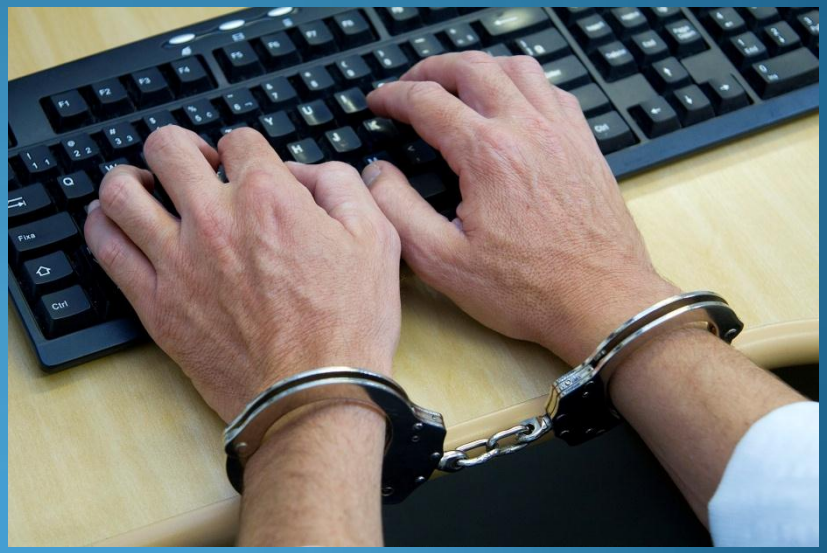
“Crimes Cibernéticos”, “Crimes Digitais”, “Crimes Informáticos”, “Crimes Eletrônicos”,



- **A consciência digital, independente da idade, é o caminho mais seguro para o bom uso da internet, sujeita às mesmas regras de ética, educação e respeito ao próximo**

- *“Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionavam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade”.*

- O criminoso informático pode cometer mais de uma conduta lesiva ao mesmo tempo, estando em diversos lugares simultaneamente, e conta com a vantagem de haver poucos profissionais de segurança pública capacitados para investigar sua ação, analisar as provas e os indícios. Sem contar a vantagem de o agente não fazer qualquer esforço e agir de forma transnacional com facilidade ímpar.

- “Crimes Cibernéticos”, “Crimes Digitais”, “Crimes Informáticos”, “Crimes Eletrônicos”, são termos para definir os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral), importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, *bullying*, terrorismo, entre outros.

- No Brasil, os ataques a computadores brasileiros quase triplicaram em 2011 em relação ao ano anterior. No ano de 2012 foram 399.515 registros de problemas com vírus, códigos maliciosos ou tentativas de fraude, enquanto em 2010 eram 142.844.

- Crimes semelhantes já estavam ocorrendo havia anos – e continuam ocorrendo - com pessoas comuns, causando prejuízos inimagináveis para os envolvidos. No caso de Carolina Dieckmann, ela teria mandado consertar um computador e não protegeu o que havia arquivado nele.

São vários tipos de infrações cometidas pela internet, entre elas estão:

- FALSIFICAÇÃO DE DADOS,
- ESTELIONATOS ELETRÔNICOS,
- PORNOGRAFIA INFANTIL (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito),
- RACISMO E XENOFOBIA (difusão de imagens, idéias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica, injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade).

- O *sexting* é resultado da união de duas palavras em inglês: *sex* (sexo) e *texting* (envio de mensagens). Por definição, o *sexting* seria a prática em que adolescente usam seus celulares, câmeras fotográficas, e-mail, chats, mensagens instantâneas e redes sociais para produzir e enviar fotos sensuais de seu corpo nu ou em trajes íntimos. Também se enquadram neste conceito os textos eróticos (em dispositivos móveis ou internet) com convites e insinuações sexuais para namorado (a), pretendentes ou amigos (as).
- *Sexting* não consiste em crime em si, mas certamente é uma grande porta que os usuários da internet deixam aberta para que criminosos possam agir de imediato ou mais tarde.

- Uma vez produzidas e divulgadas, as mensagens e imagens não estão mais no controle de quem as produziu ou divulgou. Elas ganharão eternidade na rede e cedo ou tarde vão aparecer novamente.
- A “falsa idéia” de achar que o arquivamento eletrônico é seguro é onde está o grande problema. Nada é seguro em se tratando de redes que se comunicam continuamente, porque a própria dinâmica de comunicação pela *web* exige certo grau de exposição pública.
- Mesmo os dados que não são públicos ficam de certa maneira “disponíveis” para quem estiver mal intencionado. Da mesma forma que se rouba um objeto material, informações preciosas podem ser roubadas – basta que essas informações estejam digitalizadas em alguma máquina ou dispositivo eletrônico.

- Outro fator importantíssimo e comumente utilizado é o celular. Ele é utilizado para fazer fotos e filmes que acabam ficando esquecidos, até o dia em que o aparelho é extraviado, roubado ou vai parar em mãos erradas.
- O ciúme também é um dos motores da pornografia na *internet*. Namorados (as), companheiros (as), maridos, esposas e amigos podem ser movidos pela vingança no final de um relacionamento.

- Quadrilhas procuram sinais de ostentação na web. Golpistas, entre eles chantagistas e ladrões, necessitam de informações para cometer seus crimes.

- Antigamente, os criminosos se valiam de informantes que atuavam muito próximo a suas futuras vítimas: amigos, colegas de trabalho, empregados, etc. Quando não podiam contar com informantes, os criminosos partiam para um longo processo de observação dos hábitos da vítima.

- Esses métodos não foram abandonados nos dias de hoje, mas, com a internet, a partir da difusão do uso de redes sociais, esse trabalho de obtenção de informações foi facilitado.

- Rede mundial de computadores mostra-se um cenário em que os usuários em potenciais vítimas, são, em diversos casos, os condutores de seu próprio rumo e destinos virtuais.
- Não são somente as crianças e os adolescentes que estão sujeitos a serem vítimas de crimes na *internet*; adultos incautos também estão.
- O caráter subsidiário do Direito Penal deve ser sempre buscado, especialmente com medidas preventivas de inclusão digital, educando e conscientizando as pessoas quanto ao uso racional dos meios informáticos.

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.

- **A PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

- Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

- Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

Invasão de dispositivo informático

- 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:
- Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

- Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
- § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
- § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
- Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
- § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

- § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
- I - Presidente da República, governadores e prefeitos;
- II - Presidente do Supremo Tribunal Federal;
- III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
- IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

- “**Ação penal**
- Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”

- Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
- **“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
- Art. 266. .....
- § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
- § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
- **“Falsificação de documento particular**
- Art. 298.

- **Falsificação de cartão**
- Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)
- Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

- Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.