DELITO VIRTUAL: UM DIÁLOGO SOBRE AS TRANSGRESSÕES ONLINE DO MUNDO REAL

VIRTUAL CRIME: A DIALOGUE ABOUT ONLINE TRANSGRESSIONS ON REAL WORLD

> Ricardo Silva¹ UFPE

Resumo

Ao relacionar o delito no âmbito virtual, principalmente à internet, estabelece-se o objetivo deste artigo, ao dialogar sobre as transgressões online sobre a lógica do mundo real, ao fazer enlaces epistemológicos sobre tecnologia e sociedade, criando um percurso discursivo e analítico em caminhos, por vezes, tortuosos, das ações humanas no meio internet. A metodologia adotada é descritiva, explicativa, qualitativa e baseada em inferências sobre as referências teóricas abordadas.

Palayras-chave

Delito virtual. Crimes na Internet. Direito Digital.

Abstract

By relating online crime, especially to the Internet, the purpose of this article is to discuss online transgressions about the logic of the real world, making epistemological links about technology and society, creating a way of discursive and analytical path, sometimes tortuous, of human actions in the internet context. The methodology adopted is descriptive, explanatory, qualitative and based on inferences about the theoretical references.

Keywords

Virtual crime. Crimes on the Internet. Digital Rights.

¹ Doutor em Educação Matemática pela UFPE. Professor Universitário.

1 INTRODUÇÃO

O delito, por definição, no âmbito jurídico, nos diz: "Quaisquer ações e/ou comportamentos que infrinjam uma lei já estabelecida; ação punível pela lei penal; crime; todo ato caracterizado por uma transgressão de uma moral preestabelecida; falta; flagrante delito. O delito no momento exato em que é praticado; Corpo de delito. Elemento material (indícios) da infração, prova do crime; e, etimologicamente (origem da palavra delito): do latim *delictum*.

A internet tem se tornado "alvo" de críticas acerca das ações delituosas de pessoas que não temem as "punições que não existem" ou que não estão ainda previstas por lei. Inúmeras infrações e atos ilícitos ficam flutuando no limbo situacional das consequências do "livre arbítrio".

A medida que o Direito procura "olhar" o espaço virtual como extensão do mundo real, ao considerar a regulação das ações humanas, sobretudo o olhar sobre as infrações praticadas na "rede", se faz necessário ampliar as discussões e reflexões sobre como está o processo de educação da sociedade, no uso das tecnologias da informação e comunicação, e, como esta sociedade está lidando com a sua liberdade de expressão e sua criatividade para criar ou destruir, elevar ou diminuir, fazer ou deixar de fazer².

Há uma escuta do "foi sem querer" em larga escala, em vários níveis de complexidade dos fatos delituosos que acontecem diariamente, principalmente no meio virtual. Isto, sob certo ponto de

² Brasil. *Constituição da República Federativa do Brasil de 1988*. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 20 dez. 2017.

vista, passa a falsa ideia de que "foi sem querer" é algo que pode ser perdoado, esquecido, que não causou nada demais, não machucou, não marcou para sempre.

Ao contrário deste ingênuo pensamento, delitos virtuais tem causas imensos transtornos, problemas psicológicos, alguns levando ao suicídio e ao *bullying*. O que precisa ficar claro é que o meio virtual contém o mundo real, e lá acontecem coisas muitos sérias, "querendo" e deixando rastros que não se apagam.

Portanto, a ação delituosa no meio virtual deve ser sim olhada adequadamente, investigada, considerada e, na prática, instrumentalizada como um ato humano com consequências.

2 O DELITO VIRTUAL NO MUNDO REAL

Iniciamos nosso percurso dialógico considerando as ações humanas no mundo virtual, em ambientes caóticos e organizados, dotados de regras e limitações, sob a influência do massivo estímulo ao consumo e a livre expressão, causando efeitos comportamentais em série, inclusive convidando o usuário à transgressão, por vezes, criminosa.

A "distância" da/na/entre a internet traz/cria uma sensação de "segurança", motivando as pessoas a desenvolver ações, por vezes no anonimato, "conscientes" de que não há "mal" algum em quebrar algumas regras, haja visto que estão num meio onde "tudo" é permitido, passível de punição, escondido num IP – *Internet Protocol*, número que identifica a origem da conexão com a rede.

Na Internet, vige o regime da livre iniciativa e inovação: não é necessária autorização prévia para se criar um novo serviço ou aplicação, desde que seguidas as recomendações técnicas do IETF - *Internet Engineering Task Force*. As redes de telecomunicações existentes em cada país servem como alternativas de suporte para o funcionamento da "rede de redes" que é a Internet. Apesar de estarem intimamente relacionadas, Internet e telecomunicações são atividades distintas³.

Livre iniciativa é confundida muitas vezes com permissão para "fazer o que quiser", banalizando o papel da "autoria", inclusive "reduzindo" e "distorcendo" o conceito de sociedade da "escrita", emergente da expansão da internet autoral.

De fato, há grande confusão acerca do uso de ferramentas tecnológicas de comunicação virtual e as redes sociais, tornando estas subutilizadas e suscetíveis a ações que alteram o a sua verdadeira função, social e tecnológica, e, por vezes, os usuários assumem que suas ações fazem partes de algo "neutro", sem efeito algum no mundo real, o que não é verdade.

O princípio da neutralidade de rede previsto na Lei 12.965/2014 consiste na garantia de tratamento isonômico dos pacotes de dados pelas redes dos sistemas autônomos sem degradação nem discriminação por conteúdo, origem e destino, serviço, terminal ou aplicação (cf. MCI, Art. 9º)⁴.

³ CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei. 2015. Disponível em:

http://cgi.br/media/docs/publicacoes/4/contribuicao-do-comite-gestor-da-internet-no-brasil.pdf>. Acesso em: 10 mar. 2018, p. 01.

⁴CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da

Neutralidade esta que afasta a ideia de que nenhuma ação é neutra em si mesma e que a intervenção humana define o ato, lícito ou não, e suas consequências para a pessoa que aceita a situação, seja numa conversa, transação comercial ou financeira.

Na transmissão, comutação ou roteamento estão sujeitos ao cumprimento da obrigação de dar tratamento isonômico aos pacotes de dados na Internet no Brasil: O administrador de Sistema Autônomo, a quem são designados um ou mais blocos de endereços IP pelo NIR ("National Internet Registry") brasileiro, que é o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), em conformidade com as resoluções do Comitê Gestor da Internet no Brasil (CGI.br), e que utiliza tais endereços para prover serviços ou acesso a terceiros; As entidades que se destinam a prover acesso à Internet a usuários e às quais forem delegados sub-blocos específicos de endereços IP por parte de um Administrador de Sistema Autônomo⁵.

A expansão comercial da internet aglomerou pessoas, ideias, relações e conflitos. Estar na internet, hoje, significa ter pouca privacidade e muita atenção aos dados que são fornecidos, propagados

Internet no Brasil à Regulamentação da Lei. 2015. Disponível em:

http://cgi.br/media/docs/publicacoes/4/contribuicao-do-comite-gestor-da-internet-no-brasil.pdf>. Acesso em: 10 mar. 2018, p. 02.

⁵ CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei. 2015. Disponível em:

http://cgi.br/media/docs/publicacoes/4/contribuicao-do-comite-gestor-da-internet-no-brasil.pdf>. Acesso em: 10 mar. 2018, p. 02.

e informados. Nunca se "deixou" tanto de ler contratos de adesão de serviços online como atualmente, diante de uma ansiedade exagerada, onde as pessoas não têm paciência para entender os seus direitos e deveres diante dos serviços contratado, além dos riscos de prover informações pessoais "gratuitas" que podem ser utilizadas para fins comerciais, e, até mesmo para ataques de violação de privacidade⁶.

É comum hoje a necessidade de "expor nossa localização" para ter acesso e comodidade a serviços "próximos" a nosso lar ou trabalho. As questões de segurança nem sempre são consideradas, e, em alguns casos, ficamos diante de potenciais ações criminosas, tanto no meio virtual quanto no mundo real.

Aliás, desde já necessitamos entender que virtual e real se misturam, trazendo questões de ordem social, econômica e política, para nossas vidas e o entendimento sobre o mundo em que vivemos atualmente. Afinal, recém-nascidos já saem da maternidade devidamente "localizados" virtualmente, no mundo real.

Ética é algo distante das pessoas. Considera-se, por vezes, as normas regulatórias como instrumentos de controle social. Verdade? Bem, não fiquemos apenas neste ponto ocular, mas procuremos alargar o espectro de alcance dos efeitos das leis na vida humana. Existem leis naturais, associadas ao nosso modo de viver como seres biológicos.

A transgressão comumente bate à nossa porta moral. O que nos impede de cometer um delito? No meio virtual o que é necessário para tornar as ações das pessoas delituosas? A liberdade?⁷

⁶ Bellovin, Steven M.; Blaze, Matt; Landau, Susan; Pell, Stephanie K.. It's Too Complicated: How The Internet Upends Katz, Smith, and Electronic Surveillance Law. *Harvard Journal of Law & Technology*, Volume 30, Number 1 Fall 2016.

⁷ Kees, Van Noortwijk. Integrated legal information retrieval: new developments and educational challenges. *European Journal of Law and Technology*, [S.l.], v. 8,

Olhemos para a indústria do consumo, que diariamente, constantemente e massivamente nos impele a transgressão dos nossos limites, até mesmo financeiros, nos conduzindo para situações impossíveis, inconsequentes, e, portanto, ferindo a ética. Não há dúvidas que a disrupção tecnológica tem afetado o ritmo de apropriação e entendimento sobre o modus operandi das tecnologias na vida das pessoas, mas nossa privacidade tem sim diminuído muito. Isto abre portas para os atos delituosos no meio virtual, de modo preocupante.

Não vamos aqui crucificar e acusar a internet de estabelecer o caos social em que vivemos. Existem tantas outras razões, e uma delas está associada ao desenvolvimento do pensamento coletivo. Nisto sim, a internet provocou avanços estrondosos. Nunca se aprendeu tanto colaborativamente. Nunca se produziu tanto conhecimento. A internet alterou o modo de vida das pessoas, pois,

São exemplos de situações notórias de segurança de rede em que serão permitidas práticas de discriminação de pacotes de dados na Internet e a degradação de tráfego para a mitigação de prejuízos à prestação de serviços e acesso à Internet: Filtragem de endereços IP específicos para mitigação de DoS (Negação de serviço, ou *Denial of Service*): admite-se filtragem de endereços IP envolvidos na origem de um ataque DoS, técnica pela qual um atacante, valendo-se tipicamente de recursos arregimentados de alguma forma na rede (*DDoS – Distributed Denial of Service*), visa a tirar de operação

n. 1, mar. 2017. ISSN 2042-115X.

um serviço ou aplicação; Bloqueio da porta 25 (SMTP – *Simple Mail Transfer Protocol*): admite-se e estimula-se o bloqueio da porta 25 para o combate a spam (correio eletrônico não solicitado, geralmente enviado para um grande número de usuários). Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (*Unsolicited Commercial E-mail*). A exclusivo pedido do usuário final discriminações tais como controle parental poderão ser implementadas pelo provedor de acesso na relação provedor-usuário⁸.

