Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LUCAS ORTIZ GONÇALEZ

DIREITO PENAL E NOVAS TECNOLOGIAS: APLICABILIDADE OU NÃO DAS NORMAS JÁ EXISTENTES PARA CRIMES DIGITAIS.

Assis/SP
2021

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LUCAS ORTIZ GONÇALEZ

DIREITO PENAL E AS NOVAS TECNOLOGIAS: APLICABILIDADE OU NÃO DAS NORMAS JÁ EXISTENTES PARA CRIMES DIGITAIS.

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Lucas Ortiz Gonçalez
Orientador(a): Cláudio José Palma Sanchez.

Assis/SP
2021

FICHA CATALOGRÁFICA

G635d, GONÇALEZ, Lucas Ortiz

Direito Penal e Novas Tecnologias: aplicabilidade ou não das Normas já existentes para crimes digitais / Lucas Ortiz Gonçalez. – Assis, 2021.
41 p.

Trabalho de conclusão de curso (Direito). – Fundação Educacional do Município de Assis-FEMA

Orientador: Ms. Cláudio José Palma Sanchez

1. Crimes digitais 2. Código Penal

CDD 341.55251

DIREITO PENAL E AS NOVAS TECNOLOGIAS: APLICABILIDADE OU NÃO DAS NORMAS JÁ EXISTENTES PARA CRIMES DIGITAIS.

LUCAS ORTIZ GONÇALEZ

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação de Direito, avaliado pela seguinte comissão examinadora:

Orientador: Cláudio José Palma Sanchez

Examinador: Fabio Pinha Alonso

Assis/SP
2021

DEDICATÓRIA

Dedico o presente trabalho à minha família, amigos e a quem possa se interessar por este tema.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus por ter me guiado em toda minha trajetória acadêmica, me dando fé e forças para continuar, ainda mais nesses dois últimos anos diferentes dos outros anteriores.

Aos professores e funcionários da FEMA – Fundação Educacional do Município de Assis, por todos os anos de muitas lições e aprendizados, fazendo com que eu seja eternamente grato por fazer parte do corpo discente desta Instituição.

Ao meu orientador, advogado, mestre e professor de Direito, Dr. Cláudio José Palma Sanchez, um excelente profissional e conhecedor de todas as áreas do direito, sou agradecido por toda dedicação, conselhos e paciência para que pudesse concluir este trabalho monográfico.

Finalmente, gostaria de agradecer meus pais, familiares e amigos que sempre me apoiaram para que eu pudesse e conseguisse finalizar este curso com excelência.

Obrigado a todos por fazerem parte deste momento muito importante da minha vida.

RESUMO

O presente estudo e trabalho monográfico trata de crimes digitais cometidos mediante o uso da tecnologia, mais especificamente a Internet, mostrando o surgimento desta, os crimes que podem ser cometidos em seu âmbito, bem como críticas e possíveis soluções, no Código Penal, para que estes delitos sejam punidos mais severamente e com a devida importância que devem receber.

Palavras-chave: Código Penal; Internet; Crimes Digitais.

ABSTRACT

The present study and monographic work deals with digital cries committed through the use of technology, more specifically the internet, showing its beggining, the crimes that can be commited withins its scope, as well as criticism and possible solutions, in the Penal Code, so that these offenses can be punished more severely and with the importance that they should receive.

Keywords: Penal Code; Internet; Digital Crimes.

LISTA DE ABREVIATURAS E SIGLAS

CF	CONSTITUIÇÃO FEDERAL
CPP	CÓDIGO DE PROCESSO PENAL
CP	CÓDIGO PENAL
IP	*INTERNET PROTOCOL*
ART.	ARTIGO
ARPANET	*ADVANCED RESEARCH PROJECTS ADMINISTRATION*
FAPESP	FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DE SÃO PAULO
IDC	*INTERNATIONAL DATA CORPORATION*
WWW	*WORLD WIDE WEB*
RNP	REDE NACIONAL DE PESQUISA
TIC	TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

SUMÁRIO

1. INTRODUÇÃO

O presente estudo tem como objetivo analisar os crimes praticados em ambientes digitais e a busca por uma resposta eficiente do Direito Penal, matéria que encontra pouco embasamento na doutrina brasileira, sendo os assuntos mais relacionados a este tema encontrados no âmbito mais clássico do Direito Penal.

O que aconteceu, no território nacional, basicamente, foi a adequação das práticas criminosas cibernéticas aos crimes que já se encontravam tipificadas no nosso ordenamento jurídico, ou seja, observa-se apenas o bem jurídico que já é protegido pela leipenal.

O que deve ser levado em consideração, no entanto, é que a sociedade vive em plena mudança e evolução, assim como as tecnologias. Logo, condutas que antes não eram praticadas ou, se eram, não eram consideradas criminosas, agora podem ser, e a tecnologia em constante ascensão pode ser usada, hoje em dia, para a realização de condutas ilícitas que antes eram impensáveis.

O mundo digital, ou, mais especificamente, a internet, pode ser um ambiente mais “atrativo” para o cometimento de crimes, justamente por conta de seu modus operandi maisconveniente, pois assegura um maior anonimato, deixando as pessoas menos inibidas quando se diz respeito a práticas criminosas.

Reside aqui o interesse em discutir esse tema de suma importância, sabendo- se que, com o avanço da tecnologia, há novos bens jurídicos a serem tutelados e um novo modus operandi, fazendo-se questionar se o direito também não deveria evoluir para responder esses crimes e práticas novas com mais afinco, não podendo esquecer que é necessária uma atualização legislativa para tutelar os bens jurídicos de forma mais corretae concisa.

2. CAPÍTULO 1 – A ERA DA INFORMAÇÃO E A CHEGADA DA INTERNET AO BRASIL

2.1. A ERA DA INFORMAÇÃO

Pode-se dizer que a Era da Informação é uma espécie de Terceira Revolução Industrial, ou seja, não é nada mais do que uma entre outras evoluções que acabaram por transformar o meio no qual a sociedade vivia até então. É, mais precisamente, a época que veio após a Era Industrial, depois da década de 1980. Foi, portanto, uma substituição à Era Industrial que acabou por suceder a era da agricultura, mais conhecida como Primeira Revolução Industrial.

A doutrina estrangeira divide a Era da Informação em dois diferentes tópicos, a "Era Eletrônica" que se encontra no período entre a Segunda Guerra Mundial até a década de 1980 e a "Era Digital", que veio com a produção em massa de computadores pessoais, após a década de 1980. Toda essa divisão, entretanto, parece não ser necessária, pois a "Era da Informação" diz respeito a novas práticas e condutas que foram possíveis por causa de todo o desenvolvimento tecnológico. Por isso, há uma preferência em se utilizar a expressão "Era da Informação" de Sieber[1]

É por obvio que essa nova Era trouxe muitos benefícios ao mundo, visto que houve uma integração entre espaço e pessoas que antes era inimaginável, mas, como tudo que é muito bom, há sempre um lado mais obscuro andando junto.

Um dos problemas que veio junto com toda essa avalanche de conectividade e interligação foi a "Era da Desinformação" de Kanitz[2], visto que, com a Internet, muitas pessoas podem expressar sua opinião de uma maneira que não há controle e, com isso, acaba sendo gerado muito "lixo".

