Crimes Digitais e o Legislativo Brasileiro

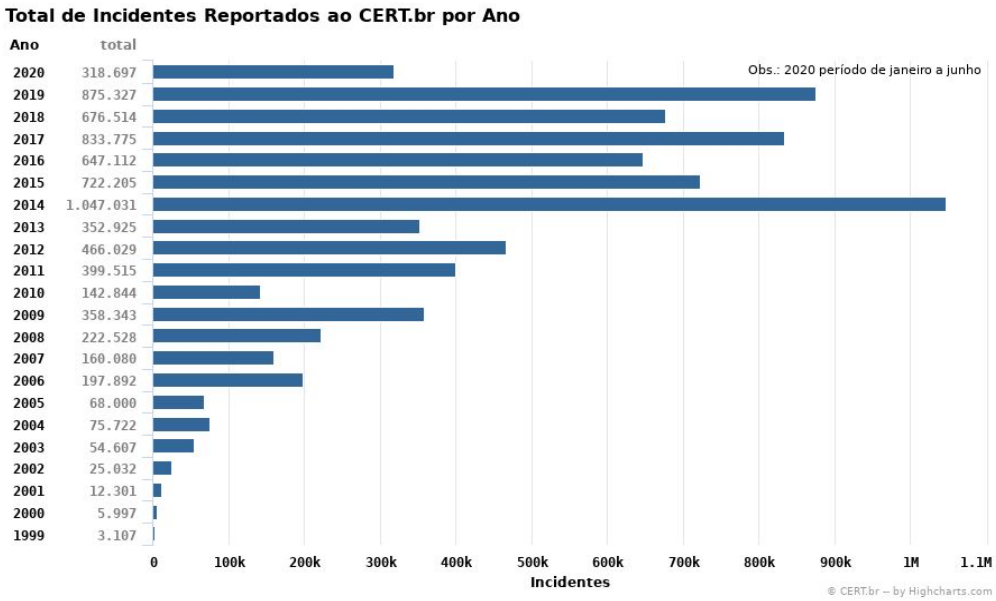
Breno de Castro Pimenta 2017114809
Helena Pato Magalhães 2017095723

1. Introdução

Não há dúvidas que a internet, enquanto meio de comunicação e partilha de informação, ocupa nas nossas vidas um papel cada vez mais central e de maior destaque. Dentro deste papel há a interação social, que junto ao advento das redes sociais, cresce de forma incessante.

Toda a relação dentro das redes é um reflexo das várias interações sociais do cotidiano e como tal é capaz de incorporar até mesmo a relação criminosa. A essas ações criminosas que se dão por meio digital denominamos de cibercrimes. Esses crimes podem ter como objetivo o dano há algo restrito à questão técnica dentro do meio digital, ou ter a lesão gerada enquadrada a algum delito previamente presente dentro da sociedade, tendo assim o meio digital apenas como agravante.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança na Internet do Brasil mantém uma estatística sobre os incidentes de cibercrimes reportados no Brasil desde 1999, como pode ser visto no gráfico abaixo. Há um aumento gradual dos incidentes até o ano de 2014, onde há uma estagnação ou até mesmo um retrocesso dos números reportados. No entanto, como apontado por Silva e Lima (2018) os números de ataques de cibercriminosos aumenta a cada ano no Brasil, tendo só em 2015 um aumento de 197%, logo podemos inferir que há uma dubiedade entre os ataques que de fato estão acontecendo e os ataques reportados. Uma das explicações para esta diferença é a levantada por Terron e Silva (2019), onde demonstram que os criminosos se adaptam rapidamente às mudanças tecnológicas e criam formas de ataques cada vez mais aprimoradas. Dentro dessa possibilidade explicativa pode-se concluir que o Brasil não só possui um número crescente desses tipos de crimes, como também padece de um despreparo não só para lidar com eles, como para reportá-los.



Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança na Internet do Brasil
https://cert.br/stats/incidentes/

2. Definições

Cibercrime é o termo usado para qualquer tipo de crime relacionado à tecnologia. Esses delitos são divididos em duas categorias, como especificado por Sudre, Martinelli e Capanema (2020). Cibercrimes **próprios** são aqueles em que computadores e sistemas de informação são utilizados como objeto da prática de crimes, como no caso de invasão de dispositivo informático. Já cibercrimes **impróprios** ocorrem quando computadores e sistemas de informação são utilizados apenas como instrumento para a prática do crime, como no caso de calúnia em rede social. Essa distinção é muito importante pois, geralmente, quando o computador é utilizado apenas como meio de execução, não há a necessidade de uma lei específica para crime digital. No caso exemplificado, a calúnia está prevista como crime no art. 138 do Código Penal.

