São Paulo, Brazil
October 29-30, 2018

The Tenth International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2018011or http://dx.doi.org/10.5769/C2018011

Crimes Eleitorais Cibernéticos nas Campanhas Eleitorais Pela Internet

Paulo Quintiliano[1]

(1) IPOG and QUINTILIANO ADVOCACIA
Email: paulo.quintiliano@hotmail.com, www.quintiliano.adv.br

Abstract: Neste artigo são abordadas várias questões relacionadas com o Direito Cibernético e suas conexões com o Direito Eleitoral, incluindo-se as *fake news* e os crimes eleitorais praticados por meio da internet. Nesse contexto, as provas digitais e as investigações cibernéticas são abordadas, com a apresentação de técnicas para identificação e localização de responsáveis por publicações apócrifas, com conteúdo ofensivo, podendo ser criminoso. A Computação Forense é abordada como importante área do conhecimento para a constituição de provas periciais, com base nas evidências digitais encontradas, para efeito de identificação dos autores das condutas investigadas.

Key words: Direito Cibernético, Direito Eleitoral, Computação Forense, fake News, investigação cibernética.

I. Introdução

O Direito Cibernético, também denominado Direito Digital ou Direito Eletrônico, está fortemente relacionado com o Direito Eleitoral, sendo que essa conexão se tornou mais forte após as últimas minirreformas eleitorais, que limitaram as possibilidades de financiamento das campanhas eleitorais. Assim, por ser de baixo custo, a internet surge como ótima alternativa para a divulgação das informações das campanhas eleitorais, devendo, em 2018, tornar-se o principal palco das disputas eleitorais. Nesse contexto, certamente surgirão muitas questões que demandarão investigações cibernéticas e perícias em Computação Forense, para efeito de constituição de provas digitais com a finalidade de comprovar a materialidade, a dinâmica e a autoria das condutas, bem como será demandada a atuação de advogados especialistas em Direito Cibernético e peritos especializados em Computação Forense para darem tratamentos adequados a essas questões tecnológicas associadas ao Direito Eleitoral.

Neste artigo serão abordados os aspectos relacionados com essas duas áreas do Direito, explorando-se as questões voltadas para a investigação cibernética, com a finalidade de se proporem alternativas para a solução dos casos de ataques contra candidatos, por meio da internet, especialmente com o uso das redes sociais, por meio de perfis falsos, com o objetivo de alterarem fraudulentamente dos resultados das eleições. São estudados os principais meios de provas utilizados em investigações cibernéticas, bem como são tratadas as questões relativas à constituição de provas digitais.

Esses ataques normalmente consistem na prática de divulgação de informações falsas,

mais conhecidas como “fake news”, cujo conteúdo muitas vezes pode ensejar o enquadramento do autor em crimes eleitorais, durante as campanhas eleitorais, principalmente nos crimes contra a honra (calúnia, difamação e injúria), previstos no Código Eleitoral. O autor das notícias falsas também pode responder civilmente, mediante a propositura de ações de reparação de danos morais e materiais. São apresentadas técnicas de investigação cibernética, incluindo-se os exames periciais de Computação Forense, necessários para a identificação e a localização de criminosos que atuam por meio do espaço cibernético, especialmente com a finalidade de atacarem adversários políticos, buscando interferirem fraudulentamente nos resultados das eleições, em proveito próprio ou de candidatos apoiados.

Os crimes eleitorais próprios, previstos na lei eleitoral, são estudados sob perspectiva da possibilidade de serem praticados com a utilização dos recursos da Informática, especialmente a internet. Nessas hipóteses, tais crimes poderiam ser classificados como crimes eleitorais de Informática ou crimes eleitorais cibernéticos, conforme o caso.

2. Direito Cibernético aplicado ao Direito Eleitoral

As provas digitais ganham cada vez maior relevância neste cenário em que a sociedade se tornou dependente da internet e de outros recursos da Informática e, portanto, faz intenso uso desses recursos tecnológicos em suas atividades cotidianas. Muitas dessas atividades podem ser configuradas como crimes praticados por meio do espaço cibernético. Neste cenário, surgem inúmeras situações envolvendo o uso de recursos tecnológicos disponíveis para toda a sociedade que precisam ser tratadas pelo Direito Cibernético, inclusive questões eleitorais.

Também são necessários alguns conhecimentos de Computação Forense, mesmo que elementares, para se trabalhar com esses novos meios de prova. A observação dos requisitos mínimos para se considerar uma evidência digital demandam esses conhecimentos. Assim, o Direito Cibernético precisa do suporte da Computação Forense, perícia de Informática e investigação cibernética para levar a bom termo as ações contenciosas e administrativas.

Ultimamente, as campanhas e pré-campanhas eleitorais utilizam intensamente os recursos da internet, especialmente as redes sociais, para seus propósitos eleitorais, lícitos e ilícitos. É muito comum a ocorrência de postagens nas redes sociais contra candidatos opositores, a partir de perfis falsos, sendo normalmente notícias falsas, muitas vezes criminosas, mais conhecidas como *fake news*. Há também a produção de ataques falsos, muitas vezes perpetrados pela própria pessoa que se apresenta como vítima, com a finalidade de acusar um terceiro suposto interessado por aquela ação, normalmente um adversário político, em que a “prova” do crime é uma mera impressão de uma postagem.

Com efeito, para que se possa dar algum crédito a uma notícia crime dessas, é necessário exigir informações adicionais da postagem, como a identificação da URL do conteúdo criminoso, para não se tornar conivente com uma *fake news*. Por meio da URL, é possível identificar o responsável pela postagem, a partir de investigações a serem perpetradas no espaço cibernético. Definitivamente, simples “prints” não provam nada, pois eles podem ser adulterados facilmente por meio de programas de processamento de imagens ou criados por meio de perfis *fakes*, gerando-se as *fake news*, sendo necessários apenas conhecimentos elementares de Informática para a produção de uma fraude dessas.