Além da desinformação que pode ser obtida através do uso da internet, ainda há males físicos e psíquicos advindos do uso excessivo de ambientes virtuais, como problemas psicológicos, que já podem ser tratados através de um "desmame" da internet onde o paciente vivencia mais experiências do mundo real[3]. Além desse tipo de tratamento,

---

[1] SIEBER, Ulrich. Documentación para uma aproximaxión al delito informático. In: MIR,
[2] KANITZ, Stephen. Disponível em: <www.kanitz.com.br, acesso em 14/04/2021>.
[3] Viciados em Internet são atendidos em São Paulo - <https://www.saopaulo.sp.gov.br/spnoticias/na-imprensa/viciados-em-internet-sao-atendidos-em-sp/, acesso em 14/04/2021>.

há, até mesmo, centro de reabilitação que atende pessoas viciadas em celular e cuida de pacientes que passam, em um dia, mais de 9 horas conectados.[4]

Hoje em dia já dependemos, em quase todos os aspectos da vida, da tecnologia e da informática, dos bancos de dados e da telemática e, por causa de toda essa ligação, estamos, diariamente, sujeitos a práticas ilícitas que prejudicam tanto as pessoas em sua individualidade quanto uma sociedade inteira.

Toda essa ligação e conectividade advindos da "Era da Informação" acabaram por facilitar e viabilizar a globalização e, consequentemente, a prática de crimes à distância.

2.2. O SURGIMENTO DA INTERNET

A Internet surgiu na década de 1960 quando algumas universidades se reuniram e criaram a chamada ARPANET (*Advanced Research Projects Administration* – Administração de Projetos e Pesquisas Avançados), que nada mais era do que um sistema de computadores com a finalidade de trocar informações e, naquele tempo, o seu uso era limitado e exclusivo das Forças Armadas dos Estados Unidos da América.

A ARPANET foi a primeira rede a utilizar o TCP/IP[5] (Protocolo de Controle de Transferência/Protocolo de Internet) que, juntas, possibilitaram o surgimento da Internet. Conforme o projeto evoluiu, várias redes separadas puderam se unir em uma rede única para que, assim, conseguissem atuar em grupo ao interligar vários computadores simultaneamente.

A ARPANET foi desativada em 1990 e, por causa dela, juntamente com o aumento vertiginoso da tecnologia, a rede virou algo imensamente maior, fazendo com que, hoje em dia, mais de 4,6 bilhões de usuários ao redor do mundo estejam navegando pela rede digital, o que representa em mais de 60% da população mundial.[6]

Entre a década de 1980 e começo de 1990, a rede sofreu melhorias e começou a aparecer na Internet a sua forma que conhecemos hoje como, por exemplo, o *world wide web* (WWW) que teve o seu lançamento em 1991 e permitiu que fossem transmitidos,

---

[4] Centro de reabilitação em São Paulo atende pessoas viciadas em celular - <https://recordtv.r7.com/jornal-da-record/fotos/centro-de-reabilitacao-em-sao-paulo-atende-pessoas-viciadas-em-celular-29092018>, a cesso em 14/04/2021>.

[5] O endereço de IP é um número diferente que é dado a cada computador quando se conecta à Internet e tem a função de identificar um computador dentro de uma rede.

[6] Número de usuários de Internet no mundo chega aos 4,66 bilhões – <https://www.istoedinheiro.com.br/numero-de-usuarios-de-internet-no-mundo-chega-aos-466-bilhoes/>, acesso em 14/04/2021.

através da rede, sons, vídeos e imagens. Após, vieram os provedores de internet que eram as empresas que vendiam o meio de utilizar a internet aos seus consumidores e clientes finais.

De 1994 para frente, a internet aumentou as suas funções tornando-se uma plataforma de comercialização de serviços e produtos, permitindo ser possível fazer compras sem ao menos sair de casa. Conforme dito pela *International Data Corporation* (IDC), a rede movimentou um montante de US$ 2,2 bilhões em 1996[7].

2.3. CHEGADA DA INTERNET AO BRASIL

Em 1988, o Laboratório Nacional de Computação Científica (LNCC) conectou-se com a Universidade de Maryland, nos Estados Unidos da América, acessando a Bitnet[8]. Neste mesmo ano, a FAPESP se conectou, por meio da Bitnet, ao *Fermi National Accelerator Laboratory (Fermilab)* em Chicago, nos Estados Unidos da América e, em 1989, a Universidade Federal do Rio de Janeiro também se conectou, com o auxílio de uma universidade, à Bitnet.

Também em 1989 foi criada a Rede Nacional de Pesquisa (RNP) que, durante os anos 90, foi a encarregada por proporcionar o acesso à internet a 600 instituições de ensino, somando o número de mais de 65 mil usuários beneficiados.

Em 1991 o acesso à já chamada Internet era utilizado também por órgãos do governo e, na época, a Internet era usufruída para a transferência de arquivos e acesso a base de dados.

Em 1992 aconteceu a inserção de uma rede que abrangia a maioria do país. No começo, onze estados faziam parte dessa rede de equipamentos e linhas de comunicação que recebia o nome de central da RNP.

Apenas em 1995 aconteceu a primeira transmissão à longa distância que compreendia os estados do Rio Grande do Sul e de São Paulo e, após, no mesmo ano, foi finalmente liberada a operação comercial no Brasil.

---

[7] Internet, a história da Internet, surgimento da Internet, a Internet no Mundo, o que é internet, o surgimento da internet no Brasil, a internet no Brasil.,
<https://monografias.brasilescola.uol.com.br/computacao/internet.htm#:~:text=Segundo%20a%20International%20Data%20Corporation,220%20bilh%C3%B5es%20no%20ano%202001, acesso em 14/04/2021>

[8] Rede remota que foi criada em 1981, que tinha como objetivo tornar possível um meio barato e rápido de comunicação para o meio acadêmico.

Em 1996 surgiram os primeiros grandes portais de informação de internet privados em nosso território pátrio e, em 1997, alguns órgãos públicos começaram a ser informatizados.

Alguns provedores de acesso gratuito começaram a aparecer no ano 2000, contavam com internet discada para o seu acesso e eram financiadas por propagandas que eram inseridas em seu navegador.

Depois, esses provedores de internet discada começaram a sair de cena, dando o seu lugar às primeiras provedoras de acesso à Internet através de banda larga[9] que, por consequência, aumentou a velocidade da conexão e permitiu que vídeos pudessem ser transmitidos pela primeira vez.

De 2004 para frente, com o surgimento das redes sociais, a Internet passou a se tornar mais e mais popular e, de 2007 em diante, com a conexão 3G e a comercialização dos primeiros smartphones, a Internet passa a fazer parte, também, dos aparelhos móveis, atingindo um número cada vez maior de usuários.

Mais de 102 milhões de internautas, o que representava 58% da população do país em 2015, se encontravam conectados à internet[10] e, em 2019, o número de usuários chegou a 134 milhões, ou 74% da população com idade superior a 10 anos, com 71% dos domicílios em território nacional com acesso à Internet, segundo a pesquisa TIC.[11]

2.4. SOCIEDADE GLOBALIZADA

Essa sociedade não começou do nada, mas a partir de um grande lapso temporal onde houve grande desenvolvimento em várias áreas, como na economia, tecnologia, relações sociais, e pode-se dizer que o seu início coincide com a Segunda Revolução Industrial.

---

[9] Evolução natural da internet discada, sendo uma internet com velocidade superior e de forma ininterrupta, dispensando que a linha telefônica seja utilizada.

[10] Pesquisa mostra que 58% da população brasileira usam a internet - <https://agenciabrasil.ebc.com.br/pesquisa-e-inovacao/noticia/2016-09/pesquisa-mostra-que-58-da-populacao-brasileira-usam-internet, acesso em 14/04/2021>.

[11] Brasil tem 134 milhões de usuários de internet, aponta pesquisa, < https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>, acesso em 14/04/2021.

Primeiramente, houve a troca da mão de obra humana e de animais pelas máquinas e, posteriormente, mais precisamente no século XX, a troca da atividade intelectual do homem pelas máquinas.

Mais tarde, com o surgimento da Internet, tudo se tornou ainda mais interligado.

É inegável o tamanho da importância da globalização para a formação do mundo tal como conhecemos hoje. A vida, em certos aspectos, se tornou muito mais fácil e ágil por conta dessa constante evolução da tecnologia do “mundo sem fronteiras”.