3. Classificações

Existe uma formalidade técnica para a classificação dos ataques dos crimes digitais e há a forma como a legislação lida com esses ataques. Dentro da formalidade técnica o padrão internacional utilizado é o CPE (Common Platform Enumeration), onde as fragilidades são enumeradas, categorizadas e correlacionadas. Diferentemente da padronização técnica, a legislação é reacionária e tenta categorizar ações baseadas no intuito de lesão existente nas condutas, com a intenção de coibir a finalidade da ação e não a técnica em si. Porém ao lidar com tecnologia trabalha-se em um âmbito de mudanças constantes e sempre haverá um espaço entre a tentativa da legislação em abarcar as ações criminosas e o linear das novas possibilidades criadas pelas inovações tecnológicas. Antes de abordar o legislativo será apresentado abaixo uma classificação holística das técnicas utilizadas para a realização dos cibercrimes:

- **Força Bruta:** consiste em adivinhar, por tentativa e erro, um nome de usuário e senha.
  - É um dos ataques mais simples e usualmente faz uso de um arquivo de texto chamado de dicionário, onde se tem as senhas mais prováveis para aquele usuário.
- **Malware**: abreviação de malicious software.
  - Termo geral para um programa de computador que queira prejudicar o usuário de alguma forma.
- **Worm**: se espalham a partir de um computador para os outros usando uma rede de computadores
  - Têm a capacidade de operar de forma autônoma e, portanto, não se ligam a outro programa.
  - São concebidos apenas para se espalhar sem causar qualquer alteração grave nos sistemas.
  - Responsáveis por consumir a largura de banda, o que diminui o desempenho da rede.
  - Possuem a capacidade de se copiar pela rede e baixar outros componentes que podem ser mais perigosos.
- **Ransomware**: criptografa todos os dados da vítima, condicionando a sua liberação ao pagamento de um resgate.
  - É um cibercrime impróprio que é enquadrado como extorsão - art. 158 do Código Penal.
- **Spyware**: Coleta informações sobre as atividades dos computadores de destino sem o conhecimento de seus usuários como teclas digitadas, atividade na web e logs de mensagens instantâneas.
  - Serve para roubar dados confidenciais, segredos industriais, informações sobre clientes, dados financeiros, dados de transações de cartão de crédito.
- **Trojan**: cavalo de Tróia.
  - Se disfarça de Software legítimo para ganhar a confiança do usuário e obter permissão para ser instalado. A partir de sua execução permite a execução de um Malware atribuído pelo atacante.
- **Adware**: Tenta expor o usuário final à publicidade indesejada e potencialmente mal-intencionada.
  - Pode redirecionar as pesquisas do navegador para páginas da web parecidas com outras promoções de produtos.
- **Phishing Scam:** crime que utiliza de engenharia social para enganar vítimas com o intuito de que compartilhem informações confidenciais como senhas e número de cartões de crédito.

- É um exemplo claro do cibercrime impróprio, pois o meio digital é sempre o meio e nunca a finalidade da ação dentro do *phishing scam*.

➔ **BotNets:** o ato de buscar, infectar e controlar uma grande quantidade de computadores, usando-os para realizar qualquer atividade sem a consciência dos usuários dessas máquinas, podendo realizar ataques coordenados como DDoS's.

➔ **Ataque de negação de serviço (DDoS):** tentativa de sobrecarregar um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus usuários.

