responda: quais os crimes eletrônicos mais comuns? Pesquise sobre essa questão e vamos discutir no fórum.

FORENSE COMPUTACIONAL

Forense computacional ou computação forense é a reunião de informações (um conjunto probatório, com cenas, dados ou evidências) de um crime no ambiente computacional, ou cometido com o uso da tecnologia. É a aplicação de técnicas de investigação e de análise para reunir, preservar, recuperar, analisar e apresentar, a partir de sistemas computacionais, dados, materiais e evidências que componham um conjunto probatório para apresentação em juízo.

O objetivo da computação forense é realizar uma investigação apurada, estruturada, reunindo e analisando evidências registradas ou documentadas para descobrir exatamente o que aconteceu em um sistema computacional e determinar o autor responsável pelo aspecto analisado.



A computação forense é determinada por um perito, um investigador especialista, que normalmente segue um conjunto padrão procedimental, como identificar o sistema ou equipamento, isolá-lo, a fim de garantir a integridade da Wanálise e evitar acidentalmente alguma contaminação das

provas. Estas perícias devem ser efetuadas com backups rotineiros para assegurar e manter as condições iniciais analisadas. Os peritos examinam os equipamentos ou sistemas computacionais, procurando evidências e provas, que auxiliarão processos judiciais ou laudos técnicos particulares.

O objetivo principal da computação forense é, conforme Bustamante (2006), extrair e analisar dados dos diferentes dispositivos, para que essas informações passem a ser caracterizadas como evidências e, posteriormente, como provas legais do fato. Consiste, portanto, no uso de métodos científicos na preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital, produzindo informações diretas como meio de prova legal (PINHEIRO, 2007). Uma evidência digital é a informação.

PERÍCIA FORENSE COMPUTACIONAL

A perícia computacional forense surge da necessidade da análise de um perito na área da computação. Ele empregará a computação forense em casos concretos, descrevendo os aspectos técnicos, investigando, analisando e determinando um laudo técnico, parecer de um especialista em processos judiciais, ou pericial, parecer técnico solicitado pelo judiciário. Este, normalmente, é realizado por um perito de confiança do juiz, atuante em processos judiciais, auxiliando na descrição dos fatos, chamado de perito.

Este profissional da computação forense poderá atuar em investigações privadas ou empresariais, não necessariamente em processos judiciais, sendo, neste caso, chamado de perito da computação. Mesmo que a perícia não seja feita para um processo judicial, sendo o profissional contratado como perito da computação para uma investigação em ambiente privado, o parecer ou o laudo pericial deverá obedecer a formalidade descritiva empregada em processos judiciais, pois essa perícia poderá, futuramente, servir como conjunto probatório em uma demanda judicial.

A Forense Computacional é a ciência que adquire, preserva, recupera e apresenta dados processados e armazenados eletronicamente por meio do computador (THOMAS; FORCHT, 2004). Freitas apud Queiroz, Vargas (2010) complementa esta definição relatando que a forense computacional é o ramo da criminalística que compreende a aquisição, a prevenção, a restauração e a análise de evidências computacionais, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.

ASPECTOS DA PERÍCIA FORENSE COMPUTACIONAL

A perícia forense computacional investigará e analisará informações, extraindo e restaurando evidências, formalizando todos os procedimentos que deverão ser descritos e apresentados em um documento assinado pelo perito.

A perícia buscará por evidências, identificando-as, preservando-as e analisando-as e, ao final, por meio da documentação formal e descritiva, exporá seu laudo técnico.

Para identificar, analisar e recuperar essas evidências, existem formas de padronização internacionais recomendadas pelo Scientific Working Group on Digital Evidence (SWGDE) e pela International Organization on Digital Evidence (IODE), em "Digital evidence: standards and principles" (2000)... Entre as sugestões da SWGDE e IODE, temos a coerência com todos os sistemas jurídicos, o uso de uma língua comum, a capacidade de incutir confiança na integridade das provas, entre outras. Alguns exemplos são:

- Após a coleta de evidências digitais, as medidas tomadas não devem alterar essas provas.
- Caso uma pessoa necessite acessar evidências digitais originais, o trabalho deve ser feito por um profissional forense competente.
- Toda atividade relacionada com a coleta, o acesso, o armazenamento ou a transferência de evidências digitais deve ser devidamente documentada, preservada e disponível para avaliação.
- As medidas ou ações tomadas a respeito de uma prova digital serão do responsável pela sua posse.
- Qualquer empresa que é responsável por guardar, acessar, armazenar ou transferir prova digital será responsável pela conformidade com esses princípios.

Tais princípios são norteadores para delimitar e padronizar ações e perícias forenses efetuadas com evidências ou provas digitais. Para organizar ações tomadas em uma investigação forense é preciso que as evidências ou provas não sejam alteradas. O acesso às evidências ou às provas digitais deverá ser controlado e identificado. Outras orientações seriam efetuar cópias de segurança, realizar um backup das evidências ou provas originais, sempre que possível, estabelecendo uma margem de segurança para preservação das provas. Assim, toda investigação deverá ser conduzida por meio de cópias, idênticas às evidências,

e provas originais.

Conforme Melo (2009), o processo de análise forense, sob a ótica da organização de etapas da perícia forense computacional, poderá ser dividido em quatro etapas: aquisição, identificação, avaliação e apresentação.