Ao mesmo tempo em que este grande repositório de informações e conhecimentos se expande, olhares temerosos veem o desenvolvimento de uma "outra" internet, onde os delitos virtuais são comuns, profissionalizados, difíceis de se alcançar, além de estarem conectados, por vezes, a interesses políticos, econômicos e ideológicos das transnacionais⁹.

Em verdade dizemos a todos os internautas, cuidado com o que posta, o que pesquisa, o que compra e o que faz no meio virtual, pois tal espaço

Em sua estrutura completa é análogo a imagem de um iceberg. A parte visível deste é denominada de Surface

⁸ CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei. 2015. Disponível em:

http://cgi.br/media/docs/publicacoes/4/contribuicao-do-comite-gestor-da-internet-no-brasil.pdf>. Acesso em: 10 mar. 2018, p. 03.

⁹ Brasil. *Marco Civil da Internet* (Lei 12.965/2014). Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 jan. 2017.

Web enquanto sua parte imersa simboliza a Deep Web, representando diversos aspectos que diferenciam o ciberespaço. Um exemplo dessa discrepância se dá nos navegadores específicos usados para ambos. Softwares conhecidos como o Google Chrome e o Firefox, enquanto específicos da Surface Web, não conseguem captar o conteúdo da Deep Web em que são utilizados navegadores como o TOR¹⁰.

Não se recomenda enveredar na *Deep Web* sem conhecimento técnico mínimo para lidar com situações "inusitadas" que surgirão, como por exemplo, ter o seu computador invadido, travado e colocado sob pagamento de "fiança" para ser libertado novamente ao seu "dono".

Mas não pensemos que lidar com o infrator, ou criminoso, seja tão simples, pois até mesmo nestes casos necessita-se de autorização para requerer a identificação da pessoa suspeita, inclusive por ordem superior, em face de que:

Para a necessária preservação da intimidade e privacidade do usuário:

1) O acesso aos dados cadastrais independentemente de ordem judicial por autoridades somente deverá ocorrer nas hipóteses determinadas em Lei. Por exemplo, Lei n.º 12.850/2013 (Lei das Organizações Criminosas) ou na Lei n.º 9.613/1998 (Lei da Lavagem de Dinheiro, tal como reformada pela Lei n.º 12.683/2012);

¹⁰ Da Silva Almeida, J.; Roque, B. V. S.. Challenges Of The Law In The Regulation Of Legal Relations In Deep Web And Cyber Crimefigshare, , 9 fev. 2018. Disponível em:

https://figshare.com/articles/challenges_of_the_law_in_the_regulation_of_legal_relations_in_deep_web_and_cyber_crime/5873892/1. Acesso em: 18 mar. 2018, p. 166.

- 2) O usuário final deve ter informação clara sobre o início e o término esperado da guarda dos registros de conexão e de acesso a aplicações de Internet, bem como do procedimento para que se formalizem solicitações para o fornecimento dessas informações.
- 3) Ordem judicial que determine a guarda de logs por prazo superior ao expresso no Marco Civil da Internet deve observar, em cada caso, o tempo remanescente do prazo prescricional pertinente, conforme o previsto no ordenamento jurídico nacional¹¹.

Neste meio tempo o desastre pode ter se instalado em sua casa, na sua vida e na vida de pessoas próximas. Voltamos, então, ao início do diálogo, sobre os cuidados que devemos ter ao prover informações, fornecer localização ou acessar ambientes que não temos segurança para navegar ou nos comunicar.

O processo de regulação na rede virtual procura "organizar" o fluxo das ações das pessoas, suas atitudes e consequências. Não obstante, tais informações armazenadas, por autorização pessoal do contratante do serviço, podem afetar sua vida no mundo real, inclusive proporcionando a propagação de informações sigilosas, para instituições financeiras e agentes de consumo, o que ocasiona, por vezes, situações desconfortáveis, sobretudo no âmbito social.

Como temos várias camadas de internet, as informações podem ser tornar armas para os infratores que cometem delitos virtuais, pois fica a sensação de impunidade, por um lado por nossa limitação de ação frente ao especialista infrator no meio virtual, por outro lado a

¹¹ CGI-BR. Comitê Gestor da Internet no Brasil. Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei. 2015. Disponível em:

http://cgi.br/media/docs/publicacoes/4/contribuicao-do-comite-gestor-da-internet-no-brasil.pdf>. Acesso em: 10 mar. 2018, p. 04.

expansão do estado de "nada acontece por aqui", portanto, os atos delituosos se expandem exponencialmente.

Quantas vezes não recebemos e-mails com contratos, boletos, cadastros, restrições financeiras pendentes, nos convidado a clicar em *links* que irão "solucionar" todos os problemas, mas que são armadilhas virtuais para captura de senhas, credenciais e informações que serão utilizadas para ataques a contas bancárias, repositórios de informações pessoais e até mesmo instrumentos tecnológicos de uso pessoal.

A falta de controle sobre o submundo virtual é capaz de promover sentimentos humanos responsáveis por euforia e sensação de inatingibilidades suficientes para condutas ilícitas que expressam a ideia de sucesso das ações. Estas devem ser cessadas com o estabelecimento de limites que tracem pontos aos quais os usuários podem atingir sem desrespeitar o direito alheio¹².

Neste mar de impunidade se fez necessário articular algumas ações regulatórias, com o teor jurídico mais acentuado e orientado a conduta dos usuários para usufruírem das possibilidades advindas do mundo virtual, influenciando e alterando suas ações e sua vida no mundo real, afinal, o real é virtual e o virtual é real.