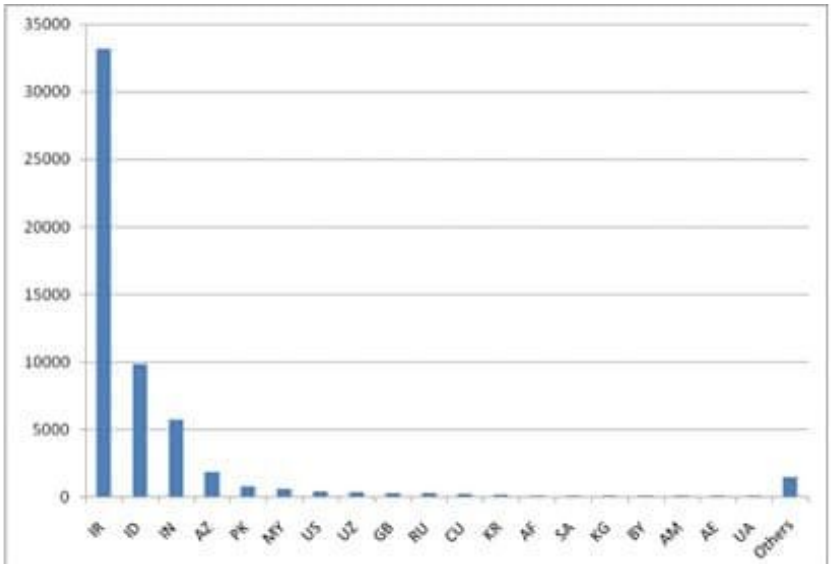
- Muito comum no contexto de servidores e é um exemplo claro do cibercrime do próprio, onde o fim da ação também pertence ao meio digital.

4. Incidentes Famosos

Stuxnet 2010

É classificado como Worm devido a sua capacidade de infectar um computador sem a necessidade de nenhuma execução por parte do usuário, utilizando-se de sete falhas do sistema operacional Windows. Na época essas falhas ainda não haviam sido registradas, portanto essas falhas são classificadas como *zero-day*, ou seja nem mesmo a Microsoft tinha consciência da existência delas na época. Ao aproveitar-se dessas aberturas o vírus conseguiu ter um nível de infecção nunca antes registrado, sendo capaz de se copiar para qualquer computador na rede, como até mesmo para um pendrive que fosse conectado, tendo tamanho de apenas 500 kbytes.

Tendo objetivos além da sua capacidade de proliferação o Stuxnet é um dos maiores marcos do que é chamado de ciberguerra (Cyberwar), pois tinha a finalidade de lesar um software de controle industrial chamado de "Sistemas de Supervisão e Aquisição de Dados" (SCADA) que é amplamente usado em indústrias de diversos países. Como demonstrado no gráfico abaixo, o worm teve uma concentração de ataques no Irã, sendo que 14 plantas industriais do país relataram ter sofrido o ataque. E o ataque mais famoso se deu na planta de enriquecimento de urânio, onde especula-se que tenha atrasado o programa nuclear do país em alguns anos. O vírus era capaz de aumentar a potência das centrífugas danificando-as e gerar relatórios falsos dos sensores para que o operadores não notassem. Na atualidade ainda não houve nenhum culpado pela criação e proliferação do vírus, porém muitos técnicos apontam que tenha sido desenvolvido por organizações governamentais, devido a complexidade e finalidade do programa.



Concentração de computadores infectados em Agosto de 2010

https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

Wannacry 2017

Dentre os ataques da atualidade, o ransomware mais famoso é o WannaCry que percorreu o mundo em 2017 sequestrando dados e pedindo resgates na criptomoeda Bitcoin. O vírus utilizava-se de uma brecha de segurança do sistema Windows que tornou-se pública após um dos vazamentos de um grupo hacker, no entanto o curioso é que na época do ataque a Microsoft já havia liberado um patch de segurança dentro da atualização para o sistema operacional Windows que impedia o uso malicioso dessa brecha, ou seja, caso o sistema estivesse atualizado na data do ataque, ele não seria infectado. No entanto, contabiliza-se que 230.000 computadores foram infectados em 150 países, sendo o Brasil o 5º país mais afetado. Uma das grandes inovações deste ataque é como ficou claro o intuito de ter uma abrangência global, o vírus possuía um tutorial claro e simples de como realizar os pagamentos e permitia ser traduzido para dezenas de línguas distintas, como pode ser visto na imagem abaixo. Uma curiosidade é que muitos técnicos, após a verificação detalhada do vírus, afirmaram que teoricamente não havia como os criminosos associarem de qual computador veio o pagamento de resgate.