Para ele, a aquisição trata da fase inicial da perícia forense, na qual o perito coletará dados e artefatos relacionados ao incidente de segurança. Na etapa da identificação, o perito classificará os dados levantados durante a etapa de aquisição, identificando vestígios, evidências e provas. Na etapa de avaliação, a perícia analisará pontualmente cada dado, sendo este um vestígio, evidência ou prova, que, inclusive, poderá desqualificar sua primeira classificação. Na quarta e última etapa, chamada de apresentação, a elaboração do laudo pericial ou parecer técnico terá que conter o maior grau de riqueza de informações possível, sendo redigido com rigor de detalhes e explicações; o perito seguirá sua linha de argumentação apoiado pelos vestígios, evidências ou provas do sistema computacional periciado.

ATOS ILÍCITOS E CRIMES ELETRÔNICOS

O avanço constante dos sistemas computacionais traz novos desafios para a sociedade. Entre eles, encontramos o ato ilícito e o crime por meios eletrônicos. O ato ilícito seria a ação, a omissão ou o abuso de poder praticado por um indivíduo que prejudicará terceiros; já o crime eletrônico, também chamado de crime informático, seria a conduta ilegal, a prática "[...] relacionada às informações arquivadas ou em rede por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar". (CORRÊA, 2000).

Crime é uma ação típica, antijurídica e culpável, determinada e identificada por lei. Com relação aos crimes cometidos por meios informáticos, temos uma vasta nomenclatura, determinada por termos sinônimos: cibercrimes, crimes virtuais, crimes de internet, crimes eletrônicos, crimes digitais, crimes informáticos, crimes de informática, crimes de computador e crimes telemáticos.



Leia sobre tipos de crimes eletrônicos em "O que são crimes virtuais?" (CASSANTI, 2015) e assista aos dez primeiros minutos do vídeo "Os Profissionais 22—Cibercrimes, QualidadedeVida e Erros de Português"

(2015), ele relata algumas profissões relacionadas ao tema de estudo, como do perito forense computacional.

O ambiente computacional possibilita a prática de crimes cada vez mais sofisticados, bem como daqueles tipificados como tradicionais, por exemplo, o furto. Estes crimes podem ser cometidos por meio de um computador ou de um sistema computacional, caracterizando-o como uma ferramenta para o crime); no entanto, um ataque criminoso pode ser contra a parte física (hardware) ou lógica (software) da máquina, caracterizando esta como objeto do crime.

Vejamos agora alguns crimes que podem ser cometidos eletronicamente e tipificados pelo código penal brasileiro.

- Crimes contra a pessoa: são crimes que visam a vida e a integridade física, como o homicídio.
- Crimes contra a honra: injúria, calúnia e difamação, indução, estímulo ou auxílio ao suicídio.
- Crimes contra o patrimônio: furto e estelionato.
- Crimes contra a propriedade imaterial: violação de direito autoral, violação do programa de computador, concorrência desleal.
- Crimes contra os costumes: pedofilia, favorecimento à prostituição, rufianismo ou lenocínio.
- Crimes contra a incolumidade pública: tráfico de drogas e de armas com ou sem associação para o tráficocontrabando.
- Crimes contra a paz pública: incitação ao crime, formação de quadrilha ou bando.
- Outros crimes: crime eleitoral.

Leia a seguir alguns exemplos de crimes virtuais na matéria "Crimes virtuais" (SALVADORI, 2013) e perceba como esta modalidade de ilícitos se aperfeiçoou com o avanço e desenvolvimento tecnológico.

Conforme essas tipificações dos crimes no direito penal, também há a classificação dos crimes de informática:

- quanto à sua origem— determinados como interno (o local do crime) ou externos (fora do local do ilícito) que podem ser distintos;
- quanto à vítima um indivíduo ou um grupo (coletividade);
- quanto ao objeto hardware ou software ou ambos;
- quanto ao ambiente ou meio impróprio ou comum (cometido no mundo físico ou no ciberespaço), próprio ou específico (somente no ciberespaço);
- tipos penais previstos no dispositivo legal:
- a) Código penal calúnia (Art. 138), difamação (Art. 139), injúria (Art. 140), ameaça (Art. 147), divulgação de segredo (Art. 153), violação de segredo profissional (Art. 154), furto (Art. 155), dano (Art. 163), estelionato (Art. 171), violação de direito autoral (Art. 184), falsa identidade (Arts. 307 e 308), inserção de dados falsos em sistema de informações (Art. 313-A), modificação ou alteração não autorizada de sistema de informações (Art. 313-B).
 - b) Lei nº 11.829/08 sobre a pedofilia (BRASIL, 2008).
- c) Lei nº 12.737/12 –Lei sobre delitos informáticos (Lei Carolina Dieckmann), incluindo os artigos 154-A e 154-B no Código Penal (BRASIL, 2012).
- d) Lei nº 9.609/98 (BRASIL, 1998). Lei do Software sobre violar o direito de autor de programa de computador (Art. 12) (BRASIL, 1998).
- e) Lei nº 12.735/12 alteração do Código Penal, tipificando condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências (BRASIL, 2012a).

Entre os tipos penais observados anteriormente, enfatizaremos alguns dispositivos legais, citando-os na íntegra, pela sua relevância na área de informática:

Lei nº 9.609/98 – Lei do Software sobre violar o direito de autor de programa de computador.

Lei nº 12.737/12 – Lei sobre delitos informáticos (Lei Carolina Dieckmann), incluindo os Arts. 154-A e 154-B no Código Penal.

Entre os crimes descritos acima, a invasão de dispositivos informáticos ganhou notoriedade atualmente devido ao aumento deste tipo de ilícito. Criminosos invadem sistemas computacionais privados a fim de obter, adulterar ou destruir dados ou informações sem autorização, colocando em risco a imagem ou reputação, comprometendo a privacidade do proprietário do sistema computacional. A lei nº 12.737/12 surgiu com o intuito de coibir esse tipo de ato ilícito, evitando que dados privados sejam repassados a terceiros sem autorização, penalizando criminosos que os praticarem.