É óbvio que neste contexto a privacidade está em jogo, cada vez

 $^{^{12}}$ Da Silva Almeida, J.; Roque, B. V. S.. Challenges Of The Law In The Regulation Of Legal Relations In Deep Web And Cyber Crimefigshare, , 9 fev. 2018. Disponível em:

https://figshare.com/articles/challenges_of_the_law_in_the_regulation_of_legal_relations_in_deep_web_and_cyber_crime/5873892/1. Acesso em: 18 mar. 2018, p. 168.

mais afetada pelos mecanismos de registro, busca e localização. Nas mãos delituosas tornam-se poderosas armas de "fogo", deixando-nos, por vezes, indefesos e reféns do acaso, do jogo do meio, da inevitabilidade dos atos ilícitos.

Não se pode impor limites onde não existe este conceito e onde regras não são obedecidas. Esta afirmação faria sentido se houve uma proteção incondicional aos infratores no mundo virtual, anônimos que intencionalmente prejudicam, aterrorizam e fazem mal a sociedade. De fato, o Marco Civil da Internet procura colocar lentes para olhos atentos aos conceitos e preceitos que regem a sociedade organizada, cidadã e pautada em valores éticos, morais e que forjam o caráter do ser humano, impendido o mundo de se tornar um cárcere do não lido pelo não dito.

Hoje, mais do que nunca, temos que estar atentos aos nossos direitos enquanto consumidores da informação e da tecnologia, pois os delitos virtuais se contextualizam, na maioria das vezes, por falta de entendimento sobre os direitos e deveres, no meio virtual.

A sensação de impunidade precisar ser extirpada da sociedade, dando lugar a consciência coletiva e ao cuidado com o bem-estar do outro. O meio virtual não é "um não lugar", mas "o lugar" das pessoas na sociedade da informação. Não pautemos nossas ações na "liquidez" desta sociedade pós-moderna, onde o efêmero é cultuado, o imediatismo adorado e a ansiedade legitimada.

Pensemos numa perspectiva inclusiva, focada no coletivo, em que toda a ação provoca uma reação, sobretudo quando "do outro lado" da tela. Nada pode descaracterizar as relações humanas, nem mesmo sua ausência.

Sabemos que os atos de infração online desconsideram qualquer iniciativa de enfrentamento regulatório, e, portanto, torna-se mais

atrativo para quem pratica o ato delituoso burlar o sistema, as leis, a ordem que contextualiza o meio virtual.

Num território onde o delito é caracterizado de modo complexo, a área jurídica busca sempre novos instrumentos para atenuar e apoiar ações corretivas, preventivas e punitivas. Não é tarefa fácil, pois os infratores têm acesso aos instrumentos do Direito.

Ao mesmo tempo em que se desenvolve tecnologias que proporcionam autoria coletiva, temos a indústria que investe no individualismo tecnológico, da personalização, criando diversos tipos de processos que envolvem segurança de alto nível até customização com base no acesso a produtos e serviços, de modo semântico.

De fato, não tínhamos tanta "liberdade" de produção, aquisição e expressão até a década de 80. Os anos 90 nos trouxeram, em seus meados, grandes possibilidades, encurtando espaços físicos inatingíveis, permitindo a inovação em ritmos nunca vistos, chegara a internet.

Diante desta evolução várias iniciativas foram tomadas na área jurídica, como por exemplo a justiça desportiva, que atualmente usufrui do meio virtual para julgar casos no futebol e outras modalidades.

Uma dificuldade presente no Brasil, diante da sua miscigenação cultural, é unificar o pensamento jurídico para o que de fato é correto, ético e eficaz.

É natural para qualquer infrator virtual estabelecer relações de poder nos contextos onde atuam, tornando ainda mais complexo o ambiente para a vítima de sua ação. Para tanto, estabelece-se referenciais do mundo real para comparar com as ações do mundo virtual, pois todo delito virtual traz uma representação de comportamentos sociais, muitas vezes construídos em torno de

conceitos industriais, fortemente influenciados pelo capitalismo.

Não se deve pensar sobre delito virtual inocente. Pelo contrário, atos planejados com muita cautela, atenção e dedicação de tempo, mesmo que em situações aparentemente banais e casuais. A vítima sempre sai perdendo, o infrator sempre com mais poder.

Há notadamente movimento direção na do 11m desenvolvimento eficaz e breve da atuação jurídica no meio virtual, principalmente nos cenários onde as tecnologias mobilizam a vontade conduzindo-as para transformações pessoas, das sociais comportamentais, motivadas pelo entretenimento, liberdade isolamento social.

Há uma relação conflituosa do infrator no meio virtual, onde ao mesmo tempo procura lidar com a solidão e os problemas do seu "eu" no mundo real, transmitindo para os "avatares" a condições de expressão da liberdade ideológica e criando um fascínio pela transgressão.

De fato, o Direito Digital tem "olhado" para estas questões num ponto focal diferente. A regulação torna-se o *modus operandi* da engrenagem pessoa-meio virtual, ao mesmo tempo que coisifica, tipifica, relaciona o imaginário com o concreto. É mais fácil hoje saber por onde "andou" o infrator, não apenas pela localização ou rastreamento, mas pelo "comportamento" adotado no meio virtual.

Há um emaranhado de situações que, por vezes, ajudam, outras vezes atrapalham a área jurídica, para apoiar ações delituosas no meio virtual. Algumas tecnologias são simplesmente criadas para regulação a ação humana no meio virtual, por exemplo, o consumo de dados, sites permitidos, tipos de conexão, bloqueio contra invasão etc.

