PERCURSO DE APRENDIZAGEM 3

Universidade de Fortaleza | EAD

ÉTICA EM COMPUTAÇÃO

TRANSTORNOS DE CONDUTA E CONFLITO NO CIBERESPAÇO

TRANSTORNOS DE CONDUTA E CONFLITO NO CIBERESPAÇO

Sumário

Sumário clicável

Abordaremos, neste percurso, um tema de grande relevância e de constante debate: os transtornos de conduta e conflito no ciberespaço. Provavelmente, você deve ter ouvido falar ou se deparado com alguma conduta considerada inadequada ou criminosa em ambientes digitais. Ao tempo em que conheceremos melhor o que caracteriza um crime digital, será necessário contextualizar a legislação que trata do assunto e que permeia questões como a privacidade e a propriedade intelectual, entre outras. Além disso, iremos entender a definição dos crimes cibernéticos e seus impactos. Relevante tipificar os crimes digitais, conhecendo sua classificação e os mecanismos que norteiam sua coibição e investigação. Acompanhe!

Olá

1. Políticas e legislação aplicadas ao ciberespaço: privacidade, pirataria, invasões e propriedade intelectual

Conforme estamos expondo ao longo deste componente curricular, a ética não é sinônimo de legislação. Porém, o debate ético também leva à reflexão sobre a criação de mecanismos legais, os quais podem conduzir o disciplinamento das relações sociais, levando à superação e redução de conflitos nas mais diferentes esferas do comportamento.

No que consiste às tecnologias da informação, não seria diferente imaginar que seu gradativo aumento e popularização exigissem disciplinamento e orientações quanto a condutas que trazem danos sociais. Por esse motivo, nos deparamos com o debate sobre as políticas e a legislação que cerca esse ambiente, dando destaque às tecnologias do ciberespaço.

Importante!

Importante ressaltar que o ciberespaço não é uma terra sem lei. É corrente a ideia de que, ao adentrar em ambientes digitais, em que se pode ter acesso a inúmeros perfis, se está "livre" de coerções sociais e legais, levando à percepção de que alguém pode ofender e praticar ilicitudes sem ser identificado. Essa ideia, contudo, é falsa; para não dizer ingênua.

Temos à disposição, contemporaneamente, mecanismos para o enfrentamento de diversas questões e condutas que disseminam "maus usos" da rede mundial de computadores. O debate perpassa usuários de diferentes níveis de competência digital – desde as mais básicas às avançadas.

Além disso, no campo profissional e ético, o conhecimento do marco legal que versa sobre as políticas de privacidade, pirataria ou propriedade intelectual, ressalta condições fundamentais para o exercício ético e técnico de profissões diretamente relacionadas à tecnologia da informação.

Perceba que do momento em que o primeiro *chip* foi criado até a fabricação e o lançamento do computador pessoal (PC) passaram-se quase vinte anos. Daí em diante, as mudanças ocorrem em escala e velocidade cada vez maiores, desencadeando e viabilizando a convergência tecnológica (PINHEIRO, 2016).

Porém, toda essa tecnologia nos traz um ponto que merece muita atenção: os crimes cometidos por meio da internet. Ainda que essa questão seja central e mais detalhada no próximo circuito, não podemos deixar de conceituar, introdutoriamente, o tema. Condutas dessa natureza podem ser chamadas de crimes virtuais, informáticos, eletrônicos, digitais ou mesmo cibercrimes (SUDRE; MARTINELLI; CAPANEMA, 2020).

Apesar de existirem leis que podem ser aplicadas ao campo digital, foi necessário pensar em normas jurídicas próprias, com o propósito de autorizar o Poder Público na realização de "[...] investigações para identificar os autores das diversas condutas delituosas, permitindo que fossem levados a julgamento, seja para cumprirem uma pena, seja para repararem um dano" (SUDRE; MARTINELLI; CAPANEMA, 2020, p. 141).

Tomar conhecimento desses parâmetros é elementar ao profissional que atua nesse universo, cujo papel social não está restrito ao conhecimento técnico, mas a atuação responsável e ética.

Nosso propósito, neste circuito, é tornar mais claro o entendimento da legislação que toca em questões essenciais no âmbito das tecnologias de informação e comunicação (TIC), cujos usos e efeitos produzem comportamentos e práticas específicas.

Assim, no que se refere ao ordenamento jurídico, cabe a preocupação em se discutir e garantir o direito à privacidade, a proteção dos direitos autorais, de imagem, a propriedade intelectual, a segurança da informação etc. Desse modo, ambienta-se o "Direito Digital", entendido como capaz de criar instrumentos para atender a tais expectativas (PINHEIRO, 2016).

Pinheiro (2016, p. 116) acrescenta que o Direito Digital se refere ao

> "[...] Direito aplicado a um modelo socioeconômico-político-jurídico de Sociedade que se manifesta de forma não presencial, por meio de testemunhas-máquinas, provas eletrônicas, e na qual o modelo de riqueza é a informação, sem fronteiras físicas ou temporais, em tempo real".