Com base nos conteúdos abordados, leia os artigos "Sobre o relatório final da CPI do Cibercrime" (MILAGRE, 2016) e "'Manda Nudes': Histórias de quem expôs a intimidade" (SCARPELINI, 2016) e assista ao vídeo "TÍTULO: Tela Mackenzie 47 – Segurança Digital"

(2015). Pesquise sobre crimes eletrônicos e atos ilícitos, participe do "Fórum – Unidade3 – Exemplo" apresentando um exemplo de crime eletrônico e comente o exemplo de pelo menos um colega.



APROFUNDANDO CONCEITOS

A seguir, você encontrará uma lista de recursos extras que complementarão o conteúdo da unidade. Essas indicações são artigos, sites e vídeos, alguns já indicados no decorrer da Unidade que auxiliarão no estudo e no aprofundamento de alguns conceitos abordados.

"Introdução à computação forense" (BUSTAMANTE, 2006).

"Forense computacional: aspectos legais e padronização" (GUIMARÃES, 2006).

"GTS 25: Novos desafios das perícias em sistemas computacionais" (2015), palestra proferida por Ricardo Kleber, em Uberlândia.

"Documentário – A verdadeira história da internet – 03 – A bolha – Discovery Channel" (2013)

"Documentário – A verdadeira história da internet – 04 – O poder das pessoas – Discovery Channel" (2013)

Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE). Digital Evidence: Standards and Principles.

Cibercrimes. Vídeo do Programa Os profissionais: (00:00 – 10:30).

CASSANTI, Moisés de Oliveira. O que são crimes virtuais? Site Crimes pela Internet.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Portal Âmbito Jurídico.



SÍNTESE

A tecnologia da informação modificou diversas áreas de atividades empresariais, pessoais e de relacionamento humano. Ambientes tecnológicos permitiram o surgimento de situações propícias à prática de crimes, potencializando a ocorrência de delitos. A computação forense surgiu como um desafio para os profissionais da área da computação e do direito, sendo que esta última necessita do profissional especializado em computação para apresentar informações provenientes do campo tecnológico. É importante notar que as devidas informações tecnológicas não terão utilidade sem o aspecto legal que deverá ser observado e aplicado. Segundo Patrícia Pinheiro (2007), a computação forense (computer forensics) compreende a aquisição, preservação, restauração e análise de evidências computacionais, quer sejam componentes físicos quer sejam dados processados eletronicamente e armazenados em mídias computacionais.

A perícia forense computacional utiliza técnicas para determinar com exatidão qual foi a ação digital criminosa, demonstrando evidências ou provas digitais indicando o ato ilícito, podendo, até mesmo, indicar a pessoa que o cometeu. Para isso, a investigação e o conjunto probatório serão profundas.

Os atos ilícitos em meios informáticos têm tornado a adequação das leis cada vez mais atualizada. Novas leis surgem tipificando crimes que utilizam sistemas computacionais, atualizando a legislação e criminalizando as ações indevidas, como a invasão de dispositivos informáticos por terceiros

Por meio dos conceitos abordados, elabore um mapa mental desta unidade, classificando os crimes e seus referenciais legais, enfatizando os dispositivos legais, ou seja, indicando o artigo e lei respectiva. Apresente este mapa mental na tarefa "Mapa Mental – Unidade 3".

Dica: para construção do mapa mental, você poderá utilizar as ferramentas on-line Mind Meister ou Coggle.



- ▶ BRASIL. Lei nº 11.829, de 25 de novembro de 2008. Altera a Lei nº 8.069, de 13 de julho de 1990 Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Diário Oficial da União, DF, 26 nov. 2008. Seção 1, p. 1. Disponível em: http://moodle.mackenzie.br/link/1bi. Acesso em:23 maio 2016.
- ▶ BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 Código Penal; e dá outras providências. Diário Oficial da União, DF, 3 dez. 2012. Seção 1, p. 1. Disponível em: http://moodle.mackenzie.br/link/1bj>. Acesso em: 23 maio 2016.
- BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da União, DF, 20 fev. 1998. Seção 1, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9609. htm>. Acesso em: 23 maio 2016.
- BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Diário Oficial da União, DF, 3 dez. 2012a. Seção 1, p. 1. Disponível em: http://moodle.mackenzie.br/link/1bk. Acesso em:23 maio 2016.

- CARNEIRO, A. G. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, n. 99, abr. 2012. Disponível em: http://moodle.mackenzie.br/link/1bl. Acesso em: 16 maio 2016.
- CASSANTI, M. O. O que são crimes virtuais? Crimes pela Internet, 13 mar. 2015. Disponível em: http://www.crimespelainternet.com.br/o-que-sao-crimes-virtuais/». Acesso em: 20 maio 2016.
- ORRÊA, G. T. Aspectos jurídicos da internet. São Paulo: Saraiva, 2000.
- DIGITAL evidence: standards and principles. Forensic Science Communications, [S.l.], v. 2, n. 2, abr. 2000. Disponível em: http://moodle.mackenzie.br/link/1bm. Acesso em: 29 abr. 2016.
- DOCUMENTÁRIO A VERDADEIRA HISTÓRIA DA INTERNET 03 A BOLHA DISCOVERY CHANNEL. Direção e produção: Julian Jones. Londres: Oxford Scientific Films, 25 nov. 2013. Disponível em: http://moodle.mackenzie.br/link/1bn>. Acesso em: 9 maio 2016.
- DOCUMENTÁRIO A VERDADEIRA HISTÓRIA DA INTERNET 04 O PODER DAS PESSOAS DISCOVERY CHANNEL. Direção e produção: Julian Jones. Londres: Oxford Scientific Films, 25 nov. 2013. Disponível em: ⟨http://moodle.mackenzie.br/link/1bo⟩. Acesso em 9 maio 2016.
- FARMER, D.; VENEMA, W. Perícia forense computacional: teoria e prática aplicada. São Paulo: Pearson Prentice Hall, 2007.

