

**FACULDADE DE TECNOLOGIA SENAC GOIÁS**  
**Tecnologia em Segurança da Informação**



Aldo Filho  
Jordan Hugs  
Liniker Lettierre  
Rony Carneiro

**LEGISLAÇÃO APLICÁVEL A CRIMES  
CIBERNÉTICOS.**

Marcelo Almeida Gonzaga

GOIÂNIA,  
2016

Aldo Filho  
Jordan Hugs  
Liniker Lettierre  
Rony Carneiro

# **LEGISLAÇÃO APLICÁVEL A CRIMES CIBERNÉTICOS.**

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina de Noções de Direito e Legislação em Informática, no Curso de Tecnologia em Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Marcelo Almeida Gonzaga

GOIÂNIA,  
2016

## **SUMÁRIO**

<b>1</b>	<b>O QUE É CRIME VIRTUAL.....</b>	<b>4</b>
<b>2</b>	<b>ONDE OCORRE OS CRIMES MAIS COMUNS.....</b>	<b>4</b>
<b>3</b>	<b>OS CRIMES MAIS COMUNS E EM QUAIS LEIS ELES SÃO ABORDADOS .....</b>	<b>5</b>
<b>4</b>	<b>REFERÊNCIAS BIBLIOGRÁFICAS .....</b>	<b>10</b>

## **1 O QUE É CRIME VIRTUAL**

Os Crimes Digitais, conhecidos como Crimes Cibernéticos ou Crimes de Alta Tecnologia, representam as condutas criminosas cometidas com o uso das tecnologias de informação e comunicação, e também os crimes nos quais o objeto da ação criminosa é o próprio sistema informático.

Os crimes são previstos pelo Código Penal, mas que, quando cometidos por meio da Internet causam danos muito maiores.

Em contraposição, com o surgimento dos computadores e das redes, surgiram os crimes específicos desse meio, como a difusão de vírus de computadores e o acesso a sistemas informáticos sem autorização.

Esse tipo de delito pode ser cometido através das fronteiras nacionais, e ainda são de difícil identificação dos autores. Assim, o combate aos crimes digitais demanda alterações nas legislações penais e acordos internacionais, a fim de dotar as autoridades policiais e judiciais de instrumentos adequados à velocidade e complexidade técnica dos crimes de alta tecnologia.

Os infratores estão sujeitos a penas previstas em Lei e devem ser denunciados.

## **2 ONDE OCORRE OS CRIMES MAIS COMUNS**

Aplicativos maliciosos: Com a consagração dos smartphones, vários aplicativos são desenvolvidos especialmente para o roubo de dados em celulares;

Lojas virtuais falsas: As compras realizadas através da internet estão cada vez maiores, em virtude disso, muitos criminosos do ramo acabam criando ofertas falsas, com preços tentadores de produtos que costumam ser o sonho de consumo de muita gente;

Hotéis: Grande parte das pessoas que viajam costuma fazer as reservas de hotéis de forma online. Sabendo disso, os criminosos se aproveitam da situação para enviar e-mails falsos para os usuários solicitando que seja preenchido um formulário, assim, os criminosos conseguem várias informações sobre os usuários, incluindo dados bancários.

Redes Públicas: A forma mais comum de se conseguir dados de usuários desavisados é criar uma rede Wi-Fi falsa com um servidor de nomes (DNS). Ao se conectar nesses servidores e acessar um site importante (e-mail, redes sociais e transações financeiras), o DNS “engana” o computador fazendo com que ele acesse uma página clonada para que o usuário deposite suas informações em um banco de dados particular.

### 3 OS CRIMES MAIS COMUNS E EM QUAIS LEIS ELES SÃO ABORDADOS

**Cyberbullying:** Assédio virtual, ou cyberbullying, é uma prática que envolve o uso de tecnologias de informação e comunicação para dar apoio a comportamentos deliberados, repetidos e hostis praticados por um indivíduo ou grupo com a intenção de prejudicar o outro.

LEI Nº 13.185, Art. 3º – DE 6 DE NOVEMBRO DE 2015.

Essa lei se enquadra ao crime de cyberbullying pois deixa explícito no 3º Artigo, inciso VIII, que qualquer modo de utilização de tecnologias de informações para práticas de perturbação, aborrecimento, intimidação ou constrangimento de indivíduos estão proibidas.

Art.3 – VIII - Virtual: depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social.