Tela do sequestro do vírus Wannacry

https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-mondayhttps://cert.br/stats/incidentes/

Caso STJ 2020

Em novembro de 2020 o Superior Tribunal de Justiça (STJ) foi vítima de um ataque de ransomware. O criminoso obteve acesso à rede do tribunal e criptografou todos os dados presentes no sistema, inclusive o backup principal que estava ligado diretamente à rede principal. O ataque foi crítico devido ao processo recente de digitalização de todos os processos do tribunal, portanto, após o ataque o tribunal passou uma semana inoperante. Outro fator técnico que chama a atenção nesse ataque é que o vírus utilizado não é inovador como os dos outros exemplos acima, na verdade é um ransomware antigo tendo já sido utilizado em outros ataques, tendo sido categorizado e registrado, o que demonstra o claro despreparo das instituições brasileiras frente a este tipo de risco.

5. Dificuldades no Combate

Alguns aspectos importantes tornam o combate ao cibercrime uma tarefa complicada. Ao contrário do que muitos acreditam, a prática de cibercrimes não exige grande conhecimento técnico. Na maioria das vezes criminosos se utilizam de programas de ataque já prontos, ou contratam terceiros que possuam maior conhecimento na área. Jovens que apenas executam *scripts* prontos para realizar o ataque são chamados de "*script kiddies*".

Outra dificuldade proeminente é que, como grande parte dos delitos ocorre na internet, eles não estão sujeitos a limitações geográficas. Isso gera uma grande dificuldade de encontrar ou punir o infrator se ele estiver fora do território nacional. Por fim, também existem *hackers* com maior conhecimento técnico, e que têm uma maior capacidade de esconder suas identidades e apagar seus rastros na internet.

6. História das Leis Contra Cibercrime no Brasil

Ano 2000

No ano de 2000 houve a primeira atualização do código penal para a inclusão de cibercrimes. Os artigos adicionados são descritos a seguir.

Crime de inserção de dados falsos em sistemas de informação (art. 313-A):

> "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa"

Crime de modificação ou alteração não autorizada de sistemas de informação (art. 313-B):

> "Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa."

Ano 2012: "Lei Carolina Dieckmann" (Lei 12.737/2012)

Em maio de 2011, um *hacker* invadiu a caixa de e-mail da atriz Carolina Dieckmann, possibilitando que tivesse acesso a fotos pessoais de cunho íntimo. O invasor exigiu dez mil reais para não publicar as fotos. Como a atriz se recusou a pagar, acabou tendo suas fotos divulgadas na internet.

O fato de a vítima ser uma pessoa famosa, fez com que a discussão a respeito do delito ganhasse muita repercussão na mídia e gerou discussões populares sobre a criminalização desse tipo de prática. Toda essa pressão deu origem a uma lei, cujo processo de tramitação levou o tempo recorde de um ano. A lei, batizada com o nome da atriz, é transcrita abaixo.

Crime de "invasão de dispositivo informático" (art. 154-A, Código Penal):

> "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 três meses a um ano, e multa."

Da forma como foi redigida, essa lei sofreu muitas críticas. Uma delas é que o texto é muito vago, consequentemente, termos utilizados por ela podem ter mais de uma interpretação. A expressão “dispositivo informático”, por exemplo, se refere apenas a dispositivos de hardware ou também se aplica a serviços de internet, como e-mail e redes sociais? Também é dito que a invasão deve ocorrer mediante violação de mecanismo de segurança, isso implicaria que os dispositivos não protegidos por esse tipo de medida não serão contemplados pela lei?

Outra crítica é que a pena prevista foi considerada muito branda, podendo estimular o delito, ao invés de coibi-lo. Isso se daria nos casos em que o acusado é réu primário, podendo converter boa parte das punições em pagamento de cestas básicas.

Finalmente, uma observação em relação ao sistema judiciário brasileiro, que não teria ainda estrutura para apurar esse tipo de crime. Nessa época, quem buscava a polícia para registrar um boletim desse tipo de ocorrência, poderia esperar até três meses para ter seu equipamento periciado. Como as evidências de crimes digitais são muito voláteis, haveria grandes chances de serem perdidas antes que o equipamento fosse investigado.