Questões como essa precisam ser tratadas pelo Direito Cibernético. Nos casos de investigações não oficiais, é necessária a emissão de Ata Notarial, com a identificação da URL, comprovando-se a materialidade do fato, ressaltando-se que a Ata Notarial é um meio de prova que possui fé pública. Para se determinar a autoria, são necessárias investigações cibernéticas para a busca dos vestígios digitais deixados nos locais da conduta praticada, bem como exames periciais e a emissão dos laudos periciais, para a constituição das provas.

Com certeza, há uma megatendência de a sociedade como um todo, cada vez mais, fazer uso da internet como ferramenta na execução de suas atividades cotidianas. Nesse diapasão, as atividades políticas, tanto aquelas praticadas pelos candidatos como aquelas típicas dos eleitores, estão sendo realizadas com a utilização da internet como ferramenta, em decorrência surgindo muitas situações que precisam ser tratadas pelo Direito Eleitoral e pelo Direito Cibernético, de forma conjunta e colaborativa (RAIS et al., 2018, p. 19).

2.1. Direito Eleitoral

O Direito Eleitoral é classificado como um dos ramos do Direito Público, visto que está intimamente relacionado com os assuntos de interesse do Estado. Conforme ensina CHALITA (2014, pp. 25-28), as fontes do Direito Eleitoral podem ser classificadas em primárias ou diretas, secundárias ou subsidiárias e consultas.

Com a finalidade de buscar uma definição para Direito Eleitoral, pode-se valer da doutrina de GOMES [9]. Segundo esse autor: “Direito Eleitoral é o ramo do Direito Público cujo objeto são os institutos, as normas e os procedimentos regularizadores dos direitos políticos. Normatiza o exercício do sufrágio com vistas à concretização da soberania popular”.

As fontes primárias são: a Constituição Federal, que é considerada a maior fonte do Direito Eleitoral Brasileiro, em seus artigos 14 ao 17 e 118 ao 121; o Código Eleitoral (Lei Nº 4.737/1965) que, após sua recepção pela Constituição Federal, passou a ser classificado como Lei Complementar, embora originariamente seja lei ordinária; Lei das Eleições (Lei Nº 9.504/1997), que estabelece as normas gerais que regulamentam as eleições; Lei Orgânica dos Partidos Políticos - LOPP (Lei Nº 9.096/1995), que estabelece as regras para a organização, criação, fusão e extinção dos partidos políticos; e Lei das Inelegibilidades (Lei Complementar Nº 64/1990), que, em conformidade com o parágrafo 9º do artigo 14 da Constituição Federal, estabelece e especifica as hipóteses infraconstitucionais de inelegibilidade (ALMEIDA, 2017; CHALITA, 2014).

As fontes secundárias são: as resoluções do Tribunal Superior Eleitoral, que são atos normativos emitidos pelo Pleno desse Tribunal, em conformidade com o parágrafo único do artigo 1º e artigo 23 do Código Eleitoral; Consultas, que podem ser feitas ao TSE, relativas a determinada matéria eleitoral; Código Civil; Código de Processo Civil; Código Penal; e Código de Processo Penal (ALMEIDA, 2017; CHALITA, 2014).

Certamente, *a* utilização indevida de veículos ou meios de comunicação social pode se dar por meio do uso de recursos da internet, especialmente das redes sociais. Ressalte-se que essas condutas praticadas por meio da internet podem ter alcance ainda maior, visto que as informações permanecem disponíveis para os eleitores indefinidamente.

RAIS et al. (2018 apud AGÊNCIA BRASIL, 2017) afirmam que o Brasil é o quarto país em número de acesso à internet, perdendo apenas para a China, a Índia e os Estados Unidos da América. RAIS et al. (2018 apud DIGITAL 2017 GLOBAL OVERVIEW, 2017) apresentam estatísticas sinalizando que o Brasil possui 139 milhões de usuários de internet e que a metade da população brasileira acessa a internet por meio de dispositivos móveis e que tais usuários ficam em média 8h56 por dia conectados à grande rede. Com efeito, tais dados demonstram a importância e o grande potencial representado pela internet, inclusive para propósitos eleitorais; fato que, de per si, justifica a grande utilização desses recursos tecnológicos nas campanhas e pré-campanhas eleitorais.

Assim, considerando-se que a internet está sendo cada vez mais utilizada pelos candidatos e pré-candidatos a cargos eletivos para propósitos eleitorais, seguramente poderão ocorrer muitos abusos e utilização indevida desse meio de comunicação social, sendo que tais incidentes demandarão a atuação do Direito Cibernético e da Computação Forense, especialmente nos casos em que os autores dos abusos atuaram por meio de perfis falsos, buscando o anonimato e a impunidade. Nessas situações são necessárias investigações cibernéticas e afastamento do sigilo

telemático dos perfis falsos para a identificação dos responsáveis pelos abusos.

2.2.Direito Cibernético

Há algumas nomenclaturas diferentes para nomearem esse novo ramo do Direito, o qual está intimamente relacionado com a alta tecnologia, representada pelos recursos da Informática, incluindo-se a internet. As denominações mais utilizadas são: Direito Cibernético, Direito Digital, Direito Eletrônico e Direito Informático, sendo sinônimas todas elas. O Direito Cibernético surge a partir dessa forte relação estabelecida entre o Direito e os recursos tecnológicos providos pela Informática, tendo como finalidade tratar as questões que aparecem em decorrência das atividades praticadas pelos usuários desses recursos de alta tecnologia, especialmente quando são realizadas por meio do espaço cibernético.