Entretanto, deve-se levar em conta os aspectos negativos advindos de toda essa mudança, como é o caso do aumento da desigualdade social e problemas que toda a facilidade da tecnologia pode trazer ao ser humano.

Como as máquinas substituem a mão de obra humana, há um aumento vertiginoso no nível de desemprego. Com a falta de emprego e a necessidade de se trabalhar, há o aumento do trabalho informal e, em alguns casos, o da criminalidade, visto que o mercado de drogas e outras práticas ilícitas podem ser atraentes para quem se encontra sem dinheiro e, até mesmo, muitas vezes, em situação de miséria.

O aspecto psicológico do ser humano também pode ser afetado pela globalização, pois, mesmo que fisicamente longe uns dos outros, as redes internacionais de telecomunicação, como a Internet, proporcionam às pessoas uma troca direta, constante e natural, fazendo com que haja uma sensação de estarmos em um local sem barreiras nem fronteiras, onde tudo é uma coisa só. É como que se o mundo todo, em toda sua enorme e exuberante vastidão, seja reduzido a um único ponto, onde tudo e todos estão conectados ao mesmo momento.

Apesar de conectados com o mundo, o ser humano entrou em uma tendência de se fechar e ficar mais sozinho. Com a facilidade proporcionada pela globalização e redes conectadas, não é necessário nem ao menos se locomover para ir ao mercado, bastando pegar seu celular e fazer a compra, que chegará à sua porta, pouco tempo depois. Nem mesmo ir ao banco é mais preciso, sendo possível fazer tudo na palma de sua mão, desde transferências bancárias até mesmo – pasmem – depósitos de cheques.

Como quase tudo, há o bônus e o ônus, e, com a globalização, não poderia ser diferente. Existe o conforto e facilidade de uma pessoa poder fazer tudo sem sair de casa, mas, para isso, existe também o aspecto negativo psicológico de cada vez ficar mais recluso e isolado.

O mundo vive, desde o seu princípio, em constante evolução. A globalização é um fenômeno mais recente, sendo difícil definir quando, de fato, começou a acontecer. O mais aceito é de que começou com o final da Segunda Guerra Mundial e o fim do bloco socialista.

3. CAPÍTULO 2 – A TECNOLOGIA COMO FACILITADORA PARA PRÁTICAS CRIMINOSAS

3.1. NASCE UM NOVO MODUS OPERANDI

Conforme dito no capítulo anterior, a tecnologia foi – e é – uma grande aliada para a sociedade de forma geral. Além de ter facilitado dia a dia da maioria das pessoas, possibilitando que tarefas do cotidiano sejam feitas com muito mais praticidade e rapidez, fez também com que as fronteiras entre países e nações “desaparecessem”, por consequência da Globalização, onde tudo e todos estão interligados ao mesmo tempo.

Apesar de todos os pontos positivos da que a Era da Informação proporcionou, não se pode esquecer que, com ela, surgiram práticas criminosas que até então não eram conhecidas ou, se eram, eram feitas através de outro modus operandi outro que a internet.

Com a evolução da tecnologia, portanto, houve facilidade e atratividade para que delinquentes pudessem praticar condutas criminosas de uma maneira muito mais fácil e, frequentemente, conseguindo manter o anonimato. Os criminosos acreditam, ainda, haver certa impunidade ou que, até mesmo, muitas das vezes, não existe nem mesmo punição para suas ações ilícitas.

Além disso, várias estratégias também são criadas para que os usuários, de maneira inocente, caiam em golpes cibernéticos justamente por não terem preparo e nem informação para que possam identificar as tentativas desses golpes e se prevenir para que não acabem nessas armadilhas digitais.

Essas condutas podem ser divididas em condutas já existentes (crimes digitais impróprios) e tipificadas pelo nosso Código, mas que, com a chegada da tecnologia, mudam o meio pelo qual a prática é realizada, como no furto, por exemplo. Antes, para furtar, era necessário sair de casa e realizar o crime mediante a presença da vítima. Hoje, com a tecnologia, é possível realizar um furto sem ao menos sair do seu próprio sofá e conforto da sua casa. O furto sempre existiu e foi tipificado pelo nosso Ordenamento Jurídico. O que ocorreu foi uma mudança no modus operandi.

E há os crimes que, até a chegada da tecnologia, eram desconhecidos e impossíveis de serem cometidos sem ser por meio daquela, logo, inexistentes no nosso ordenamento jurídico, como é o caso de invadir computadores e violar dados de usuários, trabalhados na

Lei dos Crimes Cibernéticos (12.737/2012)[12], posteriormente modificada pela Lei 14.155/2021. Estes podem ser chamados de crimes digitais próprios.

3.2. CRIMES DIGITAIS PRÓPRIOS

Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.[13]

O nosso ordenamento jurídico teve diversas mudanças ao que diz respeito à legislação que é aplicada a crimes do meio digital, mas, até o ano de 2012 ainda não existia lei específica para que pudessem ser punidos os crimes digitais próprios.

Mas, com certos acontecimentos, houve a publicação de leis que tratavam a respeito de algumas partes dessa matéria, como a Lei 12.737/2012, posteriormente modificada pela Lei 14.155/2021 e a Lei 12.735/2012.[14]

3.2.1. Invasão ou Hacking.[15]

O termo hacker[16], que tem origem inglesa, começou a aparecer e se tornar mais visível com a popularização da internet, por volta dos anos 90. Muitos deles são, inclusive, contratados por grandes empresas ao redor do mundo para que testem seus sistemas para verificar se há algum tipo de falha, vazamento de conteúdo ou a possibilidade de terem os seus sistemas invadidos por outros[17].

Há, também, os chamados crackers[18] que são uma espécie de hackers “do mal”,que usam todos os seus conhecimentos e artimanhas para realizar crimes.

O acesso não autorizado, ou hacking, é adentrar, de maneira indevida, um sistema informático, por diferentes motivos por parte do agente. O bem jurídico protegido aqui não

---

[12] Conhecia como Lei Carolina Dieckamnn, que fez alterações no Código Penal Brasileiro, tipificando os crimes informáticos.
[13] JESUS, Damásio E. de. (apud CARNEIRO, 2012, [n.p.]).
[14] Também conhecida como Lei Azeredo, definiu a criação de delegacias virtuais e também tornou obrigatório que mensagens de cunho racista devessem interrompidas e, posteriormente, excluídas.
[15] Pode ser usado, também, o termo “acesso não autorizado”.
[16] Pessoa que se dedica, por inúmeros motivos, a conhecer e mudar aspectos internos (*software*) de redes de computadores, programas e dispositivos diversos.
[17] O hacker como carreira profissional - <https://economia.estadao.com.br/blogs/radar-do-emprego/o-hacker-como-carreira-profissional/, acesso em 20/04/2021>
[18] “Aquele que quebra”, no caso, aquele que quebra e invade os sistemas informáticos de segurança.

é o da inviolabilidade dos programas computacionais, mas os dados, ou seja, toda a informação ali contida.

O conceito material de crime exige que, para que este exista, haja uma afetação de um bem jurídico em consequência da ação típica praticada, logo, deve ser decidido se o comportamento de quem acessa a internet de forma indevida de fato ofende ou não um bem jurídico tutelado.

Regis Prado (2000) ensina:

> Não há delito sem que haja lesão ou perigo de lesão (princípio da lesividade ou ofensividade) a um bem jurídico determinado. Sob esta perspectiva, a tutela penal só é legítima quando socialmente necessária (princípio da necessidade), imprescindível para assegurar as condições devidas, o desenvolvimento e a paz social, tendo em conta os ditames superiores da dignidade e da liberdade da pessoa humana.[19]

Em uma sociedade, a privacidade deve ser tratada como bem jurídico fundamental, além de outros valores indispensáveis como o patrimônio, a honra, entre outros, e assim foi feito perante a Constituição Federal em seu artigo 5º, inciso X.[20]

Logo, é possível o entendimento de que a inviolabilidade das informações decorre do direito à privacidade, previsto em nossa Constituição Federal e deve ser reconhecida como bem jurídico de natureza essencial para que possa existir a convivência em sociedade.