Uma situação em que a lei poderia ser aplicada, aconteceu em 2013, quando a estudante Carolina Portaluppi teve seu telefone celular roubado e suas fotos íntimas divulgadas na rede. Já o caso da jornalista Rose Leonel é mais complicado. Em 2005, ela teve fotos íntimas divulgadas por seu ex-noivo, que estava descontente com o fim do relacionamento. Como ele tinha a posse das fotos autorizada pela ex-companheira, a legislação não poderia ser aplicada. Em 2010 ela ganhou a causa no tribunal e a pena infligida a ele foi de R$30 mil de multa. Porém, Leonel relata que, nesse meio tempo, ficou estigmatizada pelo incidente, chegando a perder dois empregos e sofrer preconceito da sociedade. Por isso, a jornalista criou o projeto de lei Maria da Penha Virtual, que adaptaria os crimes já contemplados em sua homônima para o meio digital. Porém, o projeto foi considerado inconstitucional e a lei não foi aprovada.

Considerando os incidentes já abordados, percebemos que eles têm uma característica em comum, as vítimas são todas mulheres. A violência contra a mulher na internet é um problema que não pode ser ignorado. Entre as principais agressões sofridas estão importunação moral e psicológica, exposição não consentida de imagens e vídeos íntimos, estupro virtual, *stalking*, *sextortion*, assédio sexual e golpes.

O **estupro virtual** foi um conceito que se tornou possível em 2009, através da alteração do art. 213 do código Penal, que ampliou o conceito de estupro, passando a ser definido como “constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso”. Como não é necessária a conjunção carnal o crime pode ser cometido à distância.

Já a prática de ***stalking*** é caracterizada pela perseguição obsessiva de uma pessoa, muitas vezes utilizando-se das redes sociais. *Stalking* não é tipificado como crime pela legislação brasileira, mas pode ser considerado importunação, e julgado como tal. Por fim, ***sextortion*** é uma expressão usada para representar a extorsão por meio de conteúdo sexual da vítima, como no caso de Carolina Dieckmann.

A pesquisa “A Voz das Redes: O que elas podem fazer pelo enfrentamento das violências contra as mulheres” indica que o assédio virtual cresceu 26000% entre 2015 e 2007, sendo a divulgação de conteúdo íntimo a ocorrência mais frequente.

Podemos citar também o relatório anual da ONG SaferNet, que promove a defesa dos direitos humanos nas redes. Ele aponta que, em 2018, houve 16717 denúncias de crimes na internet contra a mulher, enquanto em 2017 foram 961, um aumento de 1640%. Entre essas denúncias, 669 foram relacionadas a *sextortion*. O texto também mostra que o número de relatos de divulgação não consentida de imagens íntimas aumentou 2300% em dez anos, já que, em 2008, apenas 29 casos foram atendidos pela central. Por fim, ele comprova que as mulheres são as principais vítimas, aparecendo em 66% das denúncias (440 ocorrências).

Nessa época, quando não era possível aplicar a lei Carolina Dieckmann, recorria-se à lei Maria da Penha para responsabilizar o autor da divulgação de conteúdo íntimo sem permissão, já que ela possui um artigo que menciona agressão psicológica.

Ano 2014: Marco civil da internet (Lei nº 12.965, de 23 de abril de 2014)

Com a aprovação do Marco Civil da Internet e da lei de importunação sexual, a divulgação de "fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza à sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia" tornou-se crime.

O código Penal foi alterado em 2018 para incluir o crime de importunação sexual. Definido pela Lei n. 13.718/18, é caracterizado pela realização de ato libidinoso na presença de alguém de forma não consensual, com o objetivo de "satisfazer a própria lascívia ou a de terceiro".

O Art. 3º do MCI estabelece os seguintes princípios:

- Liberdade de expressão;
- Proteção da privacidade e dos dados pessoais;
- Neutralidade de rede;
- Estabilidade, segurança e funcionalidade da rede;
- Responsabilização dos agentes de acordo com suas atividades;
- Liberdade dos modelos de negócios promovidos na internet.

Já os artigos 10º a 12º definem que as empresas devem manter os registros de conexão para futura requisição judicial, quando houver necessidade. Para entender o que são esses registros, a lei define alguns conceitos. Um **Provedor de Aplicação de Internet** é uma empresa que se encontra na Internet provendo algum tipo de serviço e fica responsável por manter os registros de acesso às aplicações de Internet pelo prazo de seis meses. Os **Registros de Acesso a Aplicações de Internet** são o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Um **Provedor de Acesso à Internet** é a empresa que conecta um usuário à Internet, sendo responsável por manter os registros de conexão à Internet que determinado dispositivo computacional realizou pelo prazo de um ano. Os **Registro de Conexão** são o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.