Principalmente a partir do momento em que a internet se tornou muito popular, que toda a sociedade passou a fazer uso intenso desse recurso tecnológico, tornando-se completamente dependente da alta tecnologia, muitos usuários mal intencionados começaram a praticar atividades criminosas por meio da grande rede. As empresas privadas e organismos governamentais e toda a sociedade de uma forma geral passaram a utilizar a internet em suas atividades cotidianas, de forma intensa. Em razão dessa rápida e constante migração das atividades de toda a sociedade para a internet, muitas questões novas começaram a aparecer, questões essas que precisam ser tratadas pelo Direito Cibernético e pela Computação Forense.

O Direito Cibernético ainda não se estabeleceu como um ramo autônomo do Direito, visto que precisa do suporte de outras áreas do Direito. Dessa forma, está fortemente relacionado principalmente com o Direito Eleitoral, Direito do Consumidor, Direito Penal e Direito Civil.

Nas campanhas eleitorais e pré-eleitorais, os candidatos e pré-candidatos estão utilizando intensamente a internet, especialmente as redes sociais, para buscar seus objetivos eleitorais com mais eficácia e economia. Nesse contexto, surgem muitas questões envolvendo aspectos técnicos da alta tecnologia e eleitorais que precisam ser abordados conjuntamente pelo Direito Cibernético e pelo Direito Eleitoral.

Hodiernamente, é possível comprar qualquer coisa pela internet, até mesmo de países distantes, como a China. Assim, em decorrência do grande volume de compras realizadas por meio da internet, surgem inúmeras questões relacionadas, como compras pagas e não entregues, produtos recebidos com defeitos ou diferentes do anunciado, fraudes em websites de compra e venda de bens, dentre outras. Tais questões precisam ser tratadas pelo Direito Cibernético juntamente com o Direito do Consumidor, com o suporte da Computação Forense.

O crime definitivamente migrou suas atividades ilícitas para a internet, visto que as quadrilhas estão atuando fortemente por meio do espaço cibernético, em busca de mitigar os riscos e aumentar os lucros. Há alguns ataques cibernéticos mais complexos, como aqueles perpetrados por meio de redes de *botnets*, em que os administradores da rede invadem até milhões de computadores ao redor do planeta e, a partir desses computadores invadidos – denominados *bots*, lançam ataques contra alvos certos, sem que os proprietários dos computadores invadidos saibam, com a finalidade de obtenção de vantagens financeiras ilícitas. Os proprietários dessas máquinas invadidas podem ser acusados de crimes que não cometeram, visto que suas máquinas estão sendo utilizadas por criminosos escondidos na imensidão do espaço cibernético para a prática de fatos tipificados com crimes. Esses e tantos outros casos semelhantes precisam ser tratados juntamente pelo Direito Cibernético e pelo Direito Penal, também com o suporte da Computação Forense para efeito de elaboração de exames periciais específicos para a produção de provas demonstrando a inocência do acusado.

Em decorrência da atuação irresponsável de muitos usuários da internet que fazem uso inadequado dos recursos tecnológicos, surgem muitas questões cíveis, especialmente de reparação de danos morais por conta de publicações indevidas nas redes sociais com conteúdo ofensivo à honra das pessoas, com

violação ao direito de imagem, dentre muitas outras situações análogas. Nesse diapasão, essas questões precisam ser trabalhadas pelo Direito Cibernético juntamente com o Direito Civil, apoiados pela Computação Forense, para efeito de produção de provas.

3. Crimes de Informática

Não existe definição legal para crimes de Informática no ordenamento jurídico pátrio. De fato, existem várias nomenclaturas utilizadas para esses crimes que fazem uso dos recursos tecnológicos da Ciência da Computação, como: Crimes de Informática, Crimes Digitais, Crimes de Alta Tecnologia, Crimes por Computador e Crimes Eletrônicos. Definitivamente, todas essas nomenclaturas são sinônimas e querem dizer a mesma coisa, haja vista que todos os crimes de alta tecnologia, digitais e eletrônicos fazem uso de recursos da Informática, principalmente de natureza lógica (programas de computador).

Com efeito, DE LUCA et al. (p. 240), no ano distante de 2005, esboçaram uma definição para crimes de Informática, seguramente baseando-se na teoria tripartite do crime, para propor uma definição para crimes de Informática.

De fato, para se chegar a uma boa conceituação de crimes digitais, deve-se partir do conceito analítico de crime, com base na teoria tripartite, em que “crime é todo fato típico, antijurídico (ilícito) e culpável”. A partir dessa definição, pode-se conceituar crimes de Informática como sendo “todo fato típico, antijurídico e culpável, praticado com a utilização de recursos da Informática”. Como essa proposta de definição se baseia em teoria consolidada e respeitada (teoria tripartite), tende a ser robusta.

Os Crimes Cibernéticos, por sua vez, são espécie do gênero Crimes de Informática. Essa espécie de crimes digitais são os crimes praticados por meio do espaço cibernético (internet), que é um dos recursos da Informática. Assim, mais uma vez baseando-se na teoria tripartite, crimes cibernéticos podem ser definidos como “todo fato típico, antijurídico e culpável, praticado com a utilização de recursos da Informática, por meio do espaço cibernético”. Dessa forma, todo crime cibernético é crime de Informática, mas a recíproca não é verdadeira, visto que um é gênero e o outro é espécie.

Os crimes de Informática, incluindo-se os crimes cibernéticos, podem ser classificados em puros e impuros, ou próprios e impróprios. Os primeiros são os novos tipos penais, que protegem bens jurídicos novos, relativos à alta tecnologia, surgidos com o advento dos recursos da Informática, incluindo-se a internet, como a segurança da informação e segurança cibernética. Antes da era da Informática, não havia qualquer sentido em se falar na proteção desses bens jurídicos, pois não existiam naquela.

