# Introdução



Caro estudante,

Nesta aula você conhecerá alguns aspectos do direito criminal derivado das relações cibernéticas.

Toda evolução tecnológica ao longo da história resulta em novas realidades, novos negócios jurídicos, novas atitudes e novas práticas realizadas pela sociedade.

Sob a ótica jurídica, conforme é verificado pela teoria tridimensional do direito (fato, valor e norma), novos fatos sociais em cada momento da história geram novos comportamentos sociais que podem ou não ser aceitos pela sociedade conforme valores reconhecidos naquele momento histórico e cultural. Com base nos valores reconhecidos pela sociedade haverá a incidência da norma, seja para aceitar novos fatos sociais ou para refutá-los.

É exatamente este movimento que verificamos em relação aos potenciais crimes cibernéticos. Se pensarmos em um ataque hacker, antes da internet tal delito somente era viável pelo ataque interno dentro de cada empresa, já que os computadores não eram interligados pela internet. Ou, ainda, práticas como o cyberbullying e o stalking somente passaram a existir a partir da popularização da internet, especialmente com sua disseminação por aplicativos e telefones celulares.

Essas práticas, por não serem aceitas socialmente, merecem a atenção do direito.

Vamos lá!

# Cenário cibernético: questões criminais



Você certamente já ouviu a história de alguma personalidade pública que teve fotografias íntimas divulgadas indevidamente na internet, seja por um aproveitador ou por alguém buscando difamar a personalidade pelos mais variados motivos.

Também há as situações de empresas e pessoas que sofreram ataques de hackers com invasão de sistemas e/ou ataques de ransomware com o sequestro de dados e informações de uma empresa, de um Estado ou de um órgão estatal.

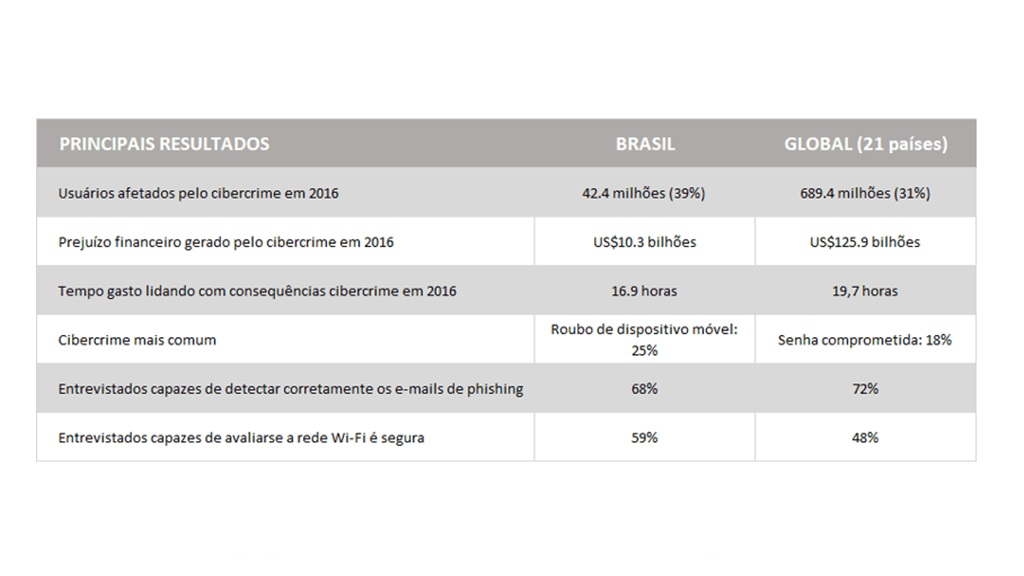
Estas práticas delitivas não eram reconhecidas pelo direito como fatos típicos penais, uma vez que a norma não tinha a previsão de algo que até então não existia no mundo fático.

Isso leva a uma necessidade de adaptação dos sistemas penais às novas realidades.