- QUIMARÃES, C. C. et al. Forense computacional: aspectos legais e padronização. iMasters, São Paulo, 21 jul. 2006. Disponível em: ⟨http://moodle.mackenzie.br/link/1bq⟩. Acesso em: 5 ago. 2016.
- MELO, S. Computação forense com software livre. Rio de Janeiro: Alta Books, 2009.
- MILAGRE, J. A. Sobre o relatório final da CPI do Cibercrime. JCNet, São Paulo, 18 maio 2016. Disponível em: http://moodle.mackenzie.br/link/1br. Acesso em: 20 maio 2016.
- MODEL SOP for Computer Forensics. Scientific Working Group on Digital Evidence, v. 3, 13 set. 2013. Disponível em: http://moodle.mackenzie.br/link/1bs. Acesso em: 8 ago. 2016.
- OS PROFISSIONAIS 22 CIBERCRIMES, QUALIDADE DE VIDA E ERROS DE PORTUGUÊS. Direção e Produção: TV Mackenzie. São Paulo: Universidade Presbiteriana Mackenzie, 2 abr. 2015. Disponível em: http://moodle.mackenzie.br/link/1bv.
- PINHEIRO, P. P. Direito digital. São Paulo: Saraiva, 2009.
- POZZEBON, R. Quais os crimes virtuais mais comuns? Oficina da Net, 30 abr. 2015. Disponível em: http://moodle.mackenzie.br/link/1bw. Acesso em: 16 maio 2016.
- QUEIROZ, C.; VARGAS, R. Investigação e Perícia Forense Computacional: certificações, Leis processuais e estudos de caso. Rio de Janeiro: Brasport, 2010.

- SALVADORI, F. Crimes virtuais. Galileu, São Paulo, 2013. Disponível em: http://moodle.mackenzie.br/link/1cj. Acesso em: 20 maio 2016.
- SCARPELINI, L. "Manda Nudes": Histórias de quem expôs a intimidade. Revide, Ribeirão Preto, 13 maio 2016. Disponível em: http://moodle.mackenzie.br/link/1ck>. Acesso em: 20 maio 2016.
- TÍTULO: TELA MACKENZIE 47 SEGURANÇA DIGITAL. Direção e Produção: TV Mackenzie. São Paulo: Universidade Presbiteriana Mackenzie, 4 dez. 2015. Disponível em: http://moodle.mackenzie.br/link/1cl. Acesso em: 20 maio 2016.
- THOMAS, D.S; FORCHT, K.A. Legal Methods of Using Computer Forensics Techniques for Computer Crime Analysis and Investigation. In: Issues in Information System. Vol. 5,n.2, 2004, p. 692-698. Disponível em: http://moodle.mackenzie.br/link/1cm. Acesso em: 20 maio 2016.

UNIDADE 4

ASPECTOS DO DIREITO RELACIONADOS COM O PROFISSIONAL DE INFORMÁTICA

Nesta unidade, você terá contato com aspectos do direito relacionados com o profissional de informática, como as relações de trabalho que se encontram na especialidade do direito chamada trabalhista. Estudará, também, conceitos relacionados ao comércio eletrônico.

Na área do direito privado, o direito do trabalho é a especialidade relacionada com os princípios, as normas e as instituições jurídicas que tratam das relações de trabalho.

Casa. Thinksead



O comércio eletrônico, ou o e-commerce, relaciona-se com o profissional da área de informática esperando sua atuação sobre a segurança do comércio eletrônico, sobre a prevenção de fraudes, golpes e; situações ilícitos que esta área comercial deve observar quando ocorrerem situações de compra e venda de produtos, de logística, de prestação de serviços e de atendimento

ao cliente. Além da segurança, o profissional de informática poderá atuar no desenvolvimento de plataformas digitais para o comércio e para a prestação de serviços no auxílio das transações comerciais eletrônicas.

Esse tema é atual e recorrente na área de informática, pois, com o aumento do uso da tecnologia, há o aumento do número de crimes no ambiente digital.



Assista, a seguir, ao vídeo "Documentário CLT 70 Anos – TRT-GO" sobre a "história do direito trabalhista, que demonstra o avanço das leis que asseguram direitos ao trabalhador.



EXPLORANDO OS CONCEITOS



Exploraremos, agora, os aspectos do direito relacionados ao profissional de informática. Caso tenha alguma dúvida ou queira discutir sobre o tema em estudo, você poderá apresentar

os questionamentos no fórum específico desta unidade, chamado "Fórum – Unidade 4", um canal de interação entre os participantes desta disciplina e o professor. Neste fórum, pesquise e apresente, como discussão inicial, exemplos de modalidades de trabalho em que um profissional de informática poderá atuar na sua vida laboral.

ASPECTOS DO DIREITO RELACIONADOS AO PROFISSIONAL DE INFORMÁTICA

O direito do trabalho pode ser considerado uma especialidade do direito, que organiza e disciplina os princípios, as normas e as instituições do direito nas relações trabalhistas; "determinam os seus sujeitos e as organizações destinadas à proteção desse trabalho em sua estrutura e atividade", conforme Amauri Mascaro Nascimento (2001, p. 61).

O trabalhador possui respaldo legal, um conjunto de direitos que o trabalho individual e coletivo deve considerar como fundamento para as relações de trabalho. Cuidados com o trabalhador foram inseridos na legislação, como a segurança e a medicina do trabalho, e nas normas trabalhistas, fundamentais para assegurar a saúde e o bem-estar do trabalhador.