MALAQUIAS (2015, p. 72) propõe definição para os crimes próprios, afirmando que seriam aqueles crimes que necessitam do espaço cibernético para serem praticados. Esse autor também procura definir o bem jurídico tutelado no crime cibernético, afirmando que seria a intimidade do indivíduo.

Contudo, em se tratando de crimes cibernéticos próprios, os bens jurídicos a serem tutelados são a segurança da informação e a segurança cibernética. Definitivamente, são bens jurídicos novos, completamente correlacionados com os recursos da alta tecnologia, da tecnologia da informação.

BRITO (2013, p. 50) ressalta a importância desses novos bens jurídicos, consubstanciados pela segurança cibernética e segurança da informação. São bens jurídicos recentes, surgidos em decorrência da popularização dos recursos da tecnologia da informação.

Dessa forma, os crimes de Informática próprios são os novos crimes, aqueles cuja prática seria impossível sem os recursos da Informática. São aqueles que atacam os novos bens jurídicos, relacionados com a Informática, surgidos com o advento da alta tecnologia. Alguns dos primeiros crimes cibernéticos puros foram tipificados por meio da Lei Caroline Dieckmann (Lei Nº 12.737/2012).

Essa lei acrescentou os artigos 154-A e 154-B ao Código Penal. O caput do artigo 154-A cria um novo tipo penal, talvez o primeiro crime cibernético puro no ordenamento jurídico pátrio: invasão de dispositivo informático alheio. Contudo, a pena

prevista de detenção de três meses a um ano e multa é muito pequena para ter o condão de realmente desmotivar a prática criminosa. Esse tipo penal tem por objetivo proteger um novo bem jurídico, surgido a partir da existência e popularização dos recursos da Informática, especialmente a internet, que é a segurança da informação ou segurança cibernética.

O parágrafo primeiro do artigo 154-A criminaliza as condutas de produzir e disseminar códigos maliciosos (vírus, cavalo de troia, vermes e demais pragas digitais), bem como dos equipamentos conhecidos como "chupa-cabras", que que são miniaturas de hardware para serem instaladas dentro dos caixas eletrônicos, com a finalidade de copiar as informações sensíveis dos clientes, incluindo-se os números do banco, agência, conta e senha, para efeito de clonagem dos cartões e posteriores saques fraudulentos nessas contas.

A Lei Caroline Dieckmann também alterou os artigos 266 e 298 do Código Penal, tendo incluído nesse último artigo o parágrafo único, *in verbis*:

> "Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito".

A criação desse dispositivo legal foi de grande importância para o enfrentamento dos crimes cibernéticos, visto que as quadrilhas de criminosos do espaço cibernético, estruturadas como crime organizado, possuem departamentos encarregados da clonagem de cartões de crédito e débito, com base nas informações sensíveis subtraídas fraudulentamente das vítimas, com a finalidade de realizarem saques e compras, dessa forma obtendo vantagens financeiras ilícitas.

Com o advento do parágrafo único do artigo 288, esses criminosos serão também enquadrados nesse tipo penal, podendo pegar pena de reclusão de um a cinco anos e multa. Cabe ressaltar que essa clonagem é muito praticada pelos membros das quadrilhas especializadas no golpe conhecido como "*Phishing Scam",* por meio do seu departamento de clonagem de cartões de crédito e débito.

Os últimos (crimes de Informática impuros) são os velhos crimes que já eram tipificados no Código Penal, como estelionato e os crimes contra a honra, praticados com a utilização de recursos da Informática, incluindo-se a internet. Nesse grupo estão inseridos, a título de exemplo, os tipos penais comuns que já existiam antes do surgimento da Informática e que agora os criminosos passaram a utilizar os recursos tecnológicos como ferramenta para a prática criminosa. Como exemplos podem ser citados: calúnia, injúria, difamação, furto, estelionato, tráfico de drogas e todos os demais crimes preceituados no Código Penal e nas leis especiais, possíveis de serem praticados com a utilização dos recursos das tecnologias da informação.

A Lei Nº 9.296/1996, a qual regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal, estabelece que, *in verbis:*

> "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
>
> Pena: reclusão, de dois a quatro anos, e multa."

Esse crime (interceptação telemática clandestina) pode ser considerado talvez o primeiro crime cibernético próprio, visto que o bem jurídico atacado é a segurança cibernética, que é um bem jurídico novo, surgido em decorrência do advento dos recursos da alta tecnologia, especialmente o espaço cibernético.

Com efeito, a sociedade, a cada dia que passa, torna-se se mais dependente dos recursos tecnológicos providos pela Informática. Hodiernamente, pode-se fazer tudo pela internet, pode-se comprar qualquer coisa, fazer propaganda eleitoral, movimentar contas bancárias, além de inúmeras outras atividades. Nesse mesmo sentido, os criminosos estão movendo suas atividades para a internet, inclusive as tradicionais quadrilhas de assalto a bancos, buscando mitigar os riscos e aumentar os lucros.

A Informática ou Ciência da Computação é uma ciência muito nova. Os primeiros computadores surgiram na década de 1940. O ENIAC (*Electronic Numerical Integrator and Computer*), considerado o primeiro computador digital eletrônico, foi lançado em 1946 e o UNIVAC *(UNIVersal Automatic Computer*), onsiderado o primeiro

computador comercial, começou a ser comercializado em 1951. Contudo, a despeito de tal ciência ser muito recente, seguramente as outras ciências, mesmo as mais antigas, quer sejam exatas, humanas, médicas, biológicas, sociais, da terra, todas se tornaram dependentes da Ciência da Computação, não sendo possível avançarem em termos de pesquisa e desenvolvimento sem a utilização dos recursos da nova ciência. Até mesmo as ciências sociais e humanas, como o Direito e a Geografia, também são muito dependentes dos recursos da Informática, como os editores de textos, bancos de dados, softwares de busca e, naturalmente, a internet, com todo o seu potencial com fontes inesgotáveis de pesquisa. (CASSANTI, 2014; MALAQUIAS, 2015).