Os registros mencionados deverão ser excluídos após o prazo previsto e são informações cruciais para o processo de investigação de cibercrimes, que será explicado à frente.

Ano 2018: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 14/08/2018)

A Lei Geral de Proteção dos Dados Pessoais está em vigor desde 18 de setembro de 2020 e seus principais objetivos são:

- Proteção à privacidade: assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais;
- Transparência: estabelecer regras claras sobre tratamento de dados pessoais;
- Desenvolvimento: fomentar o desenvolvimento econômico e tecnológico;
- Padronização de normas: estabelecer regras únicas e harmônicas sobre tratamento de dados pessoais, por todos os agentes e controladores que fazem tratamento e coleta de dados;

- Segurança jurídica: fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo;
- Favorecimento à concorrência: promover a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

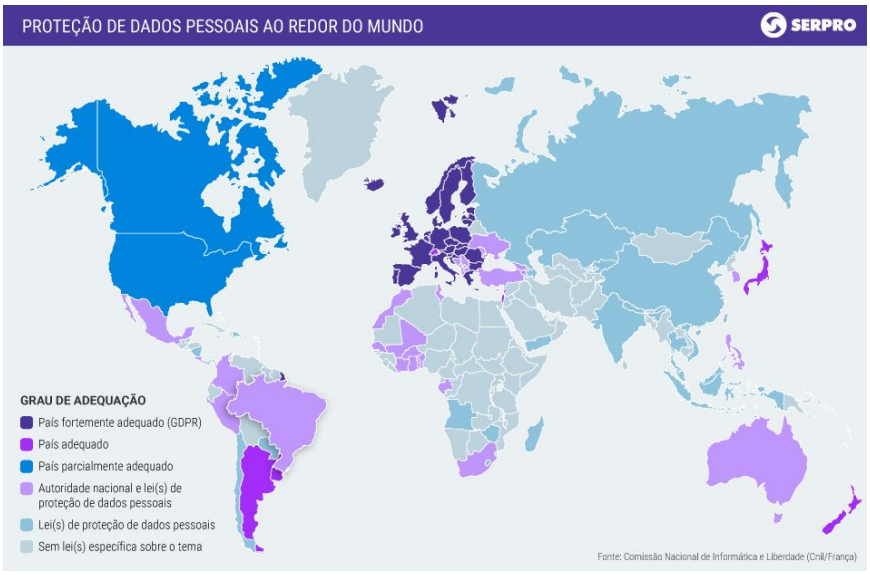
A LGPD classifica os dados gerados da seguinte forma: **Dados Pessoais** são todos aqueles que podem identificar uma pessoa, como nome e CPF. **Dados Sensíveis** são informações que podem ser utilizadas de forma discriminatória e, portanto, carecem de proteção especial, como religião e sexualidade. **Dados Pessoais de Crianças e Adolescentes** devem ter o tratamento realizado com o consentimento específico por pelo menos um dos pais ou pelo responsável legal. Por fim, **Dados Pessoais Anonimizados** são relativos a titular que não possa ser identificado, portanto estão fora do escopo de aplicação da lei.

Dentre os direitos garantidos pelo Art. 18 da lei, ao titular dos dados, estão:

- Confirmação de existência e tratamento de seus dados;
- Acesso a seus dados pessoais;
- Correção dos dados pessoais;
- Anonimização, bloqueio ou eliminação de dados pessoais;
- Obtenção de informações sobre o compartilhamento de dados pessoais;
- Revogação do consentimento dado;
- Portabilidade de dados pessoais.

A LGPD regulamentará qualquer atividade que envolva utilização de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica, no território nacional ou em países onde estejam localizados os dados. Ela se aplica extraterritorialmente no caso de a operação de tratamento dos dados ser realizada no território nacional, ou ter por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou os dados pessoais, objeto do tratamento, terem sido coletados no território nacional.

A imagem abaixo lista alguns dos deveres das empresas ao se adequarem à LGPD.



Ao lado está um mapa que ilustra o avanço em relação às leis de proteção de dados em diversos países. Nele podemos ver que o Brasil ainda tem um longo caminho a percorrer para proteger melhor os dados de sua população. A GDPR, considerada a legislação mais completa em relação a proteção de dados do mundo, tem algumas vantagens em relação à nossa norma.