Nesse sentido, conforme Pinheiro (2016), surge a necessidade de se instituir regras de convivência social. Para essa autora, na relação com o contexto digital, sobressaem temas como (PINHEIRO, 2016, p. 116):

- Privacidade do Indivíduo x Segurança Pública Coletiva;
- Liberdade de Expressão x Responsabilidade;
- Identidade Obrigatória x Anonimato;
- Proteção de Dados x Acesso à Informação;
- Crimes Digitais (novos tipos penais).

Todas essas questões perpassam usos e efeitos de ambientes digitais, trazendo complexidades às tecnologias próprias ao contexto que enfrentamos.

Sudre, Martinelli e Capanema (2020) afirmam que computadores pessoais se popularizaram no Brasil desde a década de 1980. A expansão gradativa do uso dessa tecnologia ocorre ainda no final do século XX.

Entretanto, a primeira atualização do Código Penal, visando tipificar e adequar-se a esse novo contexto só ocorreu no ano 2000, por meio dos artigos 313-A e 313-B, os quais reconhecerão como crimes (SUDRE *et al*., 2020):

- a inserção de dados falsos em sistemas de informação (art. 313-A); e
- a modificação ou alteração não autorizada de sistemas de informação (art. 313-B).

Porém, o marco legal só se tornará mais consistente no Brasil com a Lei 12.737 (apelidada de Lei Carolina Dieckmann), promulgada em 2012.

Vale recordar que, no Brasil, já se discutia um Projeto de Lei de Crimes Eletrônicos (conhecido como Lei Azeredo) desde 1999, mas o debate só consegue avançar mais

de uma década depois, após o chamado efeito “Carolina Dieckmann”, que recebeu esse título por conta da divulgação não autorizada de fotografias íntimas da atriz, seguida da tentativa de extorsão e ameaça por parte de quem havia tido acesso ao equipamento e aos seus arquivos pessoais (PINHEIRO, 2016). A lei trata do crime de “invasão de dispositivo informático” (art. 154-A, Código Penal).

Pinheiro (2016) acrescenta que dar tratamento legal à matéria não é tão simples, uma vez que é necessário conhecimento técnico sobre a questão tecnológica. Segundo esclarece a autora, o computador – ou outro dispositivo eletrônico com funções semelhantes, como um *smartphone*, por exemplo – “[...] não consegue, como testemunha que é, diferenciar uma conduta dolosa (com intenção) de uma culposa (sem intenção)” (PINHEIRO, 2016, p. 119).

Essa questão traz como consequência a possibilidade de criminalização de ações que, em tese, são inocentes, tais como enviar, sem querer ou sem conhecimento, um vírus de computador para outra pessoa. Desse modo, é preciso aprender a utilizar os recursos tecnológicos de forma ética, segura e em conformidade com princípios legais (PINHEIRO, 2016).

Importante!

Cabe salientar que o marco legal acerca da temática, devemos reforçar, é preocupação em escala internacional.

Ocorrida no início dos anos 2000 – precisamente em 23 de novembro de 2001 – a Convenção de Budapeste tornou-se conhecida como Convenção sobre o Cibercrime (MOLITOR e VELAZQUEZ, 2017).

Trata-se do primeiro tratado internacional que abordará crimes cometidos por meio da internet. A Convenção de Budapeste foi proposta pelo Conselho Europeu e entrou em vigor em 1 de julho de 2004. Até outubro de 2010, trinta países haviam assinado o tratado, aderindo à Convenção e ratificando suas proposições (MOLITOR; VELAZQUEZ, 2017).

A Convenção, em seu preâmbulo, ressalta a importância e o dever de coibir, dando tratamento jurídico-legal a atos praticados

> [...] contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos e da adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infrações tanto no nível nacional como internacional e estabelecendo disposições para uma cooperação internacional rápida e eficiente (MOLITOR e VELAZQUEZ, 2017, p. 92).

O Brasil ainda não aderiu à Convenção de Budapeste, porém, em junho de 2021, em audiência pública realizada pela Comissão de Relações Exteriores e Defesa Nacional, deu parecer favorável à adesão. Os dois principais eixos que orientam a Convenção são o compromisso em elaborar leis que tipifiquem e punam as condutas previstas no tratado internacional, e aderir às medidas de cooperação, que prevê ferramentas que tornam mais eficaz o combate a crimes cibernéticos em território nacional e supranacional (CÂMARA DOS DEPUTADOS, 2021).

O acordo é considerado importante, uma vez que pode trazer como vantagens um modelo legislativo homogêneo e o uso de mecanismos de cooperação que sejam mais ágeis na condução de processos investigativos transnacionais. Além disso, haveria o favorecimento quanto ao intercâmbio de experiências, no que diz respeito aos procedimentos e conhecimentos técnicos que já estejam sendo adotados em outros países no combate aos crimes digitais (MOLITOR; VELAZQUEZ, 2017).