Alguns doutrinadores que estudam esse tema em questão dizem que a expressão “dados” que traz o artigo da Carta Magna supracitado já protege a não violação dos dados informatizados.

A não violação das informações computadorizadas, aquelas armazenadas em sistemas de computadores, deverá ser tutelada com o surgimento de um novo bem jurídico a ser tratado pelo Direito Penal, para que a integridade e privacidade dos dados informáticos possam ser protegidos.

Depois de finalmente ser reconhecida a presença de um bem jurídico que também merece proteção, é sabido que existe crime sob o aspecto material e que uma omissão normativa não basta para que possa ser descaracterizado como objeto de estudo do Direito Penal, que o reconhece sob o aspecto material.

---

[19] PRADO, Luiz Regis. *Curso de Direito Penal Brasileiro*: parte geral. 2ª ed. rev., atual. e ampl. São Paulo: Editora Revista dos tribunais, 2000. p. 632.

[20] “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.”

A prática deste crime pela Internet é um novo modo de ilícito penal, onde não ocorre a aplicação dos meios tradicionais de prática criminosa, como contato físico com a pessoa, visto que este crime é praticado à distância.

Para melhor entendimento de como este crime ocorre, devemos entender como funciona a estrutura das redes.

A internet é uma interligação de sistemas de comutadores e, para que essa comunicação de dados seja possível, existe uma regulamentação do tráfego de dados, que se chama “protocolo”.

Cada computador ou dispositivo móvel com acesso à rede tem um número de protocolo, chamado de IP[21], que é nada mais do que um endereço que identifica qual máquina ou dispositivo de um sistema está acessando a rede.

O acesso pode acontecer em diferentes camadas. Quando entro em uma página, posso ter acesso somente à leitura, reprodução de vídeos, à escrita, ou a todos. Tudo isso depende da autorização de acesso que tenho ao entrar em um site. Esse acesso é legítimo. Contudo, se “forço” a minha entrada em camadas as quais não tenho permissão, meu acesso passa a ser ilegítimo.

Importante frisar que em todo sistema computacional existe uma pessoa responsável, que é quem administra um site, por exemplo. Esta tem amplos poderes para acessar todos os níveis de informação, mas não para cometer atos irregulares. Por exemplo: um administrador de sistema de um site de e-mails tem acesso a todas as contas dos usuários, mas somente pode ter esse acesso para garantir o pleno funcionamento do sistema, e nunca para causar dano a outra pessoa ou para simplesmente saciar a sua curiosidade.

Hoje em dia o acesso não autorizado é muitas vezes permitido por um descuido da própria vítima, por exemplo, quando visita páginas *fake*, ou seja, de mentira, acreditando serem elas as verídicas, ou até mesmo no golpe do *WhatsApp*, em que a pessoa desavisada acaba deixando, descuidadamente, que tenham acesso ao seu aplicativo, viabilizando que os criminosos apliquem golpes em terceiros.[22]

O ordenamento jurídico pátrio ainda não incriminou o acesso não autorizado de sistemas informáticos e, além de grave, parece ser apenas um caminho do crime para a

[21] *Internet Protocol.*
[22] Procon de São Paulo alerta para golpe que faz clonagem no WhatsApp. < https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/procon-de-sao-paulo-alerta-para-golpe-que-faz-clonagem-do-whatsapp, acesso em 20/04/2021>.

realização de condutas que podem gerar um prejuízo posterior, muito mais grave que somente acessar sem autorização.

Apesar de nosso ordenamento não ter incriminado essa conduta, há uma menção no que diz respeito ao acesso ilegítimo, que se verifica no campo do Direito Eleitoral, mais precisamente na Lei 9.504/97:

> "Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos:
> I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; (...)."

O artigo supracitado tipificou o acesso ao sistema computacional, mas apenas com o objetivo de interferir na contagem dos votos eleitorais, não tendo previsão para acessar outros sistemas, que não sejam relacionados, portanto, ao âmbito eleitoral.

O acesso é tratado no ordenamento, mas a desautorização não é mencionada, como é possível ver nos artigos 313-A e 313-B do CC (Código Penal, 1940):

> 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.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Ambos os artigos dizem respeito ao acesso a um sistema, mas não falam sobre a não autorização. Tratam, em verdade, da má gestão do acesso permitido.

3.2.2. Transferência e obtenção ilegal de dados

Até antes da publicação da Lei 13.709/2018, a LGPD[23], o Brasil não tinha tratamento a respeito deste tema, tendo apenas um Substitutivo o PL n. 84/99, que previa a criação do artigo 285-B do CP, para coibir a obtenção ou que dados fossem transferidos dado ou de informação:

[23] Lei Geral Sobre a Proteção de Dados.

> Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:
> Pena – reclusão, de 1 (um) a 3(três) anos, e multa.
> Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Acontece que este Substitutivo não vingou e, posteriormente, mais precisamente em 2018, foi publicada a LGPD, que diz respeito sobre o tratamento de dados pessoais, que trouxe consigo normas de como esses dados devem e podem ser guardados por pessoas físicas e empresas.

Com isso, esta Lei tem o objetivo de resguardar os direitos de privacidade, liberdade e do livre desenvolvimento da personalidade da pessoa natural.

Em tudo o que fazemos na internet, existe coleta de dados nossos em bancos de dados que armazenam informações pessoais como cidade, profissão, interesses pessoais, nome, e-mail e outros dados que são coletados pelas empresas como o Facebook, ou outra rede social e site.

Esses dados têm enorme valor econômico para essas empresas da tecnologia, porque podem dar um rumo, ou seja, servir de guia para que empresas e políticos usem essas informações como estratégia para ganhar até mesmo uma eleição, por exemplo.

Com esse cenário conturbado, foi necessária a criação de regulamentação para essa atividade de coleta e divulgação de dados pessoais, para coibir a violação dos direitos humanos, como os citados acima.

Importante salientar que essa preocupação não ocorre apenas no âmbito nacional, mas no internacional também, porque que em 25/05/2018 começou a vigorar a GPDR (sigla em inglês), ou, “Regulamento Geral de Proteção de Dados” que é uma legislação feita pela União Europeia que serviu de base para a elaboração da nossa Lei pátria e fixou regras e normas para como os órgãos públicos e as empresas devem enfrentar os dados pessoais.

3.2.3. Dano Informático

O dano é definido pelo artigo 163 do CP (Código Penal, 1940):

> “Destruir, inutilizar ou deteriorar coisa alheia:
> Pena – detenção, de um a seis meses, ou multa.”

Há muita discussão a respeito da aplicação desse tipo penal também no meio da tecnologia, sobre a sua possível aplicação aos danos causados em dados informáticos.

O que mais se percorre a respeito deste tema é sobre o objeto material deste crime. A doutrina aceita o ilícito jurídico contra coisas imóveis e móveis, mas há divergências quando se questiona o aspecto imaterial das coisas.

Não resta dúvida de que a transgressão acima mencionada é aplicável aos objetos materiais, como ao monitor do computador, ao teclado, ao mouse, à impressora e outros, pois são todos objetos materiais, palpáveis, carregados de valor econômico.

O cerne da questão diz respeito aos objetos imateriais, que não são palpáveis, como, por exemplo, um vírus enviado a alguém que causou dano irreparável aos seus arquivos digitais. Estariam esses objetos danificados também respaldados pelo mesmo ilícito jurídico de dano que é tipificado pelo artigo 163 do CP?

Ao redigir o artigo acima citado, o legislador não levou em conta o dano informático, logo, escreveu pensando em “coisa”, sempre, como algo material, palpável.