O direito trabalhista encontra-se respaldado na Constituição Federal de 1988 nos artigos 7º ao 11, e entre os artigos. 111 ao 117.

Os direitos trabalhistas são previstos pela Constituição Federal. Entre os direitos dos trabalhadores, está o direito à aposentadoria amparada pela Seguridade Social Brasileira, vista na Previdência Social. Para consolidar-se como segurado, você deverá ser filiado e cadastrado na previdência social, através do Instituto Nacional da Seguridade Social (INSS). Pesquise sobre a filiação

ao INSS e sobre a qualidade de segurado, enaltecendo o momento em que o indivíduo perde esta qualidade e quais as consequências e implicações de não estar filiado ao INSS. Faça uma Síntese dessa pesquisa e apresente na tarefa: "Síntese – Qualidade de Segurado do INSS".

O direito e as relações de trabalho encontram-se normatizados na Consolidação das Leis do Trabalho (CLT), Lei nº 5.452 de 1 de maio de 1943.

Além desta importante lei para os trabalhadores, as fontes do direito do trabalho também são consideradas:

- Constituição Federal.
- Leis esparsas;
- decretos, medidas provisórias e portarias;
- jurisprudência;
- convenções e acordos coletivos;
- regulamento interno das empresas;
- costume;
- tratados internacionais;
- doutrina.

Entre os princípios do direito, que também são empregados para o direito trabalhista, temos os específicos, que orientam esta especialidade. A seguir alguns princípios do direito trabalhista:

- Princípio da aplicação da norma mais favorável ao trabalhador.
- Princípio da irrenunciabilidade dos direitos pelo trabalhador.
- Princípio da primazia da realidade dos fatos.
- Princípio da continuidade da relação de emprego.
- Princípio da regra de condição mais benéfica, também chamada do direito adquirido.

As fontes do direito trabalhista subsidiam e protegem a relação de trabalho, que poderá confundir com contrato de emprego. Assim, você terá que entender estas classificações.

Relação de trabalho e relação de emprego são consideradas expressões distintas. A relação de emprego está formalizada pelo contrato de emprego, que se trata de uma espécie de relação de trabalho, pois "designa apenas relação entre empregador e trabalhador subordinado, ao passo que relação de trabalho abrange quaisquer relações de prestação de trabalho, mesmo não subordinado" (ZIMMERMANN NETO, 2004, p. 23). Zimmermann (2004) relata que a relação de trabalho evidencia-se quando uma pessoa presta serviço à outra e essa relação cria um vínculo jurídico, configurado pelos interesses particulares entre as partes, tendo como resultado direitos e obrigações entre as partes.

Desse modo, pode-se dizer que o contrato de trabalho (também chamado de contrato de emprego) encontra-se formalizado quando há termos de um acordo entre trabalhador e tomador do trabalho , criando uma relação de emprego, possuindo, entre outros critérios, a subordinação.

Você é responsável pelos seus atos cometidos no meio tecnológico e por isso precisa tomar cuidado para não ser vítima de fraudes ou crimes cometidos por atos ilícitos de terceiros.

Assim, conclui-se que nem toda relação de trabalho é uma relação de emprego.

Para ser considerada uma relação de emprego, deve possuir algumas características:

- Subordinação.
- Pessoalidade.
- Pessoa física.
- Onerosidade ou contraprestação.
- Continuidade ou não eventualidade.

Preenchendo os requisitos anteriores, independentemente do contrato de trabalho ou contrato de emprego assinado, estabelece-se a relação de emprego. Sobre ela, incidem todos os direitos trabalhistas de um emprego formalizado pelo contrato de trabalho, ou seja, com a carteira de trabalho assinada.

Uma relação de trabalho pode ser determinada como qualquer vínculo jurídico ao qual uma pessoa natural executa um trabalho mediante contraprestação (pagamento). Existem relações de trabalho que não se caracterizam como uma relação de emprego, pois não preenchem os requisitos necessários para tal situação.

Você verá a seguir algumas relações de trabalho que não configuram relação de emprego:

- A relação de trabalho autônomo: nesta relação de trabalho não existe dependência ou subordinação jurídica entre o prestador de serviços e o respectivo tomador. O trabalho é desenvolvido de forma autônoma, com profissionalismo e habitualidade, o risco inerente ao trabalho será do contratado autônomo.
- Relação de trabalho voluntário: esta relação de trabalho refere-se ao disposto na lei nº 9.608/98 (BRASIL, 1998), que determina que este trabalho será exercido sem o recebimento de contraprestação, sem remuneração.
- Relação de trabalho eventual: relação de trabalho de forma temporária, que não possui habitualidade e ou está relacionada com a atividade fim da empresa.
- Estágio: o estágio é uma relação de trabalho diferenciada daquilo disposto na CLT, pois possui o dispositivo legal específico: a lei nº 11.788/08.
 Essa lei assegura que o estágio é um ato escolar supervisionado (Art. 1º), que não configura vínculo empregatício desde que atenda aos requisitos

de: matrícula e frequência escolar ao curso; celebração do termo de compromisso (contrato de estágio assinado pelo educando, Instituição de Ensino e contratante do estágio); compatibilidade de atividades (Art. 3°, caput, incisos I a III).

Entre essas relações de trabalhos, não estão preenchidos "todos" os requisitos da relação de emprego; assim, não serão reconhecidos como uma relação deste tipo.