Em síntese, o Brasil conta com dispositivos jurídicos que disciplinam e dão tratamento legal aos crimes digitais. Alguns dos que já pontuamos foram: os artigos 313-A e 313-B, do Código Penal, em 2000; e a Lei nº 12.737/2012.

Marcos legais relevantes são o Marco Civil da Internet, Lei nº 12.965/2014 e a Lei Geral de Proteção de Dados, a LGPD, Lei nº 13.709/2018.

Vejamos melhor do que tratam cada um desses dispositivos (Quadro 1):

Quadro 1 – Marco Civil da Internet e Lei Geral de Proteção de Dados (LGPD)

Marco Civil	LGPD
O Marco Civil representa um primeiro passo na busca de uma proposta legislativa que seja transversal e possibilite um posicionamento consistente acerca de temas relativos às condutas na internet e que carecem de melhor disciplinamento, tais como: a proteção de dados pessoais; os direitos autorais; a governança da internet; o comércio eletrônico; os crimes digitais; a atividade de centros públicos de acesso à internet, dentre outros (MOLITOR e VELAZQUEZ, 2017).	Já a Lei Geral de Proteção de Dados (LGPD) dá outro significativo passo, tendo como objetivo proteger a privacidade, assegurando o direito à proteção de dados pessoais, por meio de ações seguras e transparentes. A proteção de dados tem em vista a regulamentação de atividades que envolvam a utilização de dados pessoais, abrangendo os meios digitais, tanto por pessoas físicas como jurídicas (LGPD BRASIL, 2021).

Fonte: elaborado pelo autor (2021)

Vale destacar o tratamento jurídico de algumas questões no âmbito digital. Questões voltadas à privacidade ou a proteção aos direitos autorais contam com dispositivos legais previamente garantidos, não significando dizer que a preocupação com essas questões advém com a internet e seus recursos. O que se discute atualmente são as

especificidades e particularidades próprias ao manuseio de informações pessoais, assim como outros assuntos, em meios digitais.

No que diz respeito à privacidade, a Constituição Federal de 1988, no artigo 5º, garante a proteção do indivíduo, assim como de sua vida privada, imagem ou reputação e direito à liberdade de expressão (PINHEIRO, 2016).

Importante!

Pinheiro (2016) esclarece que a relação entre o direito à privacidade e à liberdade de expressão fica resolvida na mesma norma, em que se determina que a manifestação de pensamento é livre, estando proibido o anonimato, tendo em vista que uma pessoa pode falar o que pensa, porém, deve responder pelo diz.

De acordo com a autora (2016, p. 116):

> [...] em apenas dois artigos da Lei Magna de nosso ordenamento jurídico, há uma tentativa de se harmonizar a vontade do indivíduo (privacidade, liberdade, anonimato) com a necessidade de proteção dos demais, do coletivo (segurança, responsabilidade, identidade obrigatória).

Regulamentar e deixar transparentes as questões que tratam da privacidade, assim como da responsabilidade no uso e divulgação de dados tem sido uma questão fundamental no contexto digital.

Aumenta gradativamente o número de organizações que disputam consumidores e usuários da internet, a fim de direcionar publicidade, via preenchimento de cadastros, formulários... dentre outros instrumentos e recursos. Ao mesmo tempo, é possível notar o maior grau de conscientização de consumidores frente a esses mecanismos, tendo em vista o atual Código do Consumidor, que também trata do uso de informações das pessoas para fins comerciais e suas advertências e sanções (PINHEIRO, 2016).

Sobressae desse cenário a preocupação com o modelo de negócio que se estabelece, na medida em que informações e dados pessoais transformam-se em moeda de troca, baseados no intenso fluxo da rede e na possibilidade de identificar “padrões de comportamento, prevendo, dentre outros, o que iremos comprar, em qual candidato votar e aptidões profissionais” (PINHEIRO, 2016, p. 96).

Nesse sentido, não é despropositado questionar: qual o limite ético de organizações e corporações quanto ao uso de informações pessoais? O Marco Civil da Internet tem em vista a preocupação com esse limite, trabalhando a transparência e o aviso prévio a clientes e usuários quanto ao que está sendo coletado e para que (PINHEIRO, 2016).

Outras questões relevantes são as que dizem respeito à propriedade intelectual, em especial ao direito autoral, que se encontra garantido pela CF de 1988, assim como por lei própria e no Código Penal.

Pinheiro (2016, p. 174-175) adverte que "[...] o direito autoral, em princípio, protege o titular do direito de autor. Parece algo simples e óbvio, mas, muitas vezes, este detalhe passa despercebido pelo usuário-consumidor do direito autoral, dos conteúdos em geral, bem como pelos concorrentes". A mesma autora orienta que o direito autoral possui dois aspectos, são eles:

- Patrimonial: voltado à valorização do trabalho de criação e inovação, bem como de sua remuneração adequada;

- Moral: representando a proteção à integridade da obra.