Não é viável fazer a interpretação de uma norma aumentando os limites da legalidade dados pelo legislador. Em suma, “coisa material” tem que ser lida de maneira diferente de “coisa imaterial”, tanto que foi criado o §3º do artigo 155, CP, para equiparar a energia elétrica a um objeto móvel.

Por esse motivo, quem causa dano a dados informatizados (objeto imaterial), não incorre neste tipo penal, que é o caso de alguém que corrompa dados digitais, por exemplo. Mas, por outro ado, se alguém destruir meu computador que arquiva meus dados, por ter destruído um objeto material (computador), incorrerá na prática prevista pelo artigo 163 do Código Penal Brasileiro.

Logo, é de suma importância a alteração legislativa para que sejam tipificados, também, os danos aos objetos imateriais.

3.2.4. Do vírus

Os vírus computacionais são também conhecidos como *malwares*, que é a junção de duas palavras inglesas: *malicious* que quer dizer malicioso e *softwares*, vindo a significar *softwares* maliciosos. São, em suma, programas de computadores que têm a função de danificar equipamentos alheios ou às próprias pessoas que os utilizam.

Esses programas usados para fazer o mal podem causar apenas uma mera lentidão ao computador do usuário, mas, se for mais poderoso, pode levar até a destruição completa de arquivos e dados. Eles vão na contramão do que os programas computacionais são feitos para fazer. Em vez de facilitar, ajudar a vida do usuário e melhorar a sua experiência virtual, ele destrói, prejudica e atrapalha.

Os vírus são disseminados e espalhados pela rede e podem ser um novo tipo de espécie de perturbação da tranquilidade; com isso em mente, o legislador, no artigo 154-A, §1º do Código Penal, diz que se um dispositivo informático alheio e que esteja conectado à Internet for invadido, desde que frente uma violação indevida do sistema de segurança para que obtenha, adultere ou destrua dados ou, até mesmo, informações desde que não permitidas pelo titular do dispositivo ou instalar programas para que consiga obter algum tipo de vantagem ilícita, obterá pena de detenção de 3 meses a um ano, somado de multa.

O parágrafo 1º deste mesmo artigo ainda diz que comete o mesmo delito quem produzir oferecer, vender, distribuir ou oferecer programa ou dispositivo de computador com o fim de permitir uma infração.

O §1º do artigo 154-A do CP tem a função de tornar crime a conduta dos que oferecem, produzem, distribuem, vendem a outras pessoas ou que somente difundem os programas computacionais com a função de invadir computadores ou dispositivos móveis no geral ou, ainda, instalar neles vulnerabilidade.

O legislador, então, tem a ideia de punir quem realiza as condutas supracitadas do artigo 154, §1º, que têm como objetivo ter acesso a informações e dados que os possam fornecer vantagens ilícitas.

Logo, com base nisso, a conduta somente estará tipificada se o sujeito ativo produzir, oferecer, distribuir, vender a pessoas alheias ou difundir programas ou dispositivos eletrônicos para ter, destruir ou adulterar informações e dados ou adulterá-los sem que seja autorizado pelo dono do aparelho ou instalar nele vulnerabilidades.

Um fato engraçado é que a divulgação de vírus com para fim de espionagem não é tipificada por este tipo, por exemplo.

Este é mais um exemplo da omissão do legislador ao não adequar de forma correta a proteção a que ele se propôs, visto que, além disso, a pena cominada a este crime em particular é super pequena e irrisória.

3.2.5. Engenharia social

A engenharia social aqui é definida como uma ação em que o próprio usuário da Internet é conduzido e induzido a realizar alguma atividade perigosa no meio digital, se colocando em risco.

Por armadilhas, o agente delitivo acaba por convencer o usuário - que muitas vezes age sem a devida prudência – a entregá-lo informações por acreditar que estava apenas fazendo uma tarefa do dia a dia, como o simples preenchimento de um formulário.

Há vários tipos de ataques feitos pela engenharia social, como é o *phishing*[24], que é quando um site engana os seus usuários para que eles os informem dados pessoais, como número do cartão magnético, senhas e números de telefone, por exemplo, ao imitarem o comportamento e aparência de um site de credibilidade (como um site bancário, site do governo, entre outros).

A engenharia social pode ser levada à caracterização de estelionato, mas, quando for adicionada à invasão de computador e prejuízo deste, pode configurar outros tipos criminais, como dano ou até mesmo a ofensa a direitos autorais.

Estelionato, porque, com a conquista das senhas e códigos pessoais, é levada a uma vantagem econômica por quem realiza o crime que se utiliza da engenharia social paralevar o usuário a erro e, com a obtenção desses dados, o criminoso faz saques bancários, compras online, entre muitas outras coisas.

Quando há vantagem indevida, fraude e prejuízo alheio restará configurado o tipo penal de estelionato, conforme com o artigo 171 do CP (Código Penal, 1940):

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
> Pena – reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Entretanto, apenas fazer circular mensagens fraudulentas não é, pelo nosso ordenamento, considerado fato típico, porque não houve a aquisição de vantagem ilícita.

Houve o Substitutivo ao PL nº. 84/99 que previa a criação do estelionato eletrônico na qual se propunha a adicionar um inciso ao §2º do artigo 171 do Código Penal com o objetivo de punir quem propagasse código malicioso com a intenção de tornar mais fácil ou

[24] É um neologismo da palavra *fishing*, que significa pescar em inglês, referindo-se ao ato de que o sujeito passivo “morda a isca”, ou seja, caia na armadilha.

permitir acesso descabido a sistema informático, devendo esta pessoa cumprir as mesmas penas previstas no caput.

Com isso, apenas mandar um e-mail ou mensagens em geral que possam transmitir fraudes já pode ser tipificado como crime. Logo, se houver o provimento de dados particulares e, posteriormente, uma vantagem indevida seja obtida, já se teria configurado o crime de estelionato, conforme o artigo 171 do Código Penal e a Súmula 17 do STJ[25].

Com essa alteração legislativa, a engenharia social já seria passível de punição como uma figura típica, mesmo que com ela não viesse junto um prejuízo econômico necessariamente. Havendo, ter-se-ia configurado o estelionato.

Tratar da engenharia social é de suma importância porque diz respeito a um ilícito formal, o qual não depende do resultado, ao contrário do estelionato, que é um crime material, ou seja, só resta configurado com a obtenção do resultado previsto no tipo penal, qual seja ter, de fato, uma vantagem ilícita.

O que deveria ser feito é a implantação de um parágrafo no artigo 171 do Código Penal com uma redação que equipare a engenharia social à de estelionato, tipificando-a como um crime formal.

3.3. CRIMES DIGITAIS IMPRÓPRIOS

Os crimes digitais impróprios, como já ditos anteriormente, são os crimes realizados usando o computador para de um delito que já é tipificado por nosso Código. Referem-se, portanto, aos crimes já praticados e conhecidos, mas aqui são praticados através de um novo modus operandi, sendo este a tecnologia.

Segundo o jurista e professor Damásio de Jesus (2012):

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço “real”, ameaçando ou lesando outros bens, não computacionais ou diversos da informática.[26]

Há vários exemplos de crimes digitais impróprios, sendo alguns deles: crimes de ameaça, contra a honra e falsidade ideológica.

---

[25] “Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido”.
[26] JESUS, Damásio E. de. (apud CARNEIRO, 2012, [n.p.]).

3.3.1. Crimes contra a honra

Estes crimes, apesar de já tipificados em nosso Ordenamento, mais precisamente nos artigos 138, 139 e 140 do Código Penal, foram muito difundidos com a tecnologia.

A honra abrange as qualidades da pessoa, que compõe sua autoestima e deve ser protegida, pois traz consigo o valor social da pessoa dentro de um ambiente de onde ela vive.