**Phishing:** uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais.

LEI Nº 12.965, Art. 3º, 7º, 8º e 9º, DE 23 DE ABRIL DE 2014. (Marco civil) e LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012 (Carolina Dieckmann).

Essas leis se enquadra no caso de phishing( quando informações particulares ou sigilosas são capturadas por outrem) por infringir a inviolabilidade da intimidade e da vida privada, inviolabilidade e sigilo de suas comunicações privadas armazenadas e pela internet, agir sem proporcionalidade, transparência, Invadir dispositivo informático alheio a 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.

**Engenharia Social:** A engenharia social, no contexto de segurança da informação, refere-se a manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

A engenharia social faz com que a vítima forneça credenciais de acesso ou mesmo acesse voluntariamente determinado programa que libera o acesso a seu dispositivo, fica eliminada, em tese, a incidência do delito em comento, podendo o agente, diante do caso concreto, responder por outros delitos do Código Penal, de acordo com a extensão do dano.

**Sniffing:** Interceptação de tráfego, ou sniffing, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de Sniffers.

LEI Nº 12.965, Art. 7º e 8º, DE 23 DE ABRIL DE 2014.

Esse ataque se enquadra pois vai contra a inviolabilidade e sigilo de fluxo de suas comunicações pela internet e comunicações privadas armazenadas, já que o ataque intercepta tráfego na rede, podendo espionar dados privados e confidenciais.

**SQL Injection (SQLi):** Quando existe uma falha de segurança no banco de dados, os hackers podem injetar um código (query) via aplicação web, obtendo acesso às informações confidenciais da organização, como senhas, logins, número de cartões de crédito dos clientes, entre outros.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Se enquadra pois vai contra a inviolabilidade e sigilo de suas comunicações privadas armazenadas, uma vez que o SQL injection usa de injeção de códigos na aplicação web para obter dados sigilosos em banco de dados, inclusive podendo capturar senhas de acesso a dispositivos e sistemas.

**Pirataria:** A pirataria de software refere-se a práticas que envolvem cópias de software não autorizadas.

LEI Nº 9.609, Art. 5º, DE 19 DE FEVEREIRO DE 1998 e a LEI Nº 10.695, DE 1º DE JULHO DE 2003, LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998.

A pirataria se enquadra em várias leis, como na Lei nº 9.609, que aborda mais a cópia não autorizada para fins lucrativos no que se refere a computadores, como programas e softwares, conforme Art. 5º: Os direitos sobre as derivações autorizadas pelo titular dos direitos de programa de computador, inclusive sua exploração econômica, pertencerão à pessoa autorizada que as fizer, salvo estipulação contratual em contrário. Aborda também uma lei mais geral em relação a pirataria, que se encontra logo no Art.1º, da LEI

Nº10.695, onde a violação consiste em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, e na Lei nº 9.610, que aborda os direitos autorais, que são simplesmente ignorados pela prática da pirataria.

**Cross Site Scripting (XSS):** Os hackers clonam uma página da loja para redirecionar o usuário a sites que contenham conteúdos maliciosos, para infectar seu dispositivo e obter acessos aos seus dados.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Afeta a proteção dos dados pessoais, pois o ataque consiste em usar códigos em sites para que o usuário possa ser redirecionado a conteúdos maliciosos e expor dados de natureza privada.

**Espionagem industrial:** Transferência de informações sigilosas de uma empresa para o concorrente.

Lei 9.279/1996.

Se enquadra na Lei da Propriedade Industrial, que protege segredos industriais, impedindo concorrência desleal o seu uso desautorizado. A legislação impede o uso de dados de natureza confidencial que tenham sido obtidos durante relação contratual ou empregatícia, ou que tenham sido obtidos de forma ilícita ou fraudulenta, de acordo com o artigo 195, incisos XI e XII.

**Brute Force:** Um ataque de força bruta, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014 e LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Se enquadra a esse tipo de ataque pois ele pode, por tentativa e erro, adquirir senha de sites, computadores, serviços, informações confidenciais e privilégios do usuário, descumprindo a Lei nº 12.737, no requisito de invasão de dispositivo informático e contra a inviolabilidade da privacidade e da vida privada, além da qualidade e neutralidade de serviços.