Em tempos de tecnologias mais avançadas, há certa facilidade em se adulterar e modificar obras; ao tempo em que existem recursos que permitem a criação de chaves de proteção da obra original. Cabe lembrar que a obra não é mais necessariamente distribuída materialmente, tal como um livro ou CD que se adquiria numa loja. Nos meios digitais, ocorre a "desmaterialização" de tais produtos, levando a novos modelos de distribuição e consumo. Um grande desafio é compreender que nem sempre o que está publicado na internet é "público e pode pegar", levando a cópias e consumo inadvertidos (PINHEIRO, 2016).

Destaca-se que a propriedade intelectual também atinge correspondência eletrônica, programas de computador, artigos, fotografias, bancos de dados disponíveis em servidores etc., são passíveis de receber proteção jurídica autoral. Pinheiro (2016, p. 178) esclarece que

> [...] a Lei já diz que cabe ao autor determinar o que será permitido ou não fazer com sua obra. Sendo assim, de certo modo, os autores podem criar as regras a seu modo, no caso concreto, decidindo o que querem ceder ou não de seu direito. Por isso, muitos têm aderido ao uso da licença *Creative Commons*. Não se pode permitir a formação de uma geração de plagiadores, de copiadores, de pessoas que dizem "achei no Google".

Kon *et al* (2020) comentam que o movimento *Creative Commons*, criado pelo professor de direito da Universidade de Harvard, tem como objetivo o compartilhamento de outras formas de conhecimento – além do que já acontecia com o *software* livre – como algo vantajoso para a sociedade. Desse modo, tais licenças permitem uso e redistribuição sem fins comerciais, mediante permissões específicas e não dispensam atribuição da autoria.

Tai medidas visam o enfrentamento de questões próprias ao que vivenciamos nos meios digitais, preservando preceitos éticos fundamentais.

No próximo circuito, aprofundaremos o tratamento dos crimes digitais e suas implicações.

2. Crimes cibernéticos e seus impactos sociais e profissionais

Como apontamos no circuito um, existem importantes marcos legais que orientam o tratamento jurídico de condutas inadequadas, praticadas por meio de recursos digitais. A interatividade trazida pelos ambientes digitais também trouxe atitudes e reações consideradas inadequadas, trazendo danos a pessoas e instituições.

Por consequência, um importante efeito social decorrente da internet são os transtornos de conduta e as práticas criminosas que provocam mal-estar social. Uma dessas consequências são comportamentos considerados abusivos e ilícitos, incentivados pela (ainda que falsa) sensação de anonimato que pessoas possuem em ambientes digitais.

Condutas que trazem danos às pessoas e à sociedade em geral encontram lugar na internet, possibilitando roubo de dados e senhas bancárias, extorsão, redes de tráfico de ilícitos (drogas ilegais, armas, dentre outros), *cyberbullying*, redes de pedofilia, crimes de vingança, perseguições ou mesmo ameaças.

> Tanto presencial como virtualmente essas situações ocorrem. Nos meios digitais, o rastreamento dos acessos, com o auxílio de medidas legais, ajuda a identificar agressores e podem dar fim aos abusos.

Como já tivemos a oportunidade de discutir no circuito anterior, você verá inúmeros termos associados a condutas indevidas em meio digital, são eles: cibercrimes, crimes virtuais, crimes informáticos, crimes digitais, crimes eletrônicos, cibernéticos... importante compreender que todos são sinônimos para o mesmo fenômeno.

Vamos adotar, ao longo deste circuito, a nomenclatura “crimes digitais” e, em alguns momentos, “cibercrimes”, para nos referir a essa questão.

Mas como podemos definir o que são os crimes digitais? Quais são suas especificidades? Em que se distinguem de condutas criminosas já praticadas e existentes em ambientes físicos e presenciais?

A definição é simples:

Importante!

Crimes digitais são "condutas criminosas cometidas no ciberespaço" (SUDRE *et al.*, 2020, p. 141).

Ressalte-se que uma conduta criminosa é aquela que fere princípios fundamentais da sociedade, atentando contra a vida, a saúde, ou o direito à privacidade, por exemplo.

Práticas que já são reconhecidas como lesivas podem ser reproduzidas no meio digital, trazendo transtornos. Porém, os crimes digitais possuem modo de atuação que lhes são próprios, distinguindo-se dos que são praticados por meios convencionais e não cibernéticos.

Mas que situações poderiam se enquadrar em crimes digitais?