Os requisitos para configurar-se como uma relação de emprego serão conceituados conforme a seguir:

- Subordinação relação de dependência, hierarquia. O empregado é subordinado ao empregador, que poderá aplicar penalidades ao empregado (advertência, suspensão disciplinar e dispensa por justa causa).
- Pessoalidade trabalho executado pessoalmente pelo empregado contratado, ou por quem possuir uma relação de trabalho; este não poderá ser substituído por outro indivíduo.
- Pessoa física trabalho executado por pessoa física ou natural, não podendo ser pessoa jurídica.
- Onerosidade trabalho com contraprestação, remuneração, ao empregado, dos serviços prestados. Caso não ocorra o pagamento de uma remuneração, trata-se de trabalho voluntário.
- Continuidade trabalho não eventual, prestado em caráter contínuo, no qual o empregado executa a atividade laboral continuamente, com habitualidade.

Independente de assinado, ou não, o contrato de trabalho entre o empregador e empregado, a relação de trabalho que preencher os critérios anteriores, como forma de requisitos da relação de emprego, o trabalhador já se configura com os direitos trabalhistas de um contrato formal de emprego, incidindo verbas e benefícios sob todo o tempo de trabalho configurado nestes requisitos.

CONTRATO INDIVIDUAL DE TRABALHO

O contrato de trabalho é considerado um acordo tácito ou expresso, correspondente à relação de emprego. O empregado receberá uma remuneração para prestar um trabalho a outra pessoa, chamado empregador. Os requisitos do contrato de trabalho são: capacidade dos contratantes, idoneidade do objeto, ou seja, objeto lícito, forma prescrita e não defesa em lei (conforme a legalidade), caso contrário, não preenchendo estes requisitos, o contrato é nulo ou anulável.

Os contratos de trabalho poderão estabelecer que o trabalho seja desenvolvido ou efetuado em domicílio. Neste caso, será realizado no domicílio do empregado, resguardando os direitos oficiais e não se distinguindo a relação entre o trabalho realizado no estabelecimento do contratante/empregador ou no domicílio do contratado/empregado, conforme o Art. 6º da CLT. Para verificar o que a lei entende como domicílio, recorreremos ao Art. 70 do Código Civil, que descreve como domicílio da pessoa natural o lugar em que esta estabelece a sua residência com ânimo definitivo.

TERCEIRIZAÇÃO

Outra relação de trabalho encontrada é a terceirização. Trata-se do "contrato pelo qual a empresa produtora (tomador de serviços) entrega a outra empresa a execução de determinada tarefa (atividades e serviços não incluídos em seus fins sociais) para que esta realize habitualmente através de seus próprios empregados" (CARRION, 2009, p. 307).

Somente será terceirizada a atividade meio da empresa, que corresponde à atividade complementar, de apoio, que não integra o fim principal buscado. Assim, a atividade fim não será terceirizada, a atividade fim corresponde ao trabalho preponderante dentro da empresa, a atividade essencial, e conforme o Ministério do Trabalho e Emprego (MTE) entende-se que está ligada ao objeto social da empresa, aquilo que a empresa é especializada.

RELAÇÃO DE TRABALHO DO PROFISSIONAL DE INFORMÁTICA

O profissional da área de informática, comumente, poderá optar pelo contrato de trabalho, estabelecendo uma relação de emprego, mas também, poderá optar por prestar o trabalho como "Pessoa Jurídica" (PJ).

Quando este trabalhador opta pela relação de emprego, efetuando um contrato de trabalho ou de emprego, supõe-se todos os requisitos necessários para configuração desta relação e todos os benefícios concedidos aos trabalhadores, conforme a CLT e os direitos estabelecidos pelos registros de classe profissional. Entre estes benefícios, encontramos: carteira de trabalho assinada pelo empregador, repouso semanal remunerado, décimo terceiro salário, direito à férias remuneradas mais um terço (1/3) do salário, Fundo de Garantia por Tempo de Serviço (FGTS), horas extras remuneradas, aviso prévio, seguro desemprego, entre outros.

Outra forma encontrada é chamada de "PJ". Quando o trabalhador opta por se tornar Pessoa Jurídica e prestar o serviço ao contratante, receberá o pagamento pelo serviço prestado e emitirá Nota Fiscal como comprovação de pagamento, recolhendo os tributos vinculados. Neste caso, o profissional de informática abrirá uma empresa, em seu nome, como empresário individual, passando a configurar outra forma de relação de trabalho, somente de prestador de serviços, sem direitos as verbas indenizatórias do trabalhador com relação de emprego. Em contrapartida, trabalhar como Pessoa Jurídica (PJ) poderá trazer vantagens. Trata-se de mais uma forma de atuação profissional. Conforme a necessidade individual de cada trabalhador, este poderá analisar duas opções de

atuação profissional e decidir qual melhor se refere aos seus objetivos pessoais.

O trabalhador, caracterizado como Pessoa Jurídica, deve abrir uma empresa e prestar o serviço que consta no contrato social da empresa. Esta empresa deverá ser registrada, possuir um Cadastro Nacional de Pessoa Jurídica (CNPJ), com enquadramento tributário conforme sua atuação, efetuar o pagamento dos impostos referenciados conforme uma empresa qualquer, sendo que, neste caso, a empresa prestará o serviço. Este trabalhador será classificado como Microempresário Individual (MEI) ou Empresário Individual (EI), dependendo do faturamento da empresa.

A contratação da prestação de serviço na modalidade PJ será feita por um contrato comercial de prestação de serviço. Não apresenta-se o vínculo empregatício, pois não preenche os requisitos necessários para relação de emprego, sendo o primeiro ausente a subordinação. O contrato poderá ser rescindido conforme as cláusulas de rescisão estabelecidas no contrato comercial.