Por outro lado, o efeito regulatório do Direito sobre a tecnologia procura atenuar algumas potenciais situações delituosas que

poderiam ocorrer devido a "ausência" do estado de prevenção do crime virtual, motivando as pessoas na busca por segurança e diferentes atitudes frente os contextos que se constituem, durante o tempo que estão online, e, até mesmo, as possíveis consequências, após ficarem off-line.

Há uma emergência no sentido de maior aprofundamento e compreensão do meio virtual, como ele se constitui e como o Direito pode auxiliar na construção de instrumentos que favoreçam o livre acesso, a colaboração, o desenvolvimento e a expansão da rede.

O que precisa ficar claro, e mais compreensível, é o papel da sociedade na construção da internet. Este meio virtual não se constrói sozinho, mas a partir de ações humanas. O anonimato é um atestado da incapacidade de se apresentar para o coletivo, o desenvolvimento e a contribuição pensando no "nós", mesmo sendo estimulados ao "eu", ao "só", ao "meu".

Não sejamos ingênuos em acreditar que estamos próximos de "limpar" a internet dos atos delituosos, em todos os níveis, pois a cada dia cresce ainda mais a motivação para a transgressão. Seja na pirataria, na invasão, na agressão, em qualquer outro contexto desta natureza, a motivação humana define o caminho e o perfil da rede.

Sempre haverá transgressão em ambientes regulados. Pessoas que não seguem normas ou que não se importam com o bem-estar alheio. Que não enxergam na colaboração possibilidades de construção. É melhor ver "o circo pegar fogo", sem objetivo aparente, apenas pela motivação de ver algo não dar certo, para alguns ou para alguém. O criminoso virtual fica a espreita, sempre atento aqueles que estão em situações de fragilidade de segurança dos dispositivos, conexões frágeis, fora do alcance da possibilidade de vencer o infrator e a infração.

O ritmo das situações delituosas que ocorrem no meio virtual demanda para a área jurídica energia e esforço para estabelecer leis eficazes para punir e prevenir ações criminosas, por vezes frutos das "brechas' no sistema jurídico, que permite ao infrator liberdade de ação, impunidade e livre acesso a rede.

Atos regulatórios, normalmente, são atacados diretamente com ações ainda mais complexas e danosas. Por exemplo, cercear o direito a pesquisa, adotado por alguns países radicais, motiva muitas pessoas ao crime de acesso indevido à informação, criando bases de dados não oficiais, sujeitas a ações de invasão, monitoramento indevido e apropriação de informações pessoais sem autorização.

Estamos diante de inúmeros exemplos de delitos virtuais, como por exemplo, burlar sistemas de repositórios de informações indexadas pagas, criando brechas para supressão das credenciais de segurança para o acesso, estabelecendo cenários propícios para o crime de apropriação indevida de informações pessoais, a medida que a vítima usufrui do documento indevidamente acesso, o infrator usufrui dos dados pessoais da vítima, promovendo um verdadeiro caos na vida social, por vezes invadindo contas bancárias, comprando com dados de crédito roubados entre outras situações.

Como quer que seja, a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação¹³.

_

¹³ Aras, Vladimir. Crimes de informática. *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em:

Está claro que a conduta humana no meio virtual determina o ato delituoso, ao caracterizar ações que vão de encontro ao estabelecido nas leis e instrumentos regulatórios. Olhando por este prisma, a internet hoje é um mar onde se navega em águas escuras, sem a noção da profundidade, se vai acontecer um maremoto, ou tempestade. Se vamos encontrar uma ilha ou um povoado. Para onde ir ou vir, num mar tão grande. Esta é a sensação pela qual milhões passam na rede, principalmente quando são vítimas de atos criminosos.

A criminalidade informática preocupa o mundo e tem reclamado definições. Para a OECD - *Organization for Economic Cooperation and Development*, o crime de computador é "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados", podendo implicar a manipulação de dados ou informações, a falsificação de programas, a sabotagem eletrônica, a espionagem virtual, a pirataria de programas, o acesso e/ou o uso não autorizado de computadores e redes¹4.

De fato, conceituar algo que se constrói socialmente não é tarefa fácil. A construção do conceito de tecnologia começa em casa, na família, no círculo de amizades, no indivíduo.

Ao socializar-se, o ser humano começa a construir outros conceitos, agregando valor ou não ao que já foi aprendido. Por

https://jus.com.br/artigos/2250. Acesso em: 5 jun. 2017, p. 07.

¹⁴ Ibid, p. 07.

exemplo, piratear filmes pode ser um ato delituoso bem convidativo para aquele fiel colecionador que não tem mais recursos financeiros para continuar sua empreitada de consumo.

Quão atraente não é pagar "nada" por algo tão valioso, material e sentimentalmente? Deixa-se de lado a ética, os valores e começam os atos, frequentes e intermináveis de transgressão, violação de direitos autorais, gerando prejuízos incalculáveis para os autores, empresas e financiadores.

Para que comprar um livro, se deslocando de casa, se posso piratear na rede, de modo rápido e ágil, apenas fazendo aquele rápido cadastrado, fornecendo minhas informações pessoais, falsificadas, em provedores de e-mails gratuitos ou redes sociais abertas? O delito parece ser fácil, não é?

De qualquer modo, ainda que não se tenha chegado a um consenso quanto ao conceito doutrinário de delito informático, os criminosos eletrônicos, ou *ciberdelinquentes*, já foram batizados pela comunidade cibernética de *hackers*, *crackers e phreakers*¹⁵.

Neste movimento de crimes virtuais surgem aqueles do "bem" e do "mal". Uns "sem" interessa aparente em prejudicar, apenas colocar em prática seu elevado conhecimento técnico ou para massagear seu ego, alimentar competição entre pares.