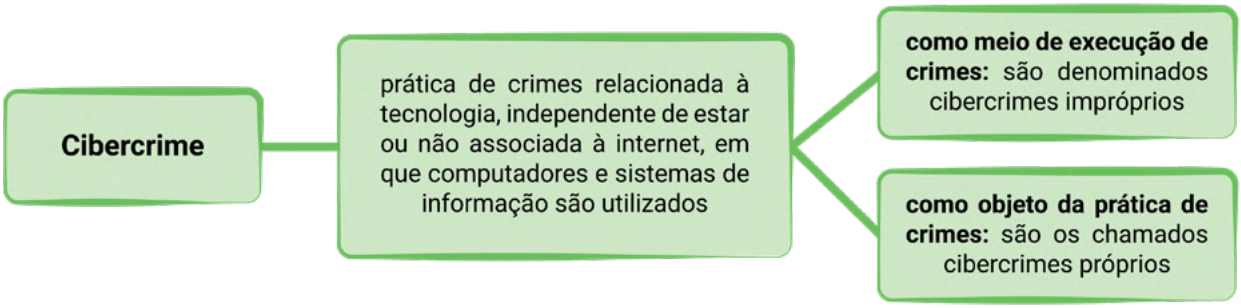
Vamos pensar mais a esse respeito?

São considerados e tipificados como crimes digitais, conforme detalha Pinheiro (2016):

- informações caluniosas e demais crimes contra a honra, publicados e compartilhados por *e-mails*, aplicativos de mensagens etc;
- ofensas digitais (difamação, calúnia e injúria), assim como a ameaça e perturbação, que causam danos sociais e psicológicos ao indivíduo (*cyberbullying*);
- a contaminação por vírus, roubo de senhas e de dados, falsidade ideológica (passar-se por outra pessoa);
- o uso não autorizado de imagens (tanto de si como de terceiros);
- infração aos direitos autorais, que envolve pirataria e plágio;
- espionagem eletrônica;
- vingança digital (uso de imagens, sequestro de perfil ou domínio, apagamento de dados, dentre outras condutas).

Sudre, Martinelli e Capanema (2020) detalham o que são e como são classificados os *cibercrimes* (Figura 1):

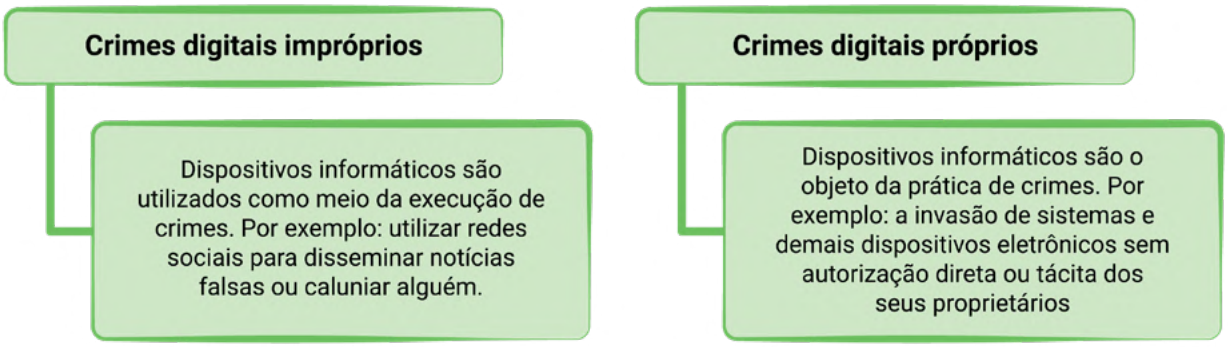
Figura 1 – Cibercrimes – conceito e classificação



Fonte: Elaborada pelo autor (2020)

Note que a classificação é adotada em função do tipo de uso que foi feito da tecnologia, que ora pode ser como meio ou como objeto do crime. Vejamos melhor o que isso significa, por meio de exemplos (Figura 2):

Figura 2 – Crimes digitais impróprios e próprios



Fonte: Elaborado pelo autor (2020).

Essa classificação é importante porque quando o dispositivo ou recurso digital é utilizado apenas como meio de execução de uma determinada prática criminosa não há a necessidade de alteração legislativa para seu reconhecimento. Por exemplo, o crime de calúnia já está tipificado no Código Penal, art. 138, variando, nesse caso, apenas em relação ao recurso e ao mecanismo utilizado para praticá-lo (SUDRE *et al.*, 2020).

EXEMPLO:

Outro exemplo é o caso do "Desafio da Baleia Azul", que veio à tona em 2017. O crime aconteceu por meio da disseminação de uma falsa brincadeira, praticada através de redes sociais digitais, em que suas fases induziam jovens a cometer suicídio. É crime instigar alguém ao suicídio, conforme o Código Penal, art. 122 (SUDRE *et al.*, 2020).