A lei brasileira, por exemplo, orienta que o tratamento de dados pessoais deve ser feito com segurança, sob orientações da Autoridade Nacional de Proteção de Dados (ANPD), mas ela não especifica qualquer técnica de segurança. Enquanto isso, a GDPR é clara ao exigir medidas para manter os bancos de dados seguros. Entre elas, estão a encriptação e a pseudoanonimização.

Outra diferença ocorre em relação ao **marketing direto** ou comercialização direta, que diz respeito ao tratamento de dados pessoais para fins de criação de perfil e marketing. Na legislação europeia, são definidos requisitos e etapas específicos, que devem ser seguidos nestas situações. Os titulares podem se opor a qualquer momento acerca do processamento de seus dados para tais fins. Já a norma brasileira não aborda o assunto diretamente, o que pode acarretar problemas de autorização implícita.

Por causa da vigência da lei, o Facebook está convidando usuários brasileiros a gerenciar suas configurações de dados pessoais. A rede alega que só usa dados pessoais sensíveis com sua permissão, tornando-os visíveis no seu perfil. O usuário tem a opção de aceitar isso, ou de visitar as configurações de privacidade para controlar se as informações podem ser vistas por “todos”, “amigos”, “amigos exceto conhecidos”, “somente eu”, entre outras opções.

Já podemos ver uma situação de aplicação da lei quando, em 2020, a Justiça de São Paulo condenou em primeira instância a construtora Cyrela a pagar indenização de R$ 10 mil por compartilhar dados de um cliente com outras empresas. O autor da ação contou que em 2018, mesmo ano em que comprou um apartamento da Cyrela, começou a ser assediado por instituições financeiras e firmas de decoração, que citavam sua recente aquisição. Ao questionar uma delas sobre a maneira em que havia conseguido seu contato, obteve a resposta:

> "Nós trabalhamos com diversas parcerias para oferecermos nossa consultoria em questão a quitação de empreendimentos de algumas construtoras. Não sei ao certo quem passou o seu contato"

Apesar de a decisão ter sido baseada na legislação, a ação é anterior à data em que a medida entrou em vigor. Dessa forma, a Cyrela poderia recorrer argumentando que a LGPD não tem efeitos retroativos. Além disso, as multas e sanções da norma passam a estar em vigor apenas a partir de agosto de 2021.

Enquanto isso, a 5ª Pesquisa Nacional Eskive sobre Conscientização em Segurança da Informação revela que menos de 30% das empresas brasileiras preparam funcionários para que eles trabalhem em conformidade com a LGPD. Nas empresas de varejo quase 80% dedicam apenas de 1% a 25% do tempo da equipe de segurança da informação a programas de conscientização dos funcionários. O estudo envolveu 300 profissionais de segurança das principais empresas brasileiras em 26 segmentos distintos.

Sabemos que, de nada adianta a existência da lei se as empresas não estiverem preparadas para lidar com ela. Portanto, podemos concluir que, apesar do tempo que as empresas tiveram para se adequar à norma, que agora já está em vigor, ainda é necessário pressioná-las e fiscalizá-las para que elas cumpram seu papel.

7. Processo de Investigação

O processo de investigação de cibercrimes se apoia muito nas normas estabelecidas pelo MCI. Ao buscar o culpado, primeiramente são checados os registros de acesso a aplicação de internet por onde o crime foi cometido. Dessa forma, por meio da data e hora do acesso, obtém-se o endereço IP da pessoa que fez o acesso e seu provedor de internet. Com o provedor, os investigadores conseguem os registros de conexão relativos ao proprietário titular assinante do serviço de internet, dono do IP encontrado.

Nesse ponto já praticamente chega-se ao criminoso, mesmo que ele não seja o titular do serviço, provavelmente é alguém próximo a ele. A não ser no caso de se tratar de uma empresa, em que ela teria métodos distintos de monitoramento da atividade de seus funcionários, que seriam usados na investigação.