 O desenvolvimento da tecnologia é ágil, e a dependência da tecnologia pelas pessoas alcançou a sociedade moderna em diversas áreas. Consequentemente há pessoas mal-intencionadas, que exploram essa vulnerabilidade das ferramentas com malware, ransomware, spyware. “O tratado do conselho europeu sobre crime cibernético usa o termo “cibercrime” para definir delitos que vão desde atividades criminosas contra dados até infrações de conteúdo e de copyright” (KRONE, 2005).

De acordo com Canongia e Junior (2009), é marcante a presença da alta tecnologia atrelada a constantes inovações com o domínio das empresas de países desenvolvidos. Esta convergência tecnológica vem nos bombardeando com novidades inimagináveis, como o acesso à internet pelo celular, permitindo envio de e-mails e realização de transações financeiras, além de múltiplas aplicações, serviços e negócios que as TICs vêm proporcionando, e que são crescentes mundialmente.

Uma pesquisa da Norton Cyber Security Insights Repor apresenta alguns resultados realizando comparações referente ao impacto dos crimes virtuais do Brasil com outros 21 países:



Sob a ótica de crimes cibernéticos à pessoa, especialmente quanto à divulgação sem autorização de imagens íntimas, foi editada a Lei nº 12.737/2012 conhecida como Lei Carolina Dieckmann (BRASIL, 2012, [s. d.]):

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Ação penal – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Antes do ano de 2012, sem uma legislação específica era mais difícil apurar e punir os chamados crimes cibernéticos em relação à divulgação de imagens e informações íntimas de pessoas, assim como a identificação dos sujeitos e dos meios de obter as provas para a condenação. Nesse sentido, para Silveira (2015) é importante destacar o Art. 154-A do Código Penal, que trouxe para o ordenamento jurídico o crime de “Invasão de Dispositivo Informático”, consistente na conduta de

[…] invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (SILVEIRA, 2015, [s. p.]).

 A pena prevista para o crime simples é de detenção de três meses a um ano e multa, havendo, entretanto, a previsão das formas qualificadas e causas de aumento de pena.

# Delitos: crimes praticados por meio eletrônico, a criança e o adolescente no meio digital – Cyberbullying e Stalking



Sob a ótica da criança e do adolescente, desde a promulgação da Constituição Federal de 1988 e posteriormente do Estatuto da Criança e do Adolescente, todo o sistema legal passou a tratar com mais cautela das relações jurídicas que envolvam tais pessoas (crianças e adolescentes), considerados presumivelmente vulneráveis.

Diante de tal realidade, toda a matéria que trata de práticas comerciais e publicitárias em qualquer veículo de comunicação – incluindo a internet – não pode resultar em práticas abusivas e/ou ofensivas à criança e ao adolescente, resultando em responsabilidade civil, administrativa e criminal de seus infratores. Neste sentido não vemos qualquer dificuldade em investigar e punir criminalmente quem realizar tais práticas comerciais abusivas.

No mesmo sentido são os crimes contra o direito de personalidade, intimidade e sexualidade de uma criança e/ou adolescente, os quais encontram a respectiva previsão no Estatuto da Criança e do Adolescente (ECA, Lei nº 8.069/1990), em seus artigos 240 e 241-E, os quais preveem, entre outros, crime de produção de pornografia infantil; crime de venda de pornografia infantil; crime de divulgação de pornografia infantil; crime de posse de pornografia infantil; crime de montagem de pornografia infantil; e crime de aliciamento de criança, entre outros.

O bullying é uma forma de agressão física, verbal e psicológica de forma contínua, com ataques a um indivíduo com base em sua aparência ou comportamento. O cyberbullying é a extensão da prática ao plano virtual.

Ações que são consideradas cyberbullying são:

* Exposição de fotografias ou montagens constrangedoras.
* Divulgação de fotografias íntimas.
* Críticas à aparência física, à opinião e ao comportamento social de indivíduos repetitivamente.

Temos no cyberbullying alguns conceitos para nomear determinadas práticas:

* Hater: seria aquele que odeia, pessoas que atacam com ofensas.
* Sexting: consiste na prática de trocar mensagens de cunho sexual.
* Revenge porn: de acordo com sua expressão – vingança pornográfica –, é o ato de divulgar imagens eróticas e de nudez de outra pessoa, como forma de vingança e punição.