Sobre crimes digitais, Sudre, *et al*., (2020, p. 146) advertem importantes características:

a) nem sempre exigirão perícia técnica: os cibercrimes, embora estejam relacionados à tecnologia, às vezes, não necessitam de grandes conhecimentos técnicos. Em geral, criminosos se utilizam de programas de ataque já prontos e disponíveis, ou os contratam de terceiros. Jovens e menores de idade que se utilizam de programas prontos para fazer ataques são chamados de "*script kiddies*".

b) não respeitam limites geográficos: como grande parte desses crimes ocorre na internet, não há limitação de ordem geográfica. Isso torna possível invasões internacionais, as quais causam dados a servidores ou roubo de dados de usuários de nacionalidades diferentes.

c) proteção da identidade: criminosos, especialmente aqueles que detém maior conhecimento técnico, costumam adotar medidas para ocultar a sua identidade e apagar rastros na internet. É comum mascarar o número IP utilizado, na tentativa de apagar "impressões digitais" de uma invasão, tentando buscar garantir anonimato.

Importante!

Porém, a sensação de total anonimato na rede mundial de computadores é falsa. Isso porque existem enormes possibilidades, com recursos técnicos e legais, de se encontrar cibercriminosos.

Sabendo o que pode ser qualificado como crime digital, um outro passo é fundamental: como identificar sua autoria?

Como se pode chegar em alguém que teve uma conduta passível de criminalização no meio digital?

Eis o ponto que leva à disseminação de crimes dessa natureza, por meio da falsa sensação, como já alertamos, de anonimato.

Sudre, *et al.*, (2020) comentam que um dos princípios mais básicos e fundamentais para isso é a identificação do endereço de IP, horário, data etc. em que se deu determinada(s) ocorrência(s).

Vale destacar, como abordamos no circuito anterior, o papel da legislação a esse respeito. A lei que possibilita o acesso às informações para que uma investigação criminal desse tipo aconteça é o Marco Civil da Internet (MCI) – Lei nº 12.965/2014 (SUDRE *et al*., 2020).

É por recomendação dessa lei que empresas devem manter registros de conexão para a necessidade de futuras requisições judiciais.

Sudre, *et al*., (2020) esclarecem que alguns pontos do MCI são fundamentais na investigação de crimes digitais. Um desses é o detalhamento e a distinção entre provedores de aplicação e provedores de acesso à internet, que terão funções e prazos específicos quanto ao armazenamento e concessão de dados de acesso e registro de usuários, conforme medidas judiciais.

Você tinha conhecimento dessa distinção? Vejamos o que significam!

a) Provedores de aplicação

- Conforme o art. 15 do MCI, são empresas que ofertam algum tipo de serviço na internet, de forma gratuita ou paga. Exemplos: *Gmail* (*Google*), o *Facebook* (*Facebook*), *WhatsApp* (*Facebook*); *Instagram* (*Facebook*); dentre outras;
- Provedores de aplicação são responsáveis por manter os registros de acesso pelo prazo de 06 meses. Esses registros identificam data e horário que determinado endereço IP realizou uma ação na rede (SUDRE; *et al*., 2020).

b) Provedores de acesso

- Conforme o art. 13 do MCI, são empresas que conectam um usuário à internet, como a Vivo, a Oi, a Claro, entre outras;
- Os provedores de acesso são responsáveis por manter os registros de conexão à internet realizada por um dispositivo pelo prazo de 01 (um) ano. Informações sobre data e hora de início e término de uma conexão, duração e endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.
- Após os prazos de armazenamento mencionados, os registros deverão ser excluídos, tanto por provedores de aplicação como de acesso (SUDRE; *et al.,* 2020).

A partir dessas informações, consegue-se investigar ocorrências em meio digital. Sudre; *et al*., (2020) expõem uma situação-problema, considerando um caso hipotético que é relevante para nossa exposição, acompanhe:

Caso hipotético

Manoel ofendeu Felipe no *Facebook*. Felipe procurou a Delegacia de Repressão aos Crimes Eletrônicos – DRCE para registrar um Boletim de Ocorrência – BO, já que a ofensa configura crime de injúria, além de poder gerar danos morais. Porém, Manoel fez tudo utilizando um perfil falso.

O Delegado, desse modo, representará, ao Juiz, o pedido para a quebra do sigilo das informações do registro de acesso do perfil que realizou a postagem ofensiva no dia e hora informados por Felipe. Salienta-se que a informação do Fuso Horário do sistema é fundamental para se chegar à correta autoria do crime, devendo também ser requerida para fins investigativos.

Após o Provedor de Aplicação de Internet disponibilizar os dados solicitados, é preciso verificar a qual Provedor de Acesso à Internet o endereço IP obtido pertence. Para isso, podem ser utilizados dois sites: o Registro.br, para endereços IP brasileiros, e o Lacnic, para endereços IP internacionais.