Agora entra o trabalho da perícia forense, em que computadores do suspeito serão investigados, podendo ser apreendidos. As evidências digitais são diferentes das evidências de crimes comuns, pois são encontradas em dispositivos eletrônicos, que podem ter um armazenamento bastante volátil. Porém, ao desligar a energia de um computador, as informações armazenadas na memória RAM não somem imediatamente, passando por um processo de descarga dos chips de memória. Assim, com técnicas adequadas, e com acesso físico ao computador, é possível recuperar todas, ou parte, das informações. Nessa etapa, o investigador deve ser muito cuidadoso para não perder essas evidências ou utilizar-se de métodos ilícitos, como software não confiável, para obtê-las pois, dessa forma, elas não poderiam ser utilizadas no julgamento.

No caso de o indivíduo que praticou a conduta criminosa não ser encontrado o julgamento pode proceder de duas formas. Para o Direito Penal, somente é possível punir quem praticou o crime. Já para o Direito Civil, caso ninguém mais seja apontado como praticante do dano moral, o proprietário da linha telefônica é quem responderá pelas ofensas.

8. Conclusão

Os crimes digitais possuem diversas formas e objetivos. Eles estão constantemente evoluindo, se tornando mais difíceis de identificar e enfrentar. Por isso, seus combatentes não podem ficar para trás, devemos adequar nossas leis para punir de forma adequada esses criminosos e ter certeza de que essas normas estão sendo devidamente aplicadas. Porém, a realidade mostra que o Brasil ainda está muito despreparado para lidar com esses delitos, uma situação que deve ser imediatamente revertida.

9. Referências

SUDRE, Gilberto; MARTINELLI, Gustavo; CAPANEMA, Walter. **Computação e Sociedade**: A tecnologia. Volume 3. 1ª edição. Capítulo 21. Cuiabá-MT: EdUFMT Digital, 2020.

SILVA, Jefferson; LIMA, Maria. Os principais cibercrimes praticados no Brasil. **V Congresso Nacional de Educação.** Recife, out. 2018.

TERRON, Leticia; SILVA, Henrique. Cibercrimes: A evolução digital. **IX SEMPEX do Centro Universitário de Santa Fé do Sul.** Santa Fé do Sul, nov. 2019.

https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
https://papers.duckdns.org/files/2011_IECON_stuxnet.pdf
https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
https://cert.br/stats/incidentes/
https://blog.fmp.edu.br/lei-carolina-dieckmann-voce-sabe-que-o-essa-lei-representa/
http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html
https://istoe.com.br/288575_LEI+CAROLINA+DIECKMANN+APENAS+O+PRIMEIRO+PASSO/
https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet
https://www.lgpdbrasil.com.br/
https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais
https://www.ecommercebrasil.com.br/noticias/empresas-preparam-funcionarios-lgpd/
https://www.privacytech.com.br/destaque/construtora-e-condenada-por-compartilhar-dados-de-cliente-com-base-na-lgpd,376420.jhtml
https://tecnoblog.net/361328/facebook-mostra-aviso-sobre-dados-pessoais-e-lgpd-no-brasil/
https://medium.com/@icyphox/what-are-ctfs-and-why-you-should-care-652f44b18221
https://realprotect.net/4-tipos-de-malware-que-voce-deve-ficar-atento/
https://cio.com.br/tendencias/8-tipos-de-malware-e-como-reconhece-los/
https://blog.hdstore.com.br/fique-de-olho-em-6-tipos-de-malwares/
https://jus.com.br/artigos/3614/insercao-de-dados-falsos-em-sistema-de-informacoes-art-313-a-e-modificacao-ou-alteracao-nao-autorizada-de-sistema-de-informacoes-art-313-b/2
http://g1.globo.com/pr/norte-noroeste/noticia/2013/08/apos-fotos-intimas-pararem-na-web-mulher-diz-sofrer-preconceito-diario.html
http://ego.globo.com/famosos/noticia/2013/12/ja-temos-um-suspeito-diz-advogado-de-portaluppi-sobre-fotos-nuas.html
https://olhardigital.com.br/2019/07/24/noticias/mulheres-sao-maiores-vitimas-de-vazamento-de-fotos-e-perseguicao-na-internet/
https://digital.fenalaw.com.br/legislao/5-diferenas-entre-lgpd-e-gdpr
https://posocco.jusbrasil.com.br/noticias/497174996/o-que-e-estupro-virtual
https://www.cnj.jus.br/cnj-servico-o-que-e-o-crime-de-importunacao-sexual/