**Cyberbullying e a lei**

A prática é passível de punição por meio do Código Penal, veja alguns exemplos:

* Artigo 140, §3º do Código Penal Brasileiro: crime de injúria racial.
* Artigo 216-B do Código Penal Brasileiro: exposição de imagens de conteúdo íntimo, erótico ou sexual.
* Artigo 218-C do Código Penal Brasileiro incluído pela Lei nº 13.718, de 2018: crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia.

Pesquisa conduzida pela Intel Security entrevistou 507 crianças e adolescentes com idades que variam entre 8 e 16 anos e revelou os seguintes dados sobre o cyberbullying no Brasil (CANALTECH, 2015, [s. p.]):

* 66% dos entrevistados presenciaram casos de agressão na internet;
* 21% afirmam ter sofrido cyberbullying;
* 24% realizaram atividades consideradas cyberbullying. Desse grupo:
* 14% admitiram falar mal de uma pessoa para outra;
* 13% afirmaram zombar de alguém por sua aparência;
* 7% marcaram alguém em fotos vexatórias;
* 3% ameaçaram alguém;
* 3% alguém de por conta de sua sexualidade;
* 2% postaram intencionalmente eventos em que um colega foi excluído para ele ver que foi excluído.

Stalking é um termo que significa perseguição obsessiva ou incessante, e tornou-se crime pela Lei nº 14.132/21, de 31 de março de 2021.

A deputada Sheridan (PSDB/RR) destaca que esse delito causa inúmeros transtornos à vítima, que passa a ter a vida controlada pelo delinquente, vivendo com medo de todas as pessoas em todos os lugares que frequenta, o que caracteriza um verdadeiro tormento psicológico.1

As atitudes de um stalker podem envolver, ligações telefônicas, mensagens, e-mails, comentários nas redes sociais, além de frequentar os mesmos lugares que a vítima frequenta. O crime é caracterizado pelo fato de ser repetitivo, obsessivo e intimidador.

\_\_\_\_\_\_\_

1 Câmara Federal. **Notícias**. Disponível em: [Câmara aprova criminalização da perseguição obsessiva ou stalking Fonte: Agência Câmara de Notícias](https://www.camara.leg.br/noticias/714712-CAMARA-APROVA-CRIMINALIZACAO-DA-PERSEGUICAO-OBSESSIVA-OU-STALKING). Acesso em 09.dez.2022

# Cenário cibernético: Riscos e fraudes, perícia computacional e metodologia para obtenção de evidências, provas eletrônicas e tipificação existente



A internet como meio de comunicação resultou na massificação de dados, conexões e acessos aos computadores, aparelhos celulares e todos os tipos de potenciais delitos cibernéticos em uma escala sem precedentes da história. Tais fatores elevam consideravelmente a gestão de risco cibernético, e as empresas devem praticar programas estruturados e eficientes de segurança da informação (SI), controle de processos, treinamento de pessoas e testes contínuos e repetitivos. Mesmo assim, os desafios são grandes e o direito ainda precisa se adaptar a inúmeras realidades sociais advindas da internet.

De acordo com Silva (2003), o aparecimento da informática no meio social ocorreu de forma rápida, e passou a exigir, com a mesma rapidez, soluções que o direito não estava preparado para oferecer. Com isso, a necessidade social aparenta estar desprovida da tutela de direito.

Em 2021, no Brasil, o estudo Device Fraud Scan 2022 da AllowMe constatou que ao menos 500 mil contas falsas foram criadas com e-mails vazados. Ou seja, uma média de 3,7 tentativas de fraude virtual por minuto e cerca de 63,7% dos casos frequentes de vazamento de dados acontecem no momento em que o usuário realiza o login.