Outros querem é prejudicar mesmo, empresas, pessoas, sistemas. Não se sentem parte de nada, e, mesmo assim, querem tomar

¹⁵ Aras, Vladimir. Crimes de informática.. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em:

https://jus.com.br/artigos/2250>. Acesso em: 5 jun. 2017, p. 08.

posse de tudo. Entram em constante contradição, numa vida de crimes sem fim.

Algumas pessoas, criminosas profissionais, conseguem burlar os sistemas de localização e rastreamento, criando coordenadas geográficas falsas, até mesmo se apropriando da identidade de outros, para não serem capturados e continuarem seus delitos¹⁶.

Mas a "terra de ninguém" está cada vez mais "terra de alguém", onde as tecnologias estão a favor da lei, na busca de orientar e coordenar as ações que possibilitem erradicar ou reduzir tais crimes, por vezes cruéis. Constantemente ouvimos falar de crimes contra a dignidade da pessoa humana, sem punição, pois não há ainda regulação jurídica para tal ato no meio virtual.

Como a Internet não é *self-authenticating* a definição de autoria fica no campo da presunção. E, para o Direito Penal, não servem presunções, ainda mais quando se admite a possibilidade de condenação. O único método realmente seguro de atribuição de autoria em crimes informáticos é o que se funda no exame da atuação do responsável penal, quando este se tenha valido de elementos corporais para obter acesso a redes ou computadores¹⁷.

¹⁶ Richet, Jean-Loup. Cybercrime and Law Enforcement Training. Harvard Law School. November, 14, 2017. Disponível em:

http://blogs.harvard.edu/jeanlouprichet/files/2016/03/Cybercrime-and-Law-Enforcement-Training.pdf. Acesso em: 12 mar. 2018.

Aras, Vladimir. Crimes de informática. *Revista Jus Navigandi*, ISSN 1518-4862,
 Teresina, ano 6, n. 51, 1 out. 2001. Disponível em:

https://jus.com.br/artigos/2250. Acesso em: 5 jun. 2017, p. 25.

Muitas empresas têm atuado junto aos usuários para protegelos de atos ilícitos no meio virtual. É o exemplo das chaves de segurança, que "fecham" a conexão ponto-a-ponto. Os bancos utilizam bastante esta tecnologia, permitindo tranquilidade nas transações online.

Por outro lado, a necessidade de proteção dos dispositivos traz a questão da proteção extra componente, ou seja, como um antivírus, que previne diversas ações invasivas através da internet. Tem se discutido bastante o papel dos programas de antivírus e se a indústria da tecnologia cria os vírus para manter um mercado milionário e aberto, a partir do "medo" de estar desprotegido.

Diante deste fato é que os crimes perpetrados neste ambiente se caracterizam pala ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas¹⁸.

Os autores dos crimes virtuais normalmente não são identificados por se esconderem nos códigos, nos avatares, nos perfis falsos, comumente encontrados nas redes sociais.

Um expert em informática como os crackers modernos podem perfeitamente se apropriar de uma senha alheia e utiliza-la para diversos fins. Desta feita, estaria usando a identidade alheia, aplicando golpes ou simplesmente

¹⁸ Terceiro, Cecílio da Fonseca Vieira Ramalho. O problema na tipificação penal dos crimes virtuais. 2002. Disponível em: <</p>

egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 12 dez. 2017, p. 03.

navegando na internet como se fosse o titular daquele código ou senha¹⁹.

Quanta vezes não ouvimos relatos de pessoas que foram atacadas nos seus *smartphones*, onde imagens, vídeos, textos e informações pessoais foram capturados. Além disso, muitos ataques acontecem com a autorização do próprio usuário, que busca aventuras virtuais, sem conhecer quem está "do outro lado", permitindo ser filmado, fotografado, conduzido num ritual que alimenta o fetichismo digital, conduzindo a situações humilhantes, embaraçosas e até prejuízo financeiro.

O sequestro do dispositivo é um ato delituoso no mundo atual. Não apenas associado a falta de segurança do dispositivo, mas a falta de entendimento e apropriação do estado de segurança pelo próprio usuário, que não enxerga o perigo, pois para ele a internet é só um meio "bom".

O Direito é uma ciência de natureza social, portanto, é lógico concluir que sofre inúmeras mudanças de acordo com o avanço da sociedade a que esteja ligado. O ser humano é um ser eminentemente social, devido a esta necessidade organizacional do homem em sociedade, é que surge a figura do Estado. Após a organização do Estado como único ente capaz de substituir a vingança particular, ultrapassando a fase da autotutela primitiva humana, depende o homem do direito para não só respaldar suas transações privadas, mas como confia e outorga-lhe o direito da devida sanção aos indivíduos que transgridem a ordem legal estabelecida²⁰.

¹⁹ Ibid.

²⁰ Terceiro, Cecílio da Fonseca Vieira Ramalho. O problema na tipificação penal

É muito difícil para os doutrinadores do Direito estabelecer referenciais de ação num meio onde passa pelo desenvolvimento social da personalidade do indivíduo. Só há vítima porque existe contexto social favorável para a construção do ato delituoso.

Também se encontra encartado infraconstitucionalmente no art. 1.º do Código Penal Brasileiro, dispondo que: Art. 1º. Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal²¹.

Portanto, a impunidade é ampliada, até que surja um parâmetro comparativo para apontar o ato delituoso e construir o paradigma de acusação. O infrator não se preocupa até que a lei chegue a ele. E isto pode demorar muito, ou não vir a acontecer.