Quando há calúnia, por exemplo, é atribuído a alguém uma falsa acusação de um fato criminoso que não foi cometido por ela. Um exemplo do crime de calúnia no meio digital é mandar, pelo WhatsApp, que certa pessoa cometeu um determinado crime sabendo-se que é mentira. Isso é feito com a finalidade de prejudicar a autoestima e a honra da pessoa vítima.

Quanto a difamação, tem-se a incumbência de uma conduta ofensiva à reputação de alguém, sem que essa conduta seja considerada crime. Um exemplo pode ser alguém postar em uma rede social que determinada pessoa se prostitui com frequência, sabendo que isso é mentira, com o único objetivo de ofender a reputação da vítima.

Nos dois crimes citados, a consumação é dada quando uma terceira pessoa tome conhecimento da ofensa proferida, ainda que o sujeito passivo em si ainda não saiba.

O crime de injúria, que é o tipo que ofende o decoro ou a dignidade de alguém, atingindo a sua honra subjetiva. Afeta as características morais, físicas ou intelectuais do ser humano, ofendendo, falando mal. Com isso, diferente dos dois crimes supracitados, a injúria só se consuma quando o agente passivo em si tomar conhecimento da ofensa proferida a ela. Um exemplo deste crime é mandar mensagens eletrônicas que falam de características negativas da pessoa, como chamá-la de gorda, imbecil...

Há também o crime de racismo, encontrado na Lei 7.716/89, diz respeito a praticar, induzir ou incitar a discriminação ou preconceito de raça, etnia, cor, religião ou procedência nacional, também teve um aumento significativo de prática no meio digital.

3.3.2. Ameaça

A ameaça, no artigo 147 do Código Penal, considerado crime com um menor potencial ofensivo, consiste na conduta de ameaçar e/ou amedrontar alguém, seja por palavras, gestos ou outros meios e de lhe causar mal grave e injusto. Mandar uma

mensagem, publicar em uma rede social falando, por exemplo: “se cuida, vou te pegar!” já configura este tipo penal.

3.3.3. Induzimento ao suicídio

O suicídio nunca foi tipificado em nosso Ordenamento Jurídico, tanto na forma consumada quanto na tentativa. O que é punível, entretanto, é a participação no suicídio.

É punido quem induz o cometimento ao suicídio, dando a ideia de fazê-lo, ou instiga, reforçando a ideia já existente na pessoa. Vai responder, portanto, quem auxilia moralmente (com palavras) ou auxilia na própria execução (emprestando ou facilitando o acesso a materiais e ferramentas que possam auxiliar a pessoa a tirar a vida própria).

Este crime é previsto pelo artigo 122 do Código Penal que teve a sua redação estendida recentemente, em 2019, com a Lei 13.968/19. [27]

No meio digital, este crime pode ser feito por pessoas que criem ou participem de comunidades ou fóruns, por exemplo, e que façam postagens auxiliando como tirar a própria vida ou, até mesmo, fazendo postagens que incentive alguém a isso, como falando “o mundo seria bem melhor sem você”, entre outras.

[27] Também conhecida como Pacote Anticrime.

4. CAPÍTULO 3 – CRIMES DIGITAIS NO ÂMBITO INTERNACIONAL E NO BRASILEIRO – MUDANÇAS NECESSÁRIAS

4.1. LEGISLAÇÃO AO REDOR DO MUNDO

Os países ao redor do mundo, por volta de 1970, começaram a tratar e reformar suas legislações com assuntos a respeito de crimes digitais visto que, até metade do século XX, as normas e códigos penais tratavam de bens e coisas tangíveis e materiais, ou seja, palpáveis.

Mais para o final do século XXI, os bens incorpóreos começaram a ter impacto e lugar no mundo, precisando, portanto, de novas formas de proteção legislativa, vindo e ser necessário à criação de novas medidas.

Os ordenamentos jurídicos, em um geral, ao redor do mundo, criaram e adaptaram suas legislações para que possam punir esse tipo de crime. Vejamos alguns exemplos de países e algumas de suas mudanças neste aspecto:

4.1.2. Portugal

Em Portugal, os crimes digitais começaram a ser tipificados por influência da recomendação R (89) 9 do Conselho da Europa, com a chegada da Lei 109/91 que começou a punir os “crimes informáticos”. Esta Lei também era conhecida como Lei de Criminalidade Informática e foi muito útil e eficaz, mas, depois de decorrido um certo tempo, ela não abrangia outras novas práticas que começaram a ser feitas com o avanço da tecnologia.

Com isso, foi revogada pela Lei 109/2009[28], também conhecida como Lei do Cibercrime, que abrangeu novas condutas, como a difusão ou produção de vírus, que não estava na Lei de 1991.

[28] “A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.”, <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis>, acesso em 28/06/2021.

Além disso, Portugal, em 2001, assinou a Convenção Sobre Cibercrime do Conselho da Europa, que é o primeiro e mais importante trabalho internacional sobre crime no espaço virtual.

4.1.3. França

Alterou seu Código Penal em janeiro de 1988 através Lei 88-19 que teve a finalidade de repreender atentados contra os sistemas informáticos e foi a primeira Lei francesa que pune certos crimes informáticos e de pirataria.

Após, em 1995, a Lei citada foi revogada porque houve a atualização do Código Penal Francês, que começou ter dois artigos, 323-1 a 323-7, que tratavam de crimes informáticos.

O artigo 323-1 do Código Penal francês passou a punir a atitude de manter-se de forma fraudulenta ou acessar um sistema de tratamento informático de dados.

Por outro lado, o artigo 323-2 passou a tornar crime conduta de colocar vírus em um sistema informático. Outro artigo, o 323-4, por exemplo, trata de reprimir a associação criminosa para que alguma conduta, como a implantação de vírus, seja preparada.

Importante frisar que a França, com sua Lei n. 78-17, do ano de 1978, foi um dos primeiros países a tratar sobre criminalidade informática.

4.1.4. Itália

Em 1993, o Código Penal italiano[29] começou a tratar de crimes informáticos, como pode ser visto em alguns artigos, como o 615 que trata, dentro da inviolabilidade de domicílio, a respeito da punição para quem acesse de forma abusiva o sistema telemático ou informático.

Outro exemplo pode ser o artigo 635 que pune o dano ao sistema telemático e informático, e pune a deterioração, destruição ou a inutilização deles ou de algum outro dado diferente.

Além desses e muitos outros artigos, a Itália tratou em sua legislação, já em 1991, sobre o uso abusivo de cartões magnéticos, no seu artigo 12 da Lei n. 197 de 1991.

---

[29] *Codice penale italiano.* Disponível em: <https://it.wikipedia.org/wiki/Codice_penale_italiano>. Acesso em 08/07/2021.

4.2. LEIS NO ÂMBITO BRASILEIRO

O Brasil, apesar de demora, agora conta com algumas – poucas – normas que tornam crimes apenas algumas condutas, sendo elas: as Leis Ordinárias 12.735/2012 e 12.737/2012, a Lei 12.965/2014, também conhecida como Marco Civil da Internet e, mais recentemente, o projeto de Lei 4.554/2020, o qual foi transformado na Lei Ordinária 14.155/2021.

A primeira lei supracitada fez algumas modificações a respeito da Lei de Crimes Raciais, fazendo com que o juiz possa permitir, até mesmo antes da instauração de um inquérito policial, ordenar que não sejam exibidos símbolos ou imagens que remetam à discriminação. Essa lei trouxe consigo uma violação a parâmetros constitucionais, mais claramente ao citado no artigo 5º da Constituição Federal, que diz que "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória", sabendo-se que é obrigação do Estado respeitar todas as fases, ou seja, desde a denúncia até o processamento e julgamento. Ademais, deve-se esperar para que a condenação transite em julgado para, posteriormente, possa aplicar os efeitos penais e extrapenais.