Segundo o conceito de Maurício Tamer (RODRIGUES; TAMER, 2021, p. 291), “pode ser entendida como a demonstração de um fato ocorrido nos meios digitais” e que “a demonstração de sua ocorrência pode se dar por meios digitais”.2 Como exemplo de provas digitais podemos citar o “envio de um e-mail, envio de uma mensagem por aplicativo de mensagens (WhatsApp, Telegram, entre outros), cópia ou desvio de base de dados, cópia de software, disponibilização de um vídeo na internet (conteúdo íntimo ou difamador), dentre outros”.

A prova digital tem capacidade de verificar a veracidade das provas através da chave ICP Brasil, em que há uma cadeia de custódia de prova que está prevista no Art. 158-A do Código de Processo Penal1:

Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

Os dados em um celular muitas vezes se tornam uma fonte valiosa de provas, contando com as características de memória, processador e câmera, entre outras. A aquisição de dados pode ser física ou lógica. Conforme descrevem Jansen e Aures (2015), a aquisição física tem vantagens sobre a aquisição lógica, uma vez que permite que os arquivos apagados e alguns dados restantes possam ser examinados, por exemplo, na memória não alocada ou em espaço do sistema de arquivos. As ferramentas forenses adquirem informações dos dispositivos sem alterar o conteúdo, ou seja, em modo somente de leitura, utilizando equipamentos denominados Write Blocker (ou bloqueadores de escrita). E, ainda, fazendo a geração de hash de modo a garantir a integridade dos dados coletados. Tal característica é muito importante perante um juiz, e cabe ao perito garantir a integridade das provas digitais por ele coletadas ou a ele confiadas.

Segundo ISFS (2009), o objetivo de ter um conjunto de melhores práticas e metodologias é estabelecer parâmetros e princípios de qualidade e abordagens para obtenção, identificação, preservação, recuperação, exame, análise e uso das evidências digitais. Altos padrões de qualidade e consistência são vitais para manter o valor probatório dos elementos encontrados em uma investigação digital.

\_\_\_\_\_\_\_

1 PEREIRA Ezequiel Alves. **Ata Notarial versus provas digitais como meio de prova em processo judicial**. Disponível em: [Ata notarial versus provas digitais como meio de prova em processo judicial](https://jus.com.br/artigos/92603/ata-notarial-versus-provas-digitais-como-meio-de-prova-em-processo-judicial). Acesso em 23.nov.2022

2 Brasil. [Decreto-Lei nº 3.689 de 03 de outubro de 1941](https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm) e alterações. Dispõe sobre o Código de Processo Penal.

# Videoaula: Cenário Penal Cibernético

Caro estudante, nesta aula você terá a oportunidade de conhecer melhor as relações jurídicas que podem resultar na prática de atos criminosos e suas consequências.

Para tanto, você compreenderá a evolução do direito neste aspecto, bem como as dificuldades de adequação da norma, a qual normalmente é derivada de atos praticados pela sociedade os quais são entendidos como não aceitos, portanto, ilícitos civis, administrativos e penais.

A disseminação de redes sociais, o acesso à internet por crianças e adolescentes e a prática de atos de abuso psicológico como o bullying passaram a ser preocupação do direito penal, já que cada dia se tornam mais frequentes, sendo necessária uma ação do Estado para coibir tais práticas.

Aproveite!

# Saiba mais



Com o objetivo de aprofundar na temática das provas e respectivas medida cautelares em relação aos crimes cibernéticos, indicamos a leitura e estudo do seguinte artigo disponível na base eletrônica da RT Online acessível pela Biblioteca Digital:

FULLER; G. P.; PEDROSA, J. M. B. F. Medidas cautelares e meios de prova nos crimes cibernéticos. **Revista dos Tribunais**, v. 1031, p. 207- 224, set. 2021, DTR\2021\45755. Disponível em Revista dos Tribunais Online.

No artigo em análise, você verá os desafios da produção da prova em face dos crimes cibernéticos, bem como conhecerá as medidas cautelares que nosso sistema prevê, viabilizando a proteção da integridade das provas e eventual condenação dos criminosos de práticas cibernéticas ilícitas.