Na modalidade de trabalho PJ, a prestação de serviço possui algumas características que, em comparação a relação de emprego (conforme a CLT), apresentam pontos positivos, tais como, possibilidade de maior rendimento imediato, estipulação de horários flexíveis conforme o contrato estabelecido, renda conforme o trabalho prestado independente de horários mínimos ou máximos, pois não há o vínculo empregatício e poderá extrapolar o número de horas trabalhadas limitadas estabelecidos pela CLT.

O trabalhador PJ deverá atentar-se que, nesta modalidade profissional, não terá os benefícios sociais garantidos pelas leis trabalhistas conforme uma contratação fixada pela relação de emprego. Entre estes benefícios, encontram-se férias, décimo terceiro salário, FGTS, seguro desemprego, licenças médicas, aviso prévio. Com isso, ao assinar um contrato como PJ, deverá efetuar os devidos cálculos financeiros para suprir minimamente estas vantagens que o trabalhador com relação de emprego possui, além de incluir os gastos com impostos e contadores.

As vantagens e desvantagens de cada modalidade de trabalho serão julgadas conforme o foro íntimo, as necessidades e os interesses individuais de cada trabalhador da área de informática.

O profissional da área de tecnologia e informação, contratado com vínculo empregatício (CLT) poderá ser contratado também por uma modalidade chamada CLT FLEX (ou CLT por Cotas).

Neste caso, o empregador contrata o empregado com a relação de emprego, mas a remuneração se diferencia da forma tradicional encontrada com todos os benefícios ou vantagens empregatícias, pois o salário contratado será recebido normalmente, mas os benefícios estipulados no contrato serão pagos sem apresentarem-se no contrato, chamado "pagamento por fora". Esta modalidade merece uma atenção especial, pois os valores recebidos "por fora", em alguns casos, poderão ultrapassar o valor do salário contratado, uma vez que não incidem para o cálculo das verbas trabalhistas.

Assim, constata-se que os benefícios seriam superiores ao valor do salário do empregado, configurando um desequilíbrio prejudicial aos direitos do empregado.

ATENÇÃO COM O COMÉRCIO ELETRÔNICO

A crescente demanda comercial por meios digitais trouxe a necessidade de um profissional de informática atento para assegurar as transações comerciais por meios digitais.



Assista aos vídeos a seguir que tratam do comércio eletrônico: "O que é e-commerce?" (2015) e "Entenda o Mercado Eletrônico" (2012).

O comércio eletrônico pode ser definido como:

Negócios conduzidos exclusivamente através de um formato eletrônico. Sistemas que se comunicam eletronicamente uns com os outros são sistemas de e-commerce, e têm de ser capazes de funcionar normalmente com quaisquer aplicações da Internet que estiver planejando utilizar. Também se refere a quaisquer funções eletrônicas que auxiliam uma empresa na condução de seus negócios. (SMITH; SPEAKER; THOMPSON, 2000, p. 74).

O comércio eletrônico trata-se de um ramo econômico, composto pela comercialização de produtos, pelos serviços, pelas informações e pela propriedade intelectual através de meios eletrônicos, principalmente pela internet.

Os ilícitos encontrados no comércio eletrônicos baseiam-se nas transações comerciais, na movimentação de dados pela internet, no uso de sistemas computacionais e, por se tratar de relações de consumo, na confiança existente em uma operação de compra e venda, ou no contrato de um serviço por meio digital.

Estes ilícitos podem ser dos mais variados tipos, como fraudes, furtos, invasões de sistemas computacionais privados, furtos de dados, falsidade ideológica, entre outros. Estes ilícitos no comércio eletrônico podem ocorrer de forma isolada ou concorrente, ou seja, de forma concomitante, associadas a outros atos. Por exemplo, invasão de sistemas computacionais privados associados com o furto de dados privados, como senhas de instituições financeiras e, posteriormente, o furto virtual.

Outra prática encontrada nos atos ilícitos em comércio eletrônico seria a propaganda enganosa em sites fraudulentos, que enganam o comprador oferendo produtos que não entregam conforme o combinado na comercialização, somente para capturar os dados pessoais e financeiros, usando-os em outras transações ilícitas.

Alguns cuidados são necessários para efetuar uma transação comercial segura pela internet, como uma pesquisa de mercado sobre o produto ou o serviço a ser contratado, sobre informações sobre o vendedor; não é recomendável utilizar links ou spams para acessar lojas ou comércios virtuais, prefira utilizar o navegador de internet com o endereço eletrônico. Pesquisar em sites de informações e reclamações comerciais sobre a comercialização pretendida, evitar a compra por impulso, sem pensar na segurança, anotar o código de rastreamento quando da entrega do produto pelos correios são dicas úteis.

Além destas medidas de segurança, aplicam-se todas as formas de cuidados com a segurança que o usuário de sistemas computacionais e de internet deva ter, com malwares e usabilidade.

O direito do consumidor protege vendedores e consumidores, regulando e enquadrando as transações comerciais, conforme a Lei nº 8.078 de 1990. Outra forma de proteção é acionar o Programa de Proteção e Defesa do Consumidor (PROCON) que auxilia a dirimir os conflitos relacionados ao direito do consumidor.

Visite o site da Associação Brasileira de Comércio Eletrônico e acompanhe as notícias e informações desta instituição.



APROFUNDANDO CONCEITOS

A seguir você encontrará uma lista de recursos extras que complementarão o conteúdo dessa unidade. Essas indicações são artigos, sites e vídeos, alguns já indicados no decorrer da Unidade, que auxiliarão no estudo e no aprofundamento dos conceitos a respeito da temática abordada. Por exemplo, o projeto de lei em curso no congresso nacional que discute a regulamentação da profissão de informática, a CLT, um vídeo contando a história do direito do trabalho, entre outros.

Leia a matéria "Profissão de Informática" (2016) no site da Sociedade Brasileira de Computação (SBC).