Em muitos casos, devido à ausência de norma que tipifique tais crimes, têm, os Tribunais, se socorrendo da analogia para o ajustamento da conduta atípica à norma penal, o que pelo Princípio da Legalidade, onde se assenta o nosso Direito punitivo, é terminantemente proibido o emprego da analogia em matéria penal²².

dos crimes virtuais. 2002. Disponível em: <

egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 12 dez. 2017, p. 05.

²¹ Ibid, p. 06.

²² Terceiro, Cecílio da Fonseca Vieira Ramalho. O problema na tipificação penal dos crimes virtuais. 2002. Disponível em: <</p>

egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 12 dez. 2017, p. 08.

Há avanços significativos no que diz respeito a punição dos crimes virtuais, baseados em crimes do mundo real. A impunidade não é algo desejável, tendo no Direito um olhar para o progresso contínuo das leis que permitam julgar, em tempo hábil, os casos que surjam.

Os Tribunais de todos os modos tentam conter os chamados "crimes virtuais", cada qual observando o caso em concreto, aplica uma solução que acha justa. Ora, na medida que a lei é omissa, deixa margens a ação do aplicador legal, que muitas vezes se ver em uma árdua tarefa, que foge a sua competência originária, pois é forçado a legislar, tudo devido a um caso concreto que lhe foi apresentado²³.

O Direito penal está dedicado a encontrar mecanismos que permitam trazer justiça ao meio virtual, onde bens apropriados indevidamente, pessoas são atacadas, vidas são marcadas.

A dogmática penal moderna, sempre se preocupou em analisar a estrutura do direito penal como um todo, individuo, sociedade, crime e seus reflexos. Analisando o Direito Penal, podemos seguramente afirmar, que o mesmo, tem como escopo principal proteger um determinado objeto de uma agressão ilícita, portanto o objeto de proteção por parte do mesmo há de ser específico e determinado. O crime em uma visão lato é uma agressão a um bem tutelado pelo Estado e prevista

²³ Ibid, p. 09.

em lei como tal²⁴.

Não há clareza em algumas situações do que está sendo atingido, embora, normalmente, a privacidade do indivíduo é afetada, tornando o ato ilícito. Invasão de privacidade tem sido um crime virtual comum atualmente. Além da fragilidade de segurança nos dispositivos, as faltas de conhecimento básico sobre determinados procedimentos de conduta online tornam ainda mais vulnerável a navegação no meio virtual.

Portanto no que tange aos crimes virtuais há de se especificar quais são os objetos a serem tutelados pela norma penal. Se observarmos, por exemplo, que a conduta do indivíduo primou em "invadir" um computador alheio apenas com o condão de visualizar suas correspondências (e-mails), aponta-se como objeto de tutela pelo estado a intimidade do indivíduo atacado, intimidade esta, indevidamente afrontada²⁵.

Diante da falta de um maior acompanhamento do desenvolvimento dos atos ilícitos no meio online, a frequência dos delitos virtuais aumenta, a medida que as lacunas legais continuam a existir, motivando ainda mais ações dirigidas e específicas, através da expertise das pessoas com alto conhecimento técnico de operação da

²⁴ Terceiro, Cecílio da Fonseca Vieira Ramalho. O problema na tipificação penal dos crimes virtuais. 2002. Disponível em: <

egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 12 dez. 2017, p. 11.

²⁵ Ibid, p. 11.

rede. Um ritmo é avassalador, enquanto o outro é consideravelmente lento e prejudicial ao cidadão que procura apenas usufruir das possibilidades do mundo online.

A balda das informações expostas, chega-se a uma ilação lógica, que devido à ausência de tipificação legal, discriminante das condutas dos agentes que utilizam a INTERNET como instrumento na prática de delitos, tal vácuo legal, encoraja o surgimento de novos delitos neste meio tecnológico²⁶.

Ainda existe grande dificuldade no Direito em acompanhar e efetivar as devidas ações que impeçam atos delituosos no meio virtual, visto que as práticas de cibercrimes são tão comuns quanto crimes no mundo real. Aliás, o meio virtual se torna parte da estratégia para atos delituosos, começando no mundo real, passando pelo real ou viceversa.

Comprovar um delito virtual é tarefa quase impossível, mesmo com a identificação do IP de origem do infrator, até de fato estabelecer uma série de documentações comprobatórias do ato. Além da burocracia junto aos provedores de serviços, o cidadão se vê isolado, muitas vezes, sem ponto de partida, para atuar em prol da solução da invasão, agressão ou sequestro de dados realizados²⁷.

²⁶ Terceiro, Cecílio da Fonseca Vieira Ramalho. O problema na tipificação penal dos crimes virtuais. 2002. Disponível em: <

egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 12 dez. 2017, p. 14.

²⁷ Martins, Jilia Diane; Rech, Francieli. A Responsabilidade Civil e Criminal nos Crimes Virtuais. *Interfaces Científicas* - Direito · Aracaju · V.6, N.2, p. 75 – 86, Fevereiro. 2018. Disponível em:

https://periodicos.set.edu.br/index.php/direito/article/view/5373/2670. Acesso

Por outro lado, muitos crimes virtuais já foram solucionados pela parceria do provedor de serviços com os órgãos da justiça, com o objetivo de reestabelecer a ordem e trazer a tranquilidade de volta a vida do cidadão. As campanhas antipirataria, situações de conscientização e mobilização da sociedade, são iniciativas que procuram atenuar a crescente onda de crimes virtuais. A reeducação social para uso da tecnologia também se torna urgente, numa sociedade marcada pela individualização e consumo exacerbados²⁸.

Cada vez mais a impunidade online tem sido combatida, com ações, mesmo que incipientes ou iniciais, mas realizadas de forma contundente e objetivando a solução e correção dos atos delituosos no meio virtual.