# Referências



BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília/DF: Presidência da República, 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 23 nov. 2022.

Brasil. **Decreto-Lei nº 3.689 de 03 de outubro de 1941** e alterações. Dispõe sobre o Código de Processo Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em 09.dez.2022

CÂMARA DOS DEPUTADOS. **Perseguição obsessiva é crime**. Plenarinho, 15 abr. 2021. Disponível em: <https://plenarinho.leg.br/index.php/2021/04/perseguicao-obsessiva-e-crime/>. Acesso em: 23 nov. 2022.

Câmara Federal. Notícias. Disponível em: <https://www.camara.leg.br/noticias/714712-CAMARA-APROVA-CRIMINALIZACAO-DA-PERSEGUICAO-OBSESSIVA-OU-STALKING>. Acesso em 09.dez.2022

CANONGIA, C.; JUNIOR, R. M. Segurança cibernética: o desafio da nova Sociedade da Informação. **Revista Parcerias Estratégicas do**Centro de Gestão e Estudos Estratégicos (CGEE), v. 14, n. 29, p. 21-46, dez. 2009. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 23 nov. 2022.

Cyber Security Insigths Report Brasil (2016). Disponível em: <https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais>. Acesso em 09.dez.2022

FULLER; G. P.; PEDROSA, J. M. B. F. Medidas cautelares e meios de prova nos crimes cibernéticos. **Revista dos Tribunais**, v. 1031, p. 207- 224, set. 2021, DTR\2021\45755.

ISFS. **Computer Forensics**. Part 2: Best Practices. Information Security and Forensics Society, ago. 2009.

JANSEN, W.; AYERS, R. Computer Security – guidelines on cell phone **forensics**. National Institute of Standards and Technology – NIST, Special Publication, 800-101, maio 2007, 104 p. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>. Acesso em: 26 fev. 2015.

PEREIRA, E. A. **Ata notarial versus provas digitais como meio de prova em processo judicial**. Jus.com.br, 29 ago. 2021. Disponível em: <https://jus.com.br/artigos/92603/ata-notarial-versus-provas-digitais-como-meio-de-prova-em-processo-judicial>. Acesso em: 23 nov. 2022.

PORFÍRIO, F. **Cyberbullying**. Brasil Escola, [s. d.]. Disponível em:  <https://brasilescola.uol.com.br/sociologia/cyberbullying.htm>. Acesso em: 23 nov. 2022.

RODRIGUES, M. A.; TAMER, M. **Justiça digital:** o acesso digital à justiça e as tecnologias da informação na resolução de conflitos. São Paulo: Jus Podivm, 2021.

SILVA, H. B. **Perícia forense computacional em dispositivos móveis**. 2015. 80 f. Trabalho de Conclusão de Curso. Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, Instituto Municipal de Ensino Superior de Assis, SP. Disponível em:  <https://cepein.femanet.com.br/BDigital/arqTccs/1211321025.pdf>. Acesso em: 23 nov. 2022.

SILVA, R. L. **Segurança cibernética:** o cenário dos crimes virtuais no Brasil. Núcleo do Conhecimento, 20 abr. 2021. Disponível em: <https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais>. Acesso em: 23 nov. 2022.

SILVEIRA, A. B. **Os crimes cibernéticos e a Lei nº 12.737/2012 (“Lei Carolina Dieckmann”)**. Jus.com.br, 25 jan. 2015. Disponível em: <https://jus.com.br/artigos/35796/os-crimes-ciberneticos-e-a-lei-n-12-737-2012-lei-carolina-dieckmann>. Acesso em: 23 nov. 2022.

TD SYNNEX CORPORATION. Fraudes na nuvem: quais são os principais riscos e como enfrentá-los? TD Synnex, [s. d.]. Disponível em: <https://digital.br.synnex.com/fraudes-na-nuvem-quais-sao-os-principais-riscos-e-como-enfrenta-los#:~:text=O%20vazamento%20de%20dados%2C%20classificado,criadas%20com%20e-mails%20vazados>. Acesso em: 23 nov. 2022.