Já a segunda lei citada acima, a 12.737/2012[30], veio para tipificar a invasão de privacidade e tipifica, no âmbito penal, os crimes informáticos que antes não eram considerados crimes. Também alterou um pouco o Código Penal ao adicionar os artigos 154-A e 154-B (Código Penal, 1940):

> O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes artigos 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.
> § 1º 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.

[30] Também conhecida como Lei Carolina Dieckmann.

> § 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."

Ao perceber a oportunidade de invasão, o estado, finalmente, vai começar a punir quem o fizer, levando em conta, por exemplo, o princípio constitucional da privacidade[31] e tem, como principal objetivo, a segurança de aparelhos eletrônicos.

> 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.
> Além de adicionar esses dois novos artigos, também mudou dois artigos que já existiam, o 266 e 298 do Código Penal.
> Art. 266 – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena – detenção, de um a três anos, e multa. Parágrafo único – Aplicam-se as penas em dobro, se o crime for cometido por ocasião de calamidade pública. § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2° Aplicam-se as penas em dobro se o crime e cometido por ocasião de calamidade pública.
> Art. 298 – Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena – reclusão, de um a cinco anos, e multa. Falsificação de cartão.
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

É inegável que o escrito no Código Penal a respeito destas novas criminalizações tem o condão de que quem invada ferramentas de segurança com o objetivo de violar a intimidade no ambiente digital dela, seja devidamente responsabilizado e punido.

O Marco Civil da Internet, também conhecida como Lei 12.965/2014, foi instituído por conta de recorrentes ataques a sites de empresas públicas e oficiais do governo, com a necessidade de tutela da informação. Esta lei, portanto, dispõe a respeito das garantias individuais dos usuários da Internet e os direitos e deveres para que a Internet possa ser utilizada de forma correta em todo território nacional. Sua aprovação dependeu de muito

[31] Artigo 5º, inciso X da Constituição Federal: *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação".*

debate, porque coloca em jogo e discussão conceitos e princípios como o de privacidade e liberdade individuais.

Depois que a referida lei foi finalmente publicada, vários fatores que dizem respeito à privacidade foram trazidos à tona, como os provedores de Internet serem obrigados a manterem os registros das conexões pelo prazo de 1 ano e de 6 meses, quando se diz respeito ao histórico de acesso.

Além de estabelecer esta obrigatoriedade no que diz respeito aos provedores de internet, a Lei 12.965/2014 também foi responsável por beneficiá-los, pois transfere ao usuário qualquer e toda responsabilidade sobre conteúdo produzido e consumido, menos os difundidos em redes sociais, cabendo ao provedor, neste caso, retirar o conteúdo do ar e, se não cumprir, poderá responder na justiça.

Também foi o Marco Civil o responsável por instituir que são os Juizados Especiais os responsáveis por decidir a respeito de se os conteúdos são ou não ilegais, aplicando-se na injúria ou ofensa à honra, que vão ser tratados da mesma maneira que ocorre quando é cometido sem o uso da tecnologia.

A competência é fixada sem depender do lugar do provedor, sendo levado em conta o lugar onde o delito foi, de fato, consumado, conforme o artigo 70 do Código de Processo Penal.[32]

Por outro lado, a competência será da Justiça Federal quando forem cometidos crimes em que haja violação de privacidade ou atos que atinjam bens, interesse ou serviço da União ou se suas empresas públicas ou autárquicas.

Finalmente, o Projeto de Lei nº. 4.554/2020, apresentado em 07/12/2020, agora transformado em Lei Ordinária nº. 14.155/2021 mudou o Código Penal Brasileiro e criou o crime de furto qualificado por meio da fraude com a utilização de aparelhos eletrônicos fornecidos de forma indevida, com o acréscimo de pena quando quem sofre a ação é pessoa de idade avançada ou é utilizado algum servidor de rede em outro país e, com isso, seja possível tornar mais grave os tipos penais de violação de aparelho informático, furto e estelionato, desde que sejam cometidos pela Internet ou de forma eletrônica.

Além disso, deseja também alterar o Código de Processo Penal para prever a competência dos crimes cometidos através da internet ou de forma eletrônica pelo lugar de residência da vítima.

---

[32] Artigo 70 do Código de Processo Civil. *“A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.”*

Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
.....
§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
§3º .....
Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
.....(NR)
Art.155. .....
.....
§ 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável ..... (NR)
Art.171.....
.....
Fraude eletrônica
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
.....
Estelionato contra idoso ou vulnerável
§ 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.
.....(NR)
Art. 2º O art. 70 do Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), passa a vigorar acrescido do seguinte § 4º:
Art.70.....
.....§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.” (NR)
Art. 3º Esta Lei entra em vigor na data de sua publicação.

4.3. DA NÃO SUFICIÊNCIA DAS NORMAS ESPECÍFICAS

É por óbvio que as leis acima citadas não são suficientes para abranger todos os tipos de crimes digitais, englobando apenas e tão somente uma pequena parcela deles. Com isso em mente, deve ser perguntado até quando o legislador se utilizará de uma legislação genérica como analogia para tentar combater esses tipos de crimes.

Deve-se ter em mente e levar em consideração que há um nível e índice muito grande de impunidade no que se diz respeito aos crimes digitais, justamente por esses crimes praticados nesse ambiente digital garantirem um maior anonimato a quem o pratica, ser mais difícil, às vezes, de se saber quem é competente para julgá-los, e por causa da falta de leis próprias para tipificar estes crimes, somado com as lacunas e obscuridade presentes nas escassas leis que já existem.

Com o passar do tempo, a tecnologia se desenvolve, avançando e conseguindo, vertiginosamente, um número maior de usuários, ainda mais quando levamos em conta o tamanho continental do Brasil, restando latente a necessidade de que haja uma legislação mais específica para tratar desse assunto.

Tudo isso fica muito mais claro e evidente quando levamos em consideração que o nosso Código Penal data do ano de 1940, sendo óbvia a necessidade de atualizá-lo, já que naquela data não existia e não se vislumbrava existir estes tipos penais cometidos no meio digital.

4.4. PROCESSO E JULGAMENTO

Quando um crime digital acontece, deve ser, primeiramente, verificada a extensão deste, ou seja, onde ele aconteceu. Acontece que, como citado acima, às vezes é difícil que a localização exata seja determinada para que, posteriormente, seja decidida quem é competente para o julgamento do crime.

Frente a isso, diversos usuários registram seus sites em servidores de países diversos de onde, de fato, residem. Com isso, pode-se residir em um determinado país e pratique crime em outro distinto.

Muitos aspectos hão de ser considerados no que diz respeito a qual lei deve, de fato, ser aplicado, como observar o endereço eletrônico, o onde a vítima tem como seu domicílio, o lugar aonde a conduta veio a se consumar ou, se não consumou, gerou efeitos, entre outros.

Na legislação pátria, os artigos 5º e 6º do Código Penal ditam qual a competência onde que os crimes praticados no ambiente digital possam ser processados e julgados.

> Art. 5º – Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
> Art. 6º – Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se oresultado.”

Com isso, torna-se evidente que o ordenamento jurídico brasileiro adaptou a teoria da ubiquidade, que “considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado” (Lei 7.209/84, , no modo onde os crimes cometidos por brasileiros vão ter sobre si incidida a lei brasileira, independente de terem ou não acontecido em território nacional.

5. CONCLUSÃO

Como já dito várias vezes, os crimes na esfera virtual acontecem muito mais rapidamente do que os outros delitos normais, mas há a percepção de que a punição e a investigação destes tipos não existem, dada a lentidão do sistema como um todo e que, com toda essa morosidade, exista um “incentivo” para a prática destes crimes.

Tudo isso poderá melhorar quando houver uma maior velocidade na expedição e cumprimento de mandatos, maior velocidade no âmbito da perícia e, principalmente, que a legislação seja modificada e atualizada – como já deveria ter sido há tempos - para melhor atender estas soluções e que, além disso, exista uma união entre as forças de segurança pública.[33]

É perceptível que o Direito Penal pátrio ainda não está preparado como deveria para lidar com esses tipos penais que são praticados por meio da internet ou que surgiram apenas após a invenção desta.