Com a posse da informação sobre o Provedor de Acesso à Internet, o Delegado deverá requerer novamente ao Juiz pedindo a quebra do sigilo, agora, do registro de conexão à Internet do endereço IP por meio do qual Felipe foi ofendido. Como resultado, serão obtidos os dados do proprietário titular, assinante do serviço de Internet pelo qual o acesso se deu. Mas nem sempre o assinante do serviço de Internet é o mesmo que praticou o crime. Para que essa dúvida seja sanada, entrará em ação a Perícia Forense[1].

No entanto, a Polícia já sabe onde estão os dispositivos que deverão ser investigados. Caso seja necessário busca e apreensão dos equipamentos, o Delegado fará esse requerimento ao Juiz. Após a conclusão do trabalho dos peritos, o ofensor e praticante do crime poderá ser identificado com maior precisão.

Fonte: adaptado de Sudre; et al., (2020, p. 149-150).

Para o mesmo caso, podemos perguntar: mas se o criminoso, ainda assim, não for identificado?

Sudre, Martinelli e Capanema (2020) ressaltam as seguintes consequências: para o Direito Penal, só se pode punir quem praticou o crime. “Já para o Direito Civil, caso ninguém mais seja apontado como praticante do dano moral, o proprietário e assinante do serviço responderá pelas ofensas” (SUDRE, *et al*., 2020, p. 150).

Se o crime ocorrer numa rede interna, a empresa responsável deve ter condições de identificar o usuário que utilizou computador ou outro dispositivo eletrônico para acessar a rede. No Brasil, alguns Estados, como o Espírito Santo, possuem leis voltadas a

1. A computação forense é um ramo profissional científico e tecnicamente relevante nesse aparato investigativo.

Voltar ao sumário

condicionar *lan houses*, *cyber* cafés e demais estabelecimentos que promovem conexão com a internet para guardar informações e registros de acesso. Ainda que os ofensores e infratores utilizem a *Deep Web*, a internet profunda, existem meios para identificá-los. As investigações têm grande chance de êxito. Porém, espera-se que haja investimentos do poder público em aparatos de investigação que amparem o trabalho dos peritos (SUDRE, *et al*., 2020).

Ressalta-se, desse modo, importantes medidas legais que permitem tipificar, classificar e investigar crimes digitais, questões que tocam em pontos sensíveis sobre efeitos e consequências de ambientes virtuais. Profissionais e demais pesquisadores e técnicos da tecnologia da informação devem estar cientes de tais parâmetros, tendo em vista o exercício ético.

RESUMO DO PERCURSO DE APRENDIZAGEM

Tratamos, neste percurso, sobre transtornos de conduta e conflito no ciberespaço. Nosso principal objetivo foi o de categorizar os tipos de crimes informáticos, assim como identificar situações e posturas em conflito com a legislação, para inferência de soluções baseadas nos valores ético-legais.

No primeiro circuito, foi necessário contextualizar e apresentar políticas e legislação que são aplicadas ao ciberespaço, destacando questões de ampla discussão e debate, tais como a privacidade, a pirataria, as invasões e a propriedade intelectual.

Todos esses assuntos perpassam o contexto digital, desafiando usuários, fornecedores de serviços *on-line*, poder público e a sociedade geral no que se refere aos limites, possibilidades, direitos e deveres de pessoas que se utilizam de ambientes digitais.

Para falar nesses temas, situamos o papel e o principal objetivo da legislação que trata juridicamente essa questão, tais como a Lei “Carolina Dieckmann”, o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

Enquanto isso, no segundo circuito, continuamos a tratar do tema, explanando mais detalhadamente a definição dos crimes cibernéticos e seus impactos sociais e profissionais.

Compreender o que são e como são tratados os crimes digitais é de suma importância para o exercício profissional ético e responsável.

Um outro ponto a se considerar é o aspecto investigativo de crimes dessa natureza, que conta com mecanismos e instrumentos técnicos e legais para permitir a atuação de profissionais e peritos. O marco legal que esclarece a questão é o Marco Civil da Internet, como ressaltamos.

Reiteramos a relevância social e ética que cerca a compreensão da problemática em questão. O conhecimento desse cenário permeia a formação e a atuação de profissionais do campo das tecnologias de informação. Esperamos que você obtenha informações e conhecimentos necessários a esse respeito e que possa exercer seu papel social e técnico de forma consciente e responsável.

Referências

BARCARO, Edson; FREIRE, Edson. A importância da disciplina ética no curso de informática. **Fasci-Tech**: Periódico Eletrônico da FATEC São Caetano do Sul, São Caetano do Sul, v.1, n. 1, Ago./Dez. 2009, p. 17 a 28.

CÂMARA DOS DEPUTADOS. Brasília, 16 jun. 2021. **CREDN aprova adesão do Brasil à Convenção de Budapeste**. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/credn-aprova-adesao-do-brasil-a-convencao-de-budapeste. Acesso em: 18 set. 2021.

COMPUTER ETHICS INSTITUTE. **The ten commandments of computer ethics**. set. 2011. Disponível em: http://cpsr.org/issues/ethics/cei/. Acesso em: 30 ago. 2021.