As pessoas precisam entender que as tecnologias de informação e comunicação estão cada vez mais imbricadas no contexto da convergência e possuem valor estratégico para a economia mundial. Diante disto, muitas pessoas entendem que cometer crimes no meio virtual torna-se até meio de vida.

Diariamente milhões de pessoas são atacadas virtualmente. Cabe a sociedade, ao Direito e os órgãos competentes buscarem corrigir falhas, criar instrumentos de proteção, atualizar as formas de regulação numa sociedade marcada pela individualização e consumo.

Os delitos virtuais continuarão a existir, enquanto a

²⁸ Bortot, Jessica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. VirtuaJus – Belo Horizonte, v.13 - n.1, p.338-362– 1º sem. 2017.

ISSN: 1678-3425. Disponível em:

em: 05 mar. 2018.

http://periodicos.pucminas.br/index.php/virtuajus/article/download/15745/15745-56007-1. Acesso em: 10 mar. 2018.

impunidade continuar a crescer.

3 CONCLUSÃO

Este artigo teve por objetivo dialogar sobre as transgressões online sobre a lógica do mundo real, ao fazer enlaces epistemológicos sobre tecnologia e sociedade, criando um percurso discursivo e analítico em caminhos, por vezes, tortuosos, das ações humanas no meio internet.

Percebemos que o Direito tem buscado compreender a realidade social em que a sociedade da informação se insere, ao relacionar os crimes do mundo virtual ao que já se conhece no mundo real.

Real e virtual se misturam, trazendo uma nova realidade para a atuação jurídica em torno da regulação do uso de tecnologias e serviços no meio online da internet. Não se pode pensar em bloquear serviços, limitar a atuação do Estado, proibir as pessoas do acesso à informação.

Não se pode cercear o direito à liberdade de expressão, frente as situações, por vezes constrangedoras, de invasão, captura de informação, roubo de dados, uso indevido de imagem, entre outras ações delituosas. A impunidade alimenta o crescimento das transgressões no meio virtual, muitas vezes motivadas pelo desafio de demonstrar alto conhecimento técnico, outras vezes para criar o caos social e econômico.

O Direito Digital necessita expandir, cada vez mais, estudos e prover recursos para fazer frente a esta realidade que afeta a sociedade, traz insegurança e mobiliza as pessoas a se limitarem diante de tantas possibilidades que a internet oferece.

Este artigo pretende ser uma ponte de interconexão com outros estudos, que retome a questão dos delitos virtuais e que outros pesquisadores continuem trazendo questões para reflexão, que gerem ações concretas para o desenvolvimento de uma sociedade mais confiante, sustentável e ética.

4 REFERÊNCIAS

Aras Vladimir. Crimes de informática. *Revista Jus Navigandi*, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: https://jus.com.br/artigos/2250. Acesso em: 5 jan. 2018.

Brasil. *Constituição da República Federativa do Brasil de 1988*. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompi lado.htm>. Acesso em: 20 dez. 2017.

_____. *Marco Civil da Internet* (Lei 12.965/2014). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 jan. 2017.

Bellovin, Steven M.; Blaze, Matt; Landau, Susan; Pell, Stephanie K.. It's Too Complicated: How The Internet Upends Katz, Smith, and Electronic Surveillance Law. *Harvard Journal of Law & Technology*, Volume 30, Number 1 Fall 2016.

Bortot, Jessica Fagundes. *Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional.* VirtuaJus – Belo Horizonte, v.13 - n.1, p.338-362– 1º sem. 2017. ISSN: 1678-3425. Disponível em: http://periodicos.pucminas.br/index.php/virtuajus/article/download/15745/15745-56007-1. Acesso em: 10 mar. 2018.

CGI-BR. Comitê Gestor da Internet no Brasil. *Contribuição do Comitê Gestor da Internet no Brasil à Regulamentação da Lei*. 2015. Disponível em: http://cgi.br/media/docs/publicacoes/4/contribuicao-do-comite-gestor-da-internet-no-brasil.pdf>. Acesso em: 10 mar. 2018.

Da Silva Almeida, J.; Roque, B. V. S.. *Challenges Of The Law In The Regulation Of Legal Relations In Deep Web And Cyber Crimefigshare*, , 9 fev. 2018. Disponível em: https://figshare.com/articles/challenges_of_the_law_in_the_regulation_of_legal_relations_in_deep_web_and_cyber_crime/5873892/1. Acesso em: 18 mar. 2018.

Kees, Van Noortwijk. Integrated legal information retrieval: new developments and educational challenges. *European Journal of Law and Technology*, [S.l.], v. 8, n. 1, mar. 2017. ISSN 2042-115X.

Martins, Jilia Diane; Rech, Francieli. A Responsabilidade Civil e Criminal nos Crimes Virtuais. *Interfaces Científicas* - Direito · Aracaju · V.6, N.2, p. 75 – 86, Fevereiro. 2018. Disponível em: https://periodicos.set.edu.br/index.php/direito/article/view/5373/26

70>. Acesso em: 05 mar. 2018.

Richet, Jean-Loup. Cybercrime and Law Enforcement Training. Harvard Law School. November, 14, 2017. Disponível em: http://blogs.harvard.edu/jeanlouprichet/files/2016/03/Cybercrime-and-Law-Enforcement-Training.pdf>. Acesso em: 12 mar. 2018.

Terceiro, Cecílio da Fonseca Vieira Ramalho. *O problema na tipificação penal dos crimes virtuais*. 2002. Disponível em: < egov.ufsc.br/portal/sites/default/files/anexos/13024-13025-1-PB.pdf>. Acesso em: 12 dez. 2017.