# **Segurança da Informação: Ataques Cibernéticos e Cibersegurança**

## Crimes e ataques cibernéticos

Com o crescente uso das novas tecnologias foi alterada a forma como muitos crimes são cometidos. A maioria dos crimes que acontecem no mundo virtual também ocorrem no mundo real. A Internet em muitos casos facilita a ocorrência de tais crimes, que em diversos casos estão relacionados com a invasão de sistemas, com programas maliciosos como os cavalos de tróia, com a perda de dados e a exposição de informações sigilosas.

Dessa forma, em razão do mundo cada vez mais globalizado e interligado por uma rede de computadores, torna-se essencial a preocupação com a segurança de dados e de informações. Frequentemente são noticiados casos de redes invadidas por hackers e de vazamentos de dados e de informações.

As organizações devem buscar mecanismos de proteção contra ataques cibernéticos, uma vez que podem ser violadas informações confidenciais das empresas, bem como, dados sensíveis de seus funcionários e de clientes.

Conforme indicado, a Internet em muitos casos é tida como um facilitador na ocorrência de crimes, principalmente pelo “anonimato” que proporciona. Pode-se dizer que o anonimato indicado é relativo, já que o ID constitui um identificador virtual, embora muitas identidades virtuais possam não ter correspondência com a identidade real.

Segundo a Advogada Patrícia Peck Pinheiro (2016) as questões relacionadas ao conceito de crime, de delito, de ato e de efeito são as mesmas aplicadas tanto pelo Direito Penal quanto pelo Direito Penal Digital. As inovações trazidas no aspecto digital se relacionam com a territorialidade e a investigação probatória, assim como a necessidade de tipificação penal de algumas modalidades, em virtude de suas peculiaridades.

Em 30 de novembro de 2012 foi promulgada a Lei nº 12.737 - Lei de Crimes Cibernéticos, conhecida como a Lei Carolina Dieckmann, que prevê como crimes cibernéticos a “invasão de dispositivo informático” - artigo 154 - A, a “interrupção ou perturbação de serviços telegráfico, telefônico, telemático ou de informação de utilidade pública” - artigo 266 - e “falsificação de documento particular - artigo 298”. Os crimes eletrônicos ou cibernéticos possuem modalidades distintas de acordo com o bem jurídico tutelado.

LEIA TAMBÉM:

* Aplicabilidade e Inaplicabilidade da LGPD
* Aspectos sobre a Lei nº 13.709 de 2018 - LGPD
* Repercussões sobre o Regulamento Geral de Proteção de Dados – GDPR
* Tecnologias de Informação e Comunicação e a Lei Geral de Proteção de Dados

Alguns criminosos clonam sites com o objetivo de roubar dados dos usuários como RG, CPF, dados bancários, residência e telefone. Os dados roubados podem ser utilizados para realizar operações comerciais.

Com a pandemia do novo coronavírus aumentaram os casos de crimes e ataques cibernéticos e de golpes de diferentes tipos. A utilização do trabalho remoto, o uso de redes por pessoas sem o devido treinamento e a ausência de cibersegurança têm facilitado a ocorrência dos crimes citados.

## Segurança da Informação e Cibersegurança

Preliminarmente, pode-se dizer que o conceito de Segurança da Informação é mais amplo do que o de Cibersegurança. A Segurança da Informação objetiva proteger tanto as informações nos arquivos físicos quanto nos digitais. A Cibersegurança pretende proteger as informações que estão nos arquivos digitais.

A Segurança da Informação pauta-se em objetivos como a confidencialidade - a informação será acessada apenas por quem for autorizado; a integridade - evitar que os dados sejam adulterados e a disponibilidade - as informações devem estar disponíveis para acesso.

Para que seja elaborada uma política de segurança da informação efetiva, a empresa deve atentar-se para disposições presentes nas ISO / IEC 27001: 2013 e ISO / IEC 27002.

Segundo Marcelo Gaspar e Viviane Fiedler (2020) a empresa pode utilizar antivírus para proteger os computadores contra infecção de arquivos que pode se propagar pela rede; antispyware para impedir que sejam instalados programas sem autorização; backup ou cópia de segurança de dados armazenados; criptografia - para o sigilo de informações -, Data Loss Protection - DLP - para proteção contra perda de dados, Firewall - aplicativo ou computador que controla o acesso à rede e monitora o tráfego de informações, entre outros.

## Lei Geral de Proteção de Dados

Com o intuito de resguardar os indivíduos de terem seus dados tratados expostos sem a sua autorização, violando a privacidade e a intimidade, foi elaborada a Lei Geral de Proteção de Dados - LGPD, inspirada no Regulamento Europeu de Proteção de Dados. A LGPD aplica-se tanto a arquivos físicos quanto a arquivos digitais.

A LGPD - Lei nº 13.709 de 2018 prevê disposições referentes ao tratamento de dados pessoais sensíveis, que são aqueles sobre a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado com relação à saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Os agentes de tratamento de dados devem adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, de perda, de alteração, de comunicação ou qualquer forma de tratamento inadequado ou ilícito. Salienta-se que a empresa será penalizada caso ocorra o vazamento de dados ainda que acidental.

Diante do exposto, percebe-se a importância de se adotar a segurança da informação e a cibersegurança nas empresas, tendo em vista que a ocorrência dos ataques cibernéticos tem sido crescente. A organização deve buscar garantir a segurança da informação, mapear todas as informações e os dados que são armazenados, verificar a existência dos dados sensíveis, que requerem tratamento específico, orientar os seus colaboradores com relação à proteção de dados e de informações e ao cuidado ao utilizar a rede.