Houve, sim, mudanças bem-vindas em nosso ordenamento, mais precisamentenos últimos anos, mas ainda não é o suficiente para acabar, ou, ao menos, coibir com queesses crimes sejam praticados.

Além de ser necessário que nossas leis sejam atualizadas ou modificadas, deve haver uma maior harmonização entre os países ao redor do mundo para que essas atividades sejam mais cercadas, por conta destes crimes terem caráter transnacional.

Por fim, é necessária, também, uma espécie de conscientização para com a população geral, visto que muitos golpes podem ser evitados se a pessoa utilizando a Internet prestar mais atenção ou tiver um pouco mais de cuidado ao entrar e navegar em sites.

[33] TEIXEIRA, Ronaldo de Quadros. Os Crimes Cibernéticos no Cenário Nacional. Escola superior aberta do Brasil – ESAB, 2013.

6. REFERÊNCIAS

Artigo 155 do Decreto Lei nº 2.848 de 07 de Dezembro de 1940. **JusBrasil.** Disponível em: <https://www.jusbrasil.com.br/topicos/10619836/artigo-155-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940>. Acesso em 16/06/2021.

BAPTISTA, Rodrigo. Lei com penas mais duras contra crimes cibernéticos é sancionada. **Senado noticias, 2021.** Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada>. Acesso em 12/07/2021.

CARNEIRO, Leandro Dias. Infrações penais e a informática: a tecnologia como meio para o cometimento de crimes. **Jus.com.br, 2016.** Disponível em: <https://jus.com.br/artigos/52698/infracoes-penais-e-a-informatica-a-tecnologia-como-meio-para-o-cometimento-de-crimes>. Acesso em 15/06/2021.

CARVALHO, Ítalo. Tentativa de suicídio é crime? **Jus.com.br, 2016.** Disponível em: <https://jus.com.br/artigos/46581/tentativa-de-suicidio-e-crime>. Acesso em 23/06/2021.

CONECTA, Blog. Para que serve o endereço de IP? **Copel Telecomunicações, 2021.** Disponível em: <https://www.copeltelecom.com/site/blog/siteblogpara-que-serve-o-endereco-de-ip/#:~:text=O%20endere%C3%A7o%20IP%20%C3%A9%20um,por%20um%20protocolo%20de%20internet.&text=A%20sigla%20IP%20significa%20Internet,nossa%20l%C3%ADngua%2C%20protocolo%20de%20internet>. Acesso em 14/04/2021.

CRESPO, Marcelo. Crimes digitais: quais são, quais leis os definem e como denunciar. **São Paulo: Editora Saraiva, 2011.** Disponível em: <https://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/>. Acesso em 12/07/2021.

CRESPO, Marcelo. Crimes digitais e os vírus computacionais. **JusBrasil, 2015.** Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/artigos/242725800/crimes-digitais-e-os-virus-computacionais>. Acesso em 17/06/2021

EBOLI, Marisa. O hacker como carreira profissional. **Estadão, 2021.** <https://economia.estadao.com.br/blogs/radar-do-emprego/o-hacker-como-carreira-profissional/>. Acesso em 16/06/2021.

ESCOLA, Equipe Brasil. Internet, a história da Internet, surgimento da Internet, a Internet no Mundo, o que é internet, o surgimento da internet no Brasil, a internet no Brasil.. **Monografias Brasil Escola.** Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/internet.htm>. Acesso em 14/04/2021.

IZALCI, Lucas. Projeto de Lei 4554/2020. **Câmara dos Deputados, 2020.** Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266148>. Acesso em 30/06/2021.

Lei do cibercrime. **Procuradoria Geral do Distrito de Lisboa, 2009.** Disponível em: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis&ficha=1&pagina=1&so_miolo=>. Acesso em 28/06/2021.

MACEDO, Herivelto Raimundo L. Surgimento E Evolução Da Internet No Brasil. **Eletronet, 2017.** Disponível em: <https://www.eletronet.com/surgimento-e-evolucao-da-internet-no-brasil/>. Acesso em 14/04/2021.

MARINHO, Guilherme. Hackers, Crackers e o Direito Penal. **JusBrasil, 2016.** Disponível em: <https://grmadv.jusbrasil.com.br/artigos/407334629/hackers-crackers-e-o-direito-penal>. Acesso em 16/06/2021.

MEDEIROS, Gutembergue Silva, UGALDE, Júlio César Rodrigues. Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet. **Âmbito jurídico, 2020.** Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/>. Acesso em 25/06/2021.

NOTÍCIAS, Agência CNJ. Crimes digitais: o que são, como denunciar e quais leis tipificam como crime? **Conselho Nacional de Justiça, 2018.** Disponível em: <https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/>. Acesso em 15/06/2021.

OPNIÃO, A nossa. A nova lei do cibercrime. 2009. **MAI Liberdade e segurança, 2009.** Disponível em: <https://opiniao.mai-gov.info/2009/10/02/a-nova-lei-do-cibercrime/>. Acesso em 28/06/2021.

PONTES, Sergio. O que fala a lei geral de proteção de dados pessoais. **JusBrasil.** <https://sergiopontes.jusbrasil.com.br/artigos/614642198/o-que-fala-a-l//ei-geral-de-protecao-de-dados-pessoais>. Acesso em 23/06/2021.

REPÚBLICA, Presidência. Constituição da república federativa do brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 16/06/2021.

REPÚBLICA, Presidência. Lei nº 12.737, de 30 de novembro de 2012. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 30/06/2021.

RIGUES, Rafael. Mãe da Internet faz 50 anos. Conheça a história da ARPANET. **Olhar Digital, 2019.** Disponível em: <https://olhardigital.com.br/2019/10/24/noticias/mae-da-internet-faz-50-anos-conheca-a-historia-da-arpanet/>. Acesso em 14/04/2021.

SÃO PAULO, Folha. Viciados em internet são atendidos em SP. **Portal do governo, 2008.** Disponível em: <https://www.saopaulo.sp.gov.br/spnoticias/na-imprensa/viciados-em-internet-sao-atendidos-em-sp/>. Acesso em 14/04/2021.

SOUZA, Ludmilla. Procon de São Paulo alerta para golpe que faz clonagem do WhatsApp. **Agencia Brasil, 2020.** Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/procon-de-sao-paulo-alerta-para-golpe-que-faz-clonagem-do-whatsapp>. Acesso em 06/07/2021.

SOUZA, Jéssica da Silva. Desemprego: reflexo do mundo globalizado. **Conteúdo Jurídico, 2012.** Disponível em: <https://www.conteudojuridico.com.br/consulta/Artigos/30252/desemprego-reflexo-do-mundo-globalizado>. Acesso em 19/04/2021.

VIANNA, Túlio Lima. Do delito de dano e de sua aplicação ao Direito Penal informático. **Jus.com.br, 2004.** Disponível em: <https://jus.com.br/artigos/5828/do-delito-de-dano-e-de-sua-aplicacao-ao-direito-penal-informatico>. Acesso em 16/06/2021.

WIKIPEDIA. Tecnologia da informação. Disponível em: <https://pt.wikipedia.org/wiki/Tecnologia_da_informa%C3%A7%C3%A3o>. Acesso em 14/04/2021.

WIKIPEDIA. Bitnet. Disponível em: <https://pt.wikipedia.org/wiki/BITNET>. Acesso em 14/04/2021.

WIKIPEDIA. Lei Carolina Dieckmann. Disponível em: **<**https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann>. Acesso em 15/06/2021.

WIKIPEDIA. Hacker. Disponível em: <https://pt.wikipedia.org/wiki/Hacker>. Acesso em 16/06/2021.