KON, Fabio; *et al*. Direitos autorais, licenças e patentes. *In*: MACIEL, Cristiano e VITERBO, José. (orgs.). **Computação e sociedade**: a tecnologia. Cuiabá: EdUFMT, 2020.

LGPD BRASIL. São Paulo. 2021. Disponível em: https://www.lgpdbrasil.com.br/. Acesso em: 18 set. 2021.

MASIERO, Paulo Cesar. **Ética em computação**. São Paulo: EdUSP, 2004.

MOLITOR, Heloísa A. V.; VELAZQUEZ, Victor Hugo T. Breve panorama sobre a legislação aplicada nos crimes eletrônicos. **Rev. de Direito, Governança e Novas Tecnologias**, Jul/Dez. 2017, Maranhão, v. 3, n. 2, p. 81-96.

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

SANTORO, Flavia Maria; COSTA, Rosa Maria E. Moreira da. Ética profissional em computação. *In*: MACIEL, Cristiano; VITERBO, José. (orgs.). **Computação e sociedade**: a profissão. Cuiabá: EdUFMT, 2020. p. 194-220.

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO (SBC). **Código de ética do profissional de informática**. 15 jul. 2013. Disponível em: https://www.sbc.org.br/documentos-da-sbc/send/144-institucional/1360-codigo-de-etica-da-sbc. Acesso em: 30 ago. 2021.

SUDRE, *et al*. Crimes digitais. *In*: MACIEL, Cristiano; VITERBO, José. (orgs.). **Computação e sociedade**: a tecnologia. Cuiabá: EdUFMT, 2020.

UNIVERSIDADE DE FORTALEZA (UNIFOR)

Presidência
Lenise Queiroz Rocha

Vice-Presidência
Manoela Queiroz Bacelar

Reitoria
Fátima Maria Fernandes Veras

Vice-Reitoria de Ensino de Graduação e Pós-Graduação
Maria Clara Cavalcante Bugarim

Vice-Reitoria de Pesquisa
José Milton de Sousa Filho

Vice-Reitoria de Extensão
Randal Martins Pompeu

Vice-Reitoria de Administração
José Maria Gondim Felismino Júnior

Diretoria de Comunicação e Marketing
Ana Leopoldina M. Quezado V. Vale

Diretoria de Planejamento
Marcelo Nogueira Magalhães

Diretoria de Tecnologia
José Eurico de Vasconcelos Filho

Diretoria do Centro de Ciências da Comunicação e Gestão
Danielle Batista Coimbra

Diretoria do Centro de Ciências da Saúde
Lia Maria Brasil de Souza Barroso

Diretoria do Centro de Ciências Jurídicas
Katherinne de Macêdo Maciel Mihaliuc

Diretoria do Centro de Ciências Tecnológicas
Jackson Sávio de Vasconcelos Silva

AUTOR
ALINE MARIA MATOS ROCHA

Doutoranda e mestra em Sociologia pela Universidade Federal do Ceará (UFC); bacharel em Ciências Sociais e licenciada em Sociologia. Pesquisadora do Laboratório de Estudos da Cidade (Lec-UFC); professora do Centro de Ciências Tecnológicas da Universidade de Fortaleza (Unifor); e professora vinculada à Secretaria Estadual de Educação (Seduc-CE). Tem experiência em pesquisa, com ênfase em tecnologias e sociedade; cibercultura e ciberativismo; educação e tecnologias; movimentos sociais urbanos e ação coletiva.

RESPONSABILIDADE TÉCNICA

UNIVERSIDADE DE FORTALEZA ENSINANDO E APRENDENDO — VRE Vice-Reitoria de Ensino de Graduação e Pós-Graduação

Universidade de Fortaleza | EAD

COORDENAÇÃO DA EDUCAÇÃO A DISTÂNCIA

Coordenação Geral de EAD
Douglas Royer

Coordenação de Ensino e Recursos EAD
Andrea Chagas Alves de Almeida

Supervisão de Planejamento Educacional
Ana Flávia Beviláqua Melo

Supervisão de Recursos EAD
Francisco Weslley Lima

Supervisão de Operações e Atendimento
Mírian Cristina de Lima

Analista Educacional
Lara Meneses Saldanha Nepomuceno

Projeto Instrucional
Maria Mirislene Vasconcelos

Revisão Gramatical
Janaína de Mesquita Bezerra
José Ferreira Silva Bastos

Identidade Visual / Arte
Francisco Cristiano Lopes de Sousa

Editoração / Diagramação
Emanoel Alves Cavalcante
Rafael Oliveira de Souza
Régis da Silva Pereira

Produção de Áudio e Vídeo
José Moreira de Sousa
Pedro Henrique de Moura Mendes

Programação / Implementação
Márcio Gurgel Pinto Dias
Renan Alves Diniz