3. Introdução

A era digital tem conseguido dar uma liberdade extravagante para as pessoas se sentirem abertos a profanar crimes anonimamente. Com a crescente utilização de tecnologias digitais, também há o crescimento de cibercrimes que se tornam cada vez mais difíceis de serem desvendados. Entretanto, mesmo com a grande evolução da tecnologia, as evidências desses delitos ainda são dificultosas de serem coletados. Apesar de existir várias regras e protocolos de proteção de dados nos aplicativos, os criminosos conseguem passar com facilidade perante essas barreiras.

É inegável que até os dias atuais a rede conhecida como internet gerou diversas mudançaspara a vida da sociedade global como um todo, em diversos aspectos é fácil apontar a inerente necessidade que hoje existe em relação a habitar espaços virtuais.

A normalização do convívio virtual gerou certo conforto inesperado. Esse elemento somado a ausência de legislação voltada ao local fez com que uma onda de crimes fosse instaurada. Tais crimes são chamados de cibercrimes, se fundamentam principalmente nas dificuldades que a força investigativa enfrenta para recolher provas que sejam suficientes para instauração do processo penal.

O ponto chave do presente artigo é compreender, o conceito de prova tradicional e o recolhimento de evidências nos meios virtuais.

Enfim o estudo elenca as dificuldades enfrentadas nos parâmetros dos ambientes virtuais com base no recolhimento e manutenção de evidencias, levando em conta os métodos de investigação cibernética após o Marco Civil da internet.

Para se chegar ao conceito, foi necessário enquadrando na teoria do conceito analítico finalista do crime, como sendo condutas típicas, antijurídicas e culpáveis, aos quais são praticadas com a utilização dos sistemas de informática, sendo a motivação por diferentes questões, sejam políticas, fins econômicos ou satisfação pessoal.

Conforme a Convenção sobre Cibercrimes em 2001, em Budapeste, informa algumas definições sobre esse tema, trazendo em seu art. 1º, alínea a, como “qualquer dispositivo isolado ou um grupo de dispositivos relacionados e interligados, me que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados” (CONVENÇÃO SOBRE CIBERCRIME, 2001, p. 3).

Mesmo com essas premissas, há outros conceitos que devem ser estudados, já que há um entendimento próprio por cada autor.

Fabrizio Rosa (2002) trabalha com o conceito de crime cibernético como sendo:

2. O „Crime de Informática “é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o Crime de Informática “pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002, p. 53).

Após entender sobre a terminologia dos crimes cibernéticos, é necessário enquadrar as características do sujeito ativo. O agente é em sua maioria composto por homens, com pouca habilidade de comunicação, ou seja, não possui um ciclo social abrangente, na faixa etária entre os 13 aos 15 anos de idade, sem ter consolidado ainda seus valores morais, no qual o mundo virtual passa a ser seu quarto de interação, sem que precise interagir diretamente com outras pessoas.

A própria rede de internet é uma ferramenta onde há técnicas de aprendizagem para pratica de crimes, de qualquer natureza, principalmente quando há zonas como a *deep web* em que não se há rastro quanto aos dados reais dos usuários devido o anonimato.

Em virtude disso, devido ao acesso facilitador da rede de comunicações, juntamente com esses sentimentos de autoconfiança e o anonimato presente para os usuários, as informações e dados compartilhados são falsos, se tornando difícil de colher provas para suficiência de autoria e comprovação da materialidade do delito.

A localização do sujeito ativo é crucial para a investigação, justamente porque o crime é consumado em uma rede de internet, onde a vítima e o agente estão distantes, sem contato direto. O anonimato interfere na identificação dos responsáveis, consequentemente, não há comprovação de autoria e materialidade.

4. Desenvolvimento

Os dados pessoais são um alvo facilmente adquiridos pelos criminosos, principalmente pela falta de legislação estabelecida para os crimes cometidos virtualmente.