**Botnet / Storm Worm:** O chamado Botnet é muito difícil de ser detectado e também analisado, pois ele se reconfigura rapidamente e pode ser transmitido através de links que apontam para endereços IP de sites infectados.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Se enquadra a esse tipo de ataque, pois se baseia em enviar um trojan malicioso que toma conta do controle das máquinas infectadas, indo contra a lei contra a invasão de dispositivos informáticos, proteção dos dados pessoais, preservação e garantia da neutralidade de rede, preservação da estabilidade, segurança e funcionalidade da rede, além de ser usado muitas vezes para envio de spans, sem conhecimento dos usuários autênticos das máquinas.

**Spyware:** Spyware (aplicativo ou programa espião) consiste num programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014 e LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Se enquadra no caso pois o spyware agride gravemente os requisitos de proteção de privacidade e de dados pessoais e secretos, além da invasão de dispositivo alheio por um software que recolhe dados sem consentimento algum da vítima.

**Spam:** O termo Spam, é uma mensagem eletrônica não-solicitada enviada em massa. Na sua forma mais popular, um spam consiste numa mensagem de correio eletrônico com fins publicitários.

Não há Lei concreta contra o envio de Spams, Tem alguns projetos de deputados mas nada que tenha sido aprovado, como o Projeto de Lei 2186 de 2003, onde é considerado spam qualquer mensagem eletrônica recebida por rede de computadores de uso público, inclusive a Internet, sem consentimento prévio do destinatário, mas na própria legislação existem “brechas” para enquadrarmos algumas situações do mundo real com o que se ocorre no mundo virtual, no caso, os Spams.

Os Spams são tipos de mensagens desagradáveis que importunam o usuário e podem, inclusive, causar danos a seu computador, que é patrimônio material. Eles ferem os



princípios constitucionais da intimidade e da privacidade, especificados, no artigo 5º, X e XII:

X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

**Worm:** Um Worm, na área da informática, é semelhante a um vírus, porém com um diferencial, é um programa autorreplicaste.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014 e LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Se enquadra nesse caso pois o ataque pode visar comprometer ou alterar um dispositivo ou rede, contrariando a preservação da estabilidade, segurança e funcionalidade da rede, a proteção da privacidade e a proteção dos dados pessoais.

**Spoofing attack:** um ataque spoofing é uma situação em que uma pessoa ou programa disfarça com sucesso como uma outra por falsificação de dados, ganhando assim uma vantagem ilegítima.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Se enquadra neste tipo de ataque pois se trata de uma técnica de falsificar um tipo de serviço, se passando por ele e transmitindo informações não íntegras ao serviço, podendo causar uma negação de serviço em sua Execução, além de obter informações da rede e dos usuários das máquinas conectadas, indo contra a Lei da proteção da privacidade, proteção dos dados pessoais, preservação, garantia da neutralidade de rede e autenticidade da rede, e preservação da estabilidade, segurança e funcionalidade da rede.

## **4 REFERÊNCIAS BIBLIOGRÁFICAS**

L9610

[http://www.planalto.gov.br/ccivil\\_03/leis/L9610.htm](http://www.planalto.gov.br/ccivil_03/leis/L9610.htm)

Acesso em 16 de junho de 2016

L12737

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm)

Acesso em 16 de junho de 2016

L12965

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm)

Acesso em 16 de junho de 2016

L9609

[http://www.planalto.gov.br/ccivil\\_03/leis/L9609.htm](http://www.planalto.gov.br/ccivil_03/leis/L9609.htm)

Acesso em 16 de junho de 2016

L10695

[http://www.planalto.gov.br/ccivil\\_03/Leis/2003/L10.695.htm](http://www.planalto.gov.br/ccivil_03/Leis/2003/L10.695.htm)

Acesso em 16 de junho de 2016

A nova arma no combate à pirataria - a Lei Nº 10.695, de 2.7.2003 - Migalhas de Peso

<http://www.migalhas.com.br/dePeso/16,MI2275,21048->

[A+nova+arma+no+combate+a+pirataria+a+Lei+N+10695+de+272003](http://www.migalhas.com.br/dePeso/16,MI2275,21048-A+nova+arma+no+combate+a+pirataria+a+Lei+N+10695+de+272003)

Acesso em 16 de junho de 2016

Será que SPAM é Crime no Brasil | Diego Brito - Publicitário, Palestrante e Professor

<http://diegobrito.com.br/sera-que-spam-e-crime-no-brasil/>

Acesso em 16 de junho de 2016

ConJur - Medidas preventivas podem garantir proteção de segredos industriais

<http://www.conjur.com.br/2014-out-21/medidas-preventivas-podem-garantir-protecao-segredos-industriais>

Acesso em 16 de junho de 2016