Após a popularização da internet e o surgimento dos crimes cibernéticos, especialmente aqueles com efeitos globais, resta evidenciado que o espaço cibernético não possui fronteiras e que o crime se aproveita dessa situação para expandir suas atividades ilícitas, em âmbito internacional. Nesse sentido, o Direito Cibernético também precisa expandir seus horizontes.

De fato, o Direito Cibernético (ou Direito Digital), tendo-se em vistas que o espaço cibernético não possui fronteiras, em que as ações praticadas por meio da internet, quer sejam lícitas ou ilícitas, possuem abrangência mundial, precisa ser abordado de forma global, naturalmente respeitando-se as legislações dos países envolvidos. Além disso, em decorrência da altíssima velocidade do desenvolvimento e da evolução da tecnologia da informação, o processo legislativo não consegue atualizar a legislação aplicada em velocidade próxima, fato que gera muitos problemas, como a falta de proteção de bens jurídicos novos, surgidos em função da evolução tecnológica.

4. Necessidade de atualização da legislação penal

Considerando-se o fato de que o atual Código Penal é de 1940 e o Código de Processo Penal de 1941, portanto de datas anteriores ao início da Informática, esses diplomas legais foram concebidos e elaborados sem se considerarem características marcantes dos crimes cibernéticos. Além disso, naturalmente não há que se falar na tipificação desses crimes na versão original do Código Penal, visto que os bens jurídicos relacionados à alta tecnologia somente surgiram recentemente, principalmente em decorrência da popularização da internet. Assim, quando os Códigos Penal e Processual Penal entraram em vigência não existiam os bens jurídicos relacionados à alta tecnologia, como segurança da informação e segurança cibernética. Portanto, os crimes de Informática puros não poderiam ter sido tipificados naquela época, visto que não havia bem jurídico a ser protegido.

Contudo, os crimes de Informática impuros já existiam desde então, como o estelionato, o furto, os crimes contra a honra, dentre inúmeros outros, sendo que sempre puderam ser objeto de persecução penal, inclusive quando praticados por meio da internet. Com efeito, os crimes cibernéticos impuros, condutas típicas como o estelionato, quando praticadas por meio da internet, possuem um potencial ofensivo inúmeras vezes maior do que quando praticados fora do espaço cibernético, sendo que, ainda assim, a pena continua sendo a mesma.

Daí, exsurge a necessidade de modernização da legislação de forma a majorar as penas aplicadas aos crimes praticados por meio da internet, em que o seu alcance e potencial ofensivo são muito muito maiores, podendo atingir milhares de vítimas ao mesmo instante, podendo os criminosos obterem vantagens financeiras ilícitas em volumes estratosféricos, em tempo muito reduzido e com pouco risco, haja vista que escondem atrás de teclados, usando softwares maliciosos, em busca de suposto anonimato e da impunidade.

O *caput* do artigo 5º do Código Penal trata da territorialidade (do local do crime), estabelecendo que se aplica a lei brasileira ao crime cometido no território nacional, *in verbis:*

> "Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional".

Contudo, quando se tratam de crimes cibernéticos com efeitos globais, em que o criminoso nacional, dentro do território nacional, perpetra ataque, por meio do espaço cibernético, contra alvos localizados em outros países, a persecução penal se torna complexa. Nesses casos, como não houve nenhum efeito do crime no território nacional, as polícias judiciárias brasileiras não tomam conhecimento do fato criminoso, sendo que seria necessário um pedido de cooperação judiciária internacional, normalmente por meio de cartas rogatórias, para que as autoridades brasileiras tomassem conhecimento do fato. Contudo, normalmente esses mecanismos são muito morosos e normalmente demoram tempo superior à obrigatoriedade dos provedores de acesso à internet de preservarem os registros de acesso à internet, que é de um ano. Assim, torna-se inviável a persecução penal desses crimes.

Conforme preleciona MALAQUIAS, 2017, p. 73, enquanto não existir uma lei específica para regulamentar os crimes cibernéticos, aplicam-se a esses novos crimes o que está disposto no artigo 5º do Código Penal, aplicando-se a lei brasileira aos crimes cometidos em território nacional.

Essa assertiva é verdadeira, contudo não se pode olvidar da necessidade da cooperação judiciária internacional para a obtenção das provas e promoção da persecução penal, sendo que a morosidade desses procedimentos normalmente torna inviável essa ação dos órgãos encarregados da persecução penal, deixando os crimes sem solução e os criminosos sem punição. Normalmente, as evidências que podem comprovar a materialidade, a dinâmica e a autoria dos crimes estão armazenadas em computadores localizados em outros países, fato que dificulta sobremaneira a investigação cibernética e a apuração dos fatos.

Mesmo com relação às normas penais não incriminadoras, pode-se constatar que inclusive elas estão desatualizadas relativamente aos crimes eletrônicos. Segundo o artigo 6º. Do Código Penal, *in verbis*:

> "Artigo 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 o resultado".

Por sua vez, o Código de Processo Penal, em seu artigo 70, estabelece que "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.

Para efeito de se demonstrar a inadequação e dificuldade de aplicação desses dispositivos legais em casos de crimes digitais, considerar-se-ão casos de ataques cibernéticos com efeitos globais, como os ataques denominados "r*ansomware*", que constituem em prática criminosa que torna os dados da vítima indisponíveis por meio de criptografia e, na sequência, exige-se valor financeiro para o resgate dos dados da vítima. (CASSANTE, 2014, p. 32).