O Marco Civil da Internet, concretizado no Brasil em 2014, estabelece princípios e regras importantíssimos para o uso de internet no país. Vale ressaltar entre esses princípios, o princípio de proteção da privacidade e dos dados pessoais. No artigo 7º, inciso VII, determina eu é vedado o fornecimento desses dados para terceiros, salvo mediante consentimento livre, expresso e informado.

Essa legislação também reconhece a importância dos dados pessoais e a necessidade de protegê-los. O artigo 7º, inciso IX, do Marco Civil estabelece que a coleta, uso, armazenamento e tratamento de dados pessoais devem ser realizados de acordo com a lei e respeitando a privacidade, a proteção dos dados e as liberdades individuais.

A LGDP (Lei Geral de Proteção de Dado), aprovada em 2018, busca garantir maior controle e transparência aos titulares dos dados, promovendo a proteção da privacidade e a segurança das informações.

A LGPD estabelece princípios fundamentais para o tratamento de dados pessoais, como a finalidade específica e legítima, a adequação, a necessidade, a transparência, a segurança, a prevenção de danos e a responsabilização dos envolvidos. Ela também prevê que o consentimento do titular dos dados seja obtido de forma clara e específica para cada finalidade de uso.

Apesar dos avanços da legislação vigente, ainda há vários desafios a serem confrontados. O crescimento e evolução da tecnologia, exige um desenvolvimento concordante das leis que abrandem esse tema.

De acordo com o site *vocesa* o vazamento de dados aumentou em 493% no Brasil. Portanto, é necessário o estabelecimento de normas mais eficazes e a cooperação entre diferentes jurisdições para garantir uma proteção adequada dos dados pessoais em escala global.

Portanto é fundamental que essas legislações vigentes sejam aprimoradas para dificultar os crimes cibernéticos, e outras leis possam ser criadas para restringir ainda mais o vazamento desses dados. Outrossim, é importante que aja estudos mais aprimorados para a busca de evidencias de tais infrações.

5. Conclusão

Neste artigo, buscou-se compreender sobre a dificuldade durante as investigações policiais com relação as provas produzidas nos crimes cibernéticos onde o anonimato predomina no perfil dos usuários, sem que deixe rastros no cometimento dos seus crimes, ao ponto de saírem impune em virtude dessa dificuldade.

Primeiramente, foi trazido o conceito de crimes cibernéticos, como um fato típico, antijurídico e culpável. Ainda, para entender sobre o crime cibernético, é necessário compreender sobre o perfil do criminoso, onde sua autoconfiança se predomina justamente pelo anonimato, podendo ser qualquer pessoa capaz, com acesso as informações e dados.

Em seguida, é trabalhada a questão da dificuldade de obtenção de provas nos meios virtuais. o cenário acaba sendo mais prejudicado pela burocracia judiciária e pelos bloqueios das lacunas legais, fazendo com que o atual enfrentamento contra crimes cibernéticos seja muito mais dificultoso em relação ao recolhimento e preservação das evidencias digitais, que são os únicos meios de provas úteis a investigação cibernética.

Por fim, os meios tradicionais de obtenção de provas, facilmente podem ser a ruina da investigação cibernética quando ignoram as evidências digitais.

6. Referencias preliminares

ALMEIDA, Juliana Evangelista e LUGATI, Lys Nunes. Da Evolução das Legislações Sobre Proteção de Dados: A Necessidade de Reavaliação do Papel do Consentimento Como Garantidor da Autodeterminação Informativa. Revista de Direito da Universidade Federal de Viçosa.

CAPELLETTI, Mauro; GARTH, Bryant. Acesso à justiça. Tradução Ellen Gracie

Castells, M. (2010). The Rise of the Network Society: The Information Age: Economy, Society and Culture (Vol. I). John Wiley & Sons.

Floridi, L. (2014). The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press.

Northfleet. Porto Alegre: Sergio Antonio Fabris, 1988.CERQUEIRA, Thalles Vilela.

Regulação de Proteção de Dados Pessoais. Belo Horizonte: Fórum, 2018.