Consolidação das leis do trabalho (BRASIL, 1943).

Associação Brasileira de Comércio Eletrônico - ABCOMM.

Documentário CLT 70 Anos - Tribunal Regional do Trabalho de Goiás -TRT-GO.

Vídeo sobre comércio eletrônico: O que é e-commerce?

Curso de direito do trabalho (BARROS, 2011). São Paulo: LTr, 2011. Ebook.

Vídeo sobre comércio eletrônico: Entenda o Mercado Eletrônico.







O profissional da área de informática deve estar atento com a legislação trabalhista, com as formas de contratação e com as relações de trabalho existentes. Verificar os critérios necessários para caracterização de uma relação de emprego e a possibilidade de constituição de uma empresa individual, para prestação de serviços, como formas de atuação profissional.

O contrato de trabalho também poderá sofrer uma flexibilização com a possibilidade de os benefícios serem pagos a parte, somente contratado o salário na relação de emprego, modalidade esta chamada de CLT Flex; no entanto, devese ter atenção reforçada neste aspecto, para que não sejam cometidos abusos de direitos em detrimento do trabalhador.

Um Projeto de Lei (PL) está no Congresso Nacional com o objetivo de regulamentar a profissão na área de informática. São eles o PL 3.065/15, de 23 de setembro de2015, e o PL 4.408/16, de 17 de fevereiro de 2016. Entre os Projetos de Lei, surge o debate sobre regulamentação da profissão de informática estabelecendo critérios e orientações para sua atuação.

A Sociedade Brasileira de Computação postou em seu site oficial informações sobre este debate. Leia a matéria, faça uma síntese sobre os projetos apresentando os prós e os contras, as suas diferenças e emita sua opinião sobre o tema, comentando com qual dos projetos de lei você está de acordo, justificando sua escolha. Poste esta síntese na tarefa: "Síntese sobre os Projetos de Lei".

Após redigir esse texto, leve sua opinião para o "Fórum - Profissão de Informática": Qual dos dois projetos de lei você está de acordo? Participe desse fórum justificando sua escolha e comentando a postagem de pelo menos um colega.



- BARROS, A. M. Curso de Direito do trabalho. São Paulo: LTr, 2011.
- ▶ BRASIL. Constituição (1988). Constituição da República Federativa do Brasil, de 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 4 abr. 2016.
- ▶ BRASIL. Lei nº 5.452, de 1 de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Diário Oficial da União, Brasília, DF, 9 ago. 1943. Seção 1, p. 11937. Disponível em: http://moodle.mackenzie.br/link/1cn. Acesso em: 5 maio 2016.
- ▶ BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, DF, 19 set. 1990. Seção 1, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm. Acesso em: 2 maio 2016.
- ▶ BRASIL. Lei nº 9.608, de 18 de fevereiro de 1998. Dispõe sobre o serviço voluntário e dá outras providências. Diário Oficial da União, Brasília, DF, 19 fev. 1998. Seção 1, p. 2. Disponível em: http://moodle.mackenzie.br/link/1co. Acesso em: 22 ago. 2016.
- ▶ BRASIL. Lei nº 11.788, de 25 de setembro de 2008. Dispõe sobre o estágio de estudantes; altera a redação do art. 428 da Consolidação das Leis do Trabalho CLT, aprovada pelo Decreto-Lei nº 5.452, de 1 de maio de 1943, e a Lei nº 9.394, de 20 de dezembro de 1996; revoga as Leis nº 6.494, de 7 de dezembro de 1977, e nº 8.859, de 23 de março de 1994, o parágrafo único do art. 82 da Lei nº 9.394, de 20 de dezembro de 1996, e o art. 6º da Medida Provisória nº 2.164-41, de 24 de agosto de 2001; e dá outras providências. Diário Oficial da União, Brasília, DF, 26 set. 2008. Seção 1, p. 3. Disponível em: http://moodle.mackenzie.br/link/1cp. Acesso em: 22 ago. 2016.

- CARRION, V. Comentários à consolidação das leis do trabalho. 34ª edição. Atualizada por Eduardo Carrion. Legislação Complementar e jurisprudência. São Paulo: Saraiva, 2009.
- DOCUMENTÁRIO CLT 70 ANOS TRT-GO. Goiânia: Núcleo de Comunicação Social do Tribunal Regional do Trabalho de Goiás, 28 maio 2013. Disponível em: http://moodle.mackenzie.br/link/1cq>. Acesso em: 1 maio 2016.
- ENTENDA O MERCADO ELETRÔNICO. Produção: Marcado Eletrônico. [S.l.]: Mercado Eletrônico, 23 maio 2012. Disponível em: http://moodle.mackenzie.br/link/1cr. Acesso em: 19 maio 2016.
- NASCIMENTO, A. M. Iniciação do direito do trabalho. São Paulo: LTr, 2001.
- MARTINS, S. P. Instituições de direito público e privado. 3. ed. São Paulo: Atlas, 2003.
- O QUE É E-COMMERCE? Produção: Hotmart. [S.l.]: Focus Market, 8 nov. 2015. Disponível em: http://moodle.mackenzie.br/link/1d2>. Acesso em: 19 maio 2016.
- Profissão de Informática. Sociedade Brasileira de Computação, Porto Alegre, 2016. Disponível em: http://moodle.mackenzie.br/link/1d5>. Acesso em: 5 maio 2016.
- REIS, H. M.; REIS, C. N. P. Direito para administradores. São Paulo: Thomson, 2006. 1. v.

- SMITH, R.; SPEAKER, M.; THOMPSON, M. O mais completo guia sobre e-commerce. 1. ed. São Paulo: Futura, 2000.