Esses ataques podem ser perpetrados por membros de quadrilhas espalhados por vários países, em que centenas de milhares ou até milhões de vítimas residentes em dezenas de países distintos podem ser atingidas por meio da mesma conduta criminosa. O ataque de "*ransomware*" consiste na exploração de vulnerabilidade dos computadores das vítimas, normalmente por falta de atualização do Sistema Operacional, de forma a restringir o acesso ao computador infectado, por meio da conduta ilícita de compactar e criptografar os dados da vítima, bem como de, na sequência, cobrar valor significativo de cada usuário, a título de resgate dos dados, para que o acesso possa ser restabelecido, por meio do fornecimento de senha para a recuperação e acesso aos dados, mediante o pagamento em criptomoeda, de forma a se garantir a não rastreabilidade da operação financeira. (CASSANTE, 2014)

Nesses casos, entende-se que o local crime, às luzes do ordenamento jurídico pátrio, compreende os países de onde partiram o ataque cibernético (local em que ocorreu a ação) e as dezenas de países onde residem as vítimas (onde se produziram os resultados da conduta criminosa). Quanto à competência da persecução penal, essa é determinada pelas dezenas de países onde residem as vítimas do crime. Tratam-se, portanto, de crimes transnacionais, em que uma mesma ação criminosa atinge vítimas espalhadas em muitos países.

Contudo, a dificuldade maior surge na persecução penal, especialmente na investigação dessas condutas típicas, na medida em que as evidências que poderão comprovar a materialidade e principalmente a autoria do crime estão espalhadas em diversos países, sendo que a sua obtenção depende de cooperação judiciária internacional, por meio de cartas rogatórias. Dessa forma, é de grande urgência e necessidade a atualização da legislação material e processual, visando a uma melhor eficácia na persecução penal dos crimes cibernéticos, especialmente aqueles com efeitos globais.

Nesse sentido, existe proposta de criação de um Tribunal Penal Internacional exclusivo para julgar crimes cibernéticos com efeitos globais. A proposta prevê a criação do tribunal na ONU. Por meio desse tribunal seria mais fácil para os Estados membros exercerem a pretensão punitiva nesses casos de crimes de alta tecnologia, praticados por meio da internet, em que milhares de pessoas espalhadas por dezenas de países se tornam vítimas da ação criminosa.

5. Notícias falsas (*fake news*) nas campanhas eleitorais

As notícias falsas, também muito conhecidas como *fake news,* sempre foram utilizadas em campanhas políticas, desde há muito tempo, com a finalidade de alterar o resultado das eleições de forma fraudulenta. De fato, uma notícia falsa, quando bem elaborada e disseminada com muita abrangência, tem o poder de alterar o resultado de uma eleição, subtraindo votos do candidato vítima da mentira e favorecendo o candidato patrocinador da fraude. Essa prática ilícita vem sendo utilizada desde tempos anteriores à era da Informática, quando a disseminações de notícias falsas eram feitas por meio da impressão e distribuição de panfletos e comunicados, pichações de muros e paredes de casas, bem como de outros meios igualmente rudimentares, porém eficazes, utilizados naquela época.

Com o pretexto de realizar propaganda política, muitas vezes são divulgadas notícias falsas de candidatos oponentes, principalmente por meio da internet, visto que o alcance é muito abrangente, as mensagens permanecem disponíveis e acessíveis para milhões de eleitores.

Contudo, hodiernamente está cada vez mais comum a divulgação de notícias falsas, principalmente por meio da internet, com a finalidade de alterar de forma fraudulenta o resultado das eleições.

Assim, há três tipos de propaganda política: a propaganda eleitoral, regulamentada pelo artigo 36, caput, da Lei Nº 9.504/1997; a propaganda intrapartidária, regulamentada pelo artigo 36, § 1º, da Lei Nº 9.504/1997; e propaganda partidária, regulamentada pelo artigo 45 da Lei Nº 9.096/1995 [1]. Em tese, todos os três tipos de propagandas eleitorais podem divulgar notícias falsas, as *fake news*.

Com a popularização da internet, especialmente das redes sociais, o potencial ofensivo dessa prática fraudulenta aumentou de forma estratosférica, com a utilização dos recursos tecnológicos da Informática, tanto para a produção do material como para a disseminação das notícias falsas. Dessa forma, milhões de pessoas podem ser alcançadas e informadas dessas notícias e influenciadas a mudarem o seu voto. Destarte, o uso da internet possibilita que a propagação das notícias falsas ganhe velocidade e poder de alcance inimagináveis, permitindo que tal prática ilícita possa ter efeitos avassaladores numa campanha política, alterando indevidamente os seus resultados. Daí, exsurge a necessidade de avanço no processo legislativo para a produção de leis que regulamentem essa situação. A ação do TSE nesse controle também é de grande relevância.

Ressalte-se que as *fake news*, de per si, não são crimes, pois não há nenhuma lei penal que tipifique tal conduta como crime. Há muitas *fake news* que nada mais são do que fofocas, como aquelas que afirmam falsamente que determinada personalidade veio a óbito, que se divorciou ou que foi visto com uma amante. Contudo, a depender do seu conteúdo, as *fake news* podem ser enquadradas em tipos penais, especialmente nos crimes contra a honra: calúnia, difamação e injúria.

Dessa forma, em decorrência da incrível rapidez da disseminação das *fake news* pela internet, é importante que as campanhas eleitorais sejam assistidas por escritórios de advocacia especializados em Direito Cibernético e Direito Eleitoral, para que possam atuar diligentemente, de forma a tomar as devidas providências necessárias para a imediata remoção dos conteúdos falsos da internet, minimizando os efeitos nocivos ao candidato. Na sequência, é necessária a adoção de medidas urgentes para o início das investigações cibernéticas, visando à identificação e à localização dos autores, bem como a propositura de ações cíveis de reparação de danos morais e queixas-crimes em face dos responsáveis pelas publicações das notícias falsas.

As investigações cibernéticas levadas a efeito de forma não oficial, conduzidas por advogado especializado em Direito Cibernético, com o apoio de peritos da área de Computação Forense, com certeza poderão ser muito mais ágeis do que as investigações oficiais, de forma a se obterem os resultados desejados dentro dos curtos prazos exigidos no Direito Eleitoral.

6. Conexão de Direito Cibernético com o Direito Eleitoral

Há uma forte conexão entre o Direito Cibernético e o Direito Eleitoral, na medida em que há várias questões tecnológicas da Ciência da Computação referentes às eleições que precisam ser tratadas por esses dois ramos do Direito, como: segurança das urnas eletrônicas, campanhas eleitorais pela internet, bem como a persecução penal dos crimes eleitorais praticados por meio pela internet, envolvendo aspectos relativos à Ciência da Computação Forense e à investigação cibernética.

Com efeito, em decorrência das últimas minirreformas eleitorais, seguramente surgirão muitas questões envolvendo a alta tecnologia que precisarão ser tratadas pelo Direito Cibernético, a Computação Forense e a investigação cibernética, como ferramentas de apoio ao Direito Eleitoral. Essas minirreformas eleitorais impuseram novas regras as serem observadas nos processos eleitorais, incluindo-se a proibição de financiamento das eleições por pessoas jurídicas, a permissão da vaquinha eletrônica (*crowdfunding*) e o impulsionamento oneroso de postagens nas redes sociais.

Como as pessoas jurídicas não poderão mais financiar as campanhas eleitorais, em tese haverá grande diminuição dos recursos financeiros nas campanhas eleitorais. Esse fato, associado com as possibilidades tecnológicas agora permitidas pela lei eleitoral, seguramente motivará ainda mais os candidatos a cargos eletivos a utilizarem cada vez mais a internet, especialmente as redes sociais, em suas atividades de campanhas políticas. Seguramente, o custo desses recursos tecnológicos é muito baixo, em comparação com outras formas utilizadas fora do espaço cibernético, sendo que os resultados a serem obtidos, considerando-se uma atuação profissional e cuidadosa, podem trazer resultados eleitorais muito melhores.

7. Ramos do Direito relacionados com o Direito Cibernético

Além do Direito Eleitoral, existem outros ramos do Direito que também se relacionam fortemente com o Direito Cibernético, como: Direito Penal, Direito do Consumidor e Direito Civil, haja vista que a sociedade como um todo está fazendo uma rápida e constante migração de suas atividades cotidianas para a internet.

Como é cediço, os criminosos estão migrando rápida e constantemente as suas atividades ilícitas para a internet. Hodiernamente, praticamente todos os crimes estão sendo praticados com a utilização de recursos da Informática como ferramentas de apoio, incluindo-se a internet nesse rol de recursos tecnológicos. Até mesmo os crimes mais simples, incluindo-se os furtos de objetos de pequeno valor, estão sendo praticados com a utilização de recursos da alta tecnologia, até mesmo os ditos “ladrões de galinha” utilizam “smart phones” e aplicativos como o *WhatsApp* para se comunicarem e acertarem detalhes do furto, produzindo-se vestígios e evidências digitais que poderão comprovar a materialidade, a dinâmica e a autoria

de fatos típicos, mediante a produção de laudos periciais nos aparelhos utilizados.

As tradicionais quadrilhas de assalto a bancos migraram suas atividades para a internet, buscando mitigar os riscos e aumentar os lucros, sem a necessidade de enfrentamento e troca de tiros com a polícia. Dessa forma, essas quadrilhas cooptam jovens com bons conhecimentos de Informática, compram "kits fraude", com programas e equipamentos para a prática de crimes cibernéticos, como a conhecida fraude de "Phishing scam", dentre outras. Nesse diapasão, surge a conexão entre o Direito Penal e o Direito Cibernético para o tratamento dessas questões no âmbito jurídico.

A forte relação do Direito Cibernético com o Direito do Consumidor surge na medida em que atualmente pode-se comprar tudo por intermédio da internet, desde pequenos objetos até imóveis de alto valor. Seguramente, nessas transações realizadas no meio digital, por intermédio da internet, surgem inúmeras questões relacionadas a essas compras e vendas online que precisam ser tratadas por esses dois ramos do Direito, visto que as provas e evidências que poderão comprovar a materialidade de autoria das condutas estão em meios digitas, muitas vezes necessitando exames periciais da área de Computação Forense para o esclarecimento de questões muito técnicas, que estão além da compreensão dos operadores do Direito.

O Direito Civil também se relaciona fortemente com o Direito Cibernético, na medida em existem muitas questões comuns a esses dois ramos do Direito, como: contratos digitais online, reparação de danos morais e materiais em decorrência de fatos ocorridos no espaço cibernético, dentre outros. Essas e tantas outras questões cíveis praticadas por meio do espaço cibernético precisam ser tratadas conjuntamente pelo Direito Civil e pelo Direito Cibernético.

8. Conclusões

Definitivamente, as pessoas da sociedade hodierna vêm sistematicamente fazendo uso cada vez mais intenso dos recursos da Informática, especialmente a internet, em suas atividades cotidianas, tornando-se totalmente dependentes desses recursos tecnológicos. Por sua vez, os criminosos vêm seguindo o mesmo ritmo, sendo que em suas atividades ilícitas eles usam intensamente os recursos tecnológicos como ferramentas para a realização de suas práticas criminosas. Daí exsurge a grande relevância do Direito Cibernético, pois é essa nova vertente do Direito que aborda todas essas questões tecnológicas e seus aspectos legais.

O Direito Cibernético ainda não se estabeleceu como um ramo autônomo do Direito, sendo que a sua área de atuação está fortemente vinculada a outras áreas, como: Direito Eleitoral, Direito Penal, Direito do Consumidor, Direito Civil, dentre outras. Assim, é necessária a busca de conhecimentos de outras áreas do Direito para permitir uma boa atuação no Direito Cibernético.

Por meio deste artigo procurou-se explorar a forte conexão existente entre o Direito Cibernético e o Direito Eleitoral, bem como foi feita contextualização de vários assuntos correlatos, como a Computação Forense, perícia digital, crimes de Informática e suas outras nomenclaturas e variações. Foram estudados os diversos crimes eleitorais próprios, tipificados na lei eleitoral, identificando-se quais poderiam ser praticados com a utilização de recursos da Informática, especialmente a internet.

Foram explorados os aspectos investigativos necessários para a responsabilização de indivíduos que fazem uso da internet para propósitos escusos, buscando o anonimato e a impunidade, para interferirem fraudulentamente nos resultados das eleições, normalmente com a utilização de perfis falsos. Conforme discutido, são possíveis a identificação e a localização dessas pessoas, visto que tudo o que se faz na internet deixam-se rastros, os quais podem ser perseguidos pelos peritos especialistas em Computação Forense, com a participação de advogado especialista em Direito Cibernético.

Dessa forma, conclui-se que o Direito Cibernético precisa ser trabalhado com outras áreas mais tradicionais do Direito, bem como precisa ter o apoio da Computação Forense para a promoção de investigações cibernéticas e de perícias digitais para se desvendarem questões muito técnicas que demandam conhecimentos

específicos dessa vertente da Ciência da Computação. Assim, por meio dessa composição de conhecimentos, é possível a solução dos casos de interesse do Direito Eleitoral, especialmente das divulgações de notícias falsas, em tempo de campanhas e pré-campanhas eleitorais, por meio da internet, com a finalidade de se promoverem fraudes para a alteração dos resultados dos pleitos, de forma fraudulenta.

Referências

[1] ALMEIDA, Roberto Moreira de. Curso de Direito Eleitoral. Editora Juspodivm, 11ª Edição, 2017. Salvador/BA. ISBN 978-85-442-1133-5. 896 páginas. 2017.

[2] BARRETO, Alessandro Gonçalves; WENDT, Emerson; e CASELLI, Guilherme. Investigação Digital em fontes abertas: Busca de dados em redes sociais, coleta de informações na Deep Web, análise de metadados. Editora Brasport, 2º edição: 2017. Rio de Janeiro. ISBN 978-85-7452-814-4.

[3] BRITO, Auriney. Direito Penal Informático. Editora Saraiva, 2013. ISBN 978-85-02-20942-8.

[4] CANDIDO, Joel José. Direito Penal Eleitoral e Processo Penal Eleitoral. Editora Edipro, 2006, ISBN 857283561X, 1ª Edição.

[5] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Editora Brasport Livros e Multimídia Ltda. 2014.

[6] CHALITA; Savio – Manual Completo de Direito Eleitoral. São Paulo: Editora Foco. 2014. ISBN

[7] DE LUCA, Newton (obra coletiva). Direito & Internet. Editora Quartier Latin do Brasil. 2ª edição, 2005.

[8] FERREIRA FILHO, Paulo Gomes. Anotações práticas sobre a coleta e a preservação de provas digitais no cumprimento de medidas cautelares de busca e apreensão. Conteúdo Jurídico, Brasília/DF: 14 out. 2016. Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.56913>. Acesso em: 21 jun. 2018.

[9] GOMES, José Jairo. Direito Eleitoral. Atlas Editora. 2013. 720 páginas. ISBN 8522477612. 9ª edição.

[10] MALAQUIAS, Roberto Darós. Crime Cibernético e prova: A investigação Criminal em Busca da Verdade. ISBN 978-85-362-5383-1. Curitiba: Editora Juruá, 2º edição revista e atualizada, 2015.

[11] NIESS, PEDRO HENRIQUE TÁVORA; SOUZA, LUCIANA TOLEDO TÁVORA NIESS; e KAHN, ANDRÉA PATRÍCIA TOLEDO TÁVORA NIESS. Direito Eleitoral. Editora Edipro. 1ª Edição, 2016. 360 páginas. ISBN 978-85-7283-909-9.

[12] PINHEIRO, Patricia Peck. Direito Digital. São Paulo: Editora Saraiva, 6º edição: 2016. ISBN 978-85-02-63561-6.

[13] PINHEIRO, Patrícia Peck (obra coletiva). Direito Digital Aplicado 2.0. São Paulo: Editora Thomson Reuters, 2ª edição: 2016. ISBN 978-85-203-6864-0.

[14] POMINI, ANDERSON. Direito Eleitoral – Teoria e Prática. ISBN 8563452010. 160 páginas. Exteriora Editora, 2010.

[15] RAIS, DIOGO. Direito Eleitoral Digital. ISBN 852037218X. 240 páginas. Editora RT, 2018.

[16] REYES, Anthony (obra coletiva). Cyber Crime Investigations. Editora Amorette Pedersen, 2007. ISBN 978-1-59749-133-4.

[17] TRIBUNAL SUPERIOR ELEITORAL. Código Eleitoral Anotado e Legislação Complementar. TSE, 2016. SGI/Coordenadoria de Jurisprudência do Tribunal Superior Eleitoral. ISBN 978-85-86611-92-6.