Quaestio Iuris

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

CRIMES SEXUAIS CONTRA A DIGNIDADE SEXUAL, ATRAVÉS DO USO DA INTERNET – UMA REVISÃO CRÍTICA À LEGISLAÇÃO BRASILEIRA

Nelson Massini[1]

Marisa da Silva Prado Lopes [2]

Resumo

Este trabalho apresenta ao leitor a consolidação do entendimento sobre os crimes sexuais com o uso da internet, como é analisado e juridicamente pela legislação brasileira. É inegável a contribuição dos avanços tecnológicos, contudo é preocupante o descontrolado crescimento do acesso à internet que facilitou a prática de atividades ilegais, tais como a difusão de pornografia infantil, fraudes, crimes sexuais, etc. O objetivo é fazer uma análise do direito comparado com a legislação internacional sobre o tema crimes informáticos e ao mesmo tempo discutir a incidência desse tipo de crime no estado do Rio de Janeiro (RJ). Neste trabalho foi realizado um levantamento estatístico quantificador dos crimes sexuais na internet no estado do Rio de Janeiro (RJ) e a tabulação de todos os registros pela análise dos boletins de ocorrência registrados na delegacia de repressão aos Crimes de Informática (DRCI) nos últimos três anos e pouco (2013, 2014, 2015 e início de 2016). Neste trabalho, obtivemos uma coleta de dados não expressiva mesmo com o aumento de denúncias referentes aos crimes sexuais pelo uso da internet nos últimos anos. Espera-se que com os resultados da pesquisa, utilize-se de respaldo para trabalhos futuros concernentes à questão tão crucial nos dias atuais.

Palavras-chave: Internet; Tecnologia; Computação Forense; Crime Sexual; Legislação.

INTRODUÇÃO

Torna-se inegável a contribuição que a ciência e a tecnologia nos proporcionam, contudo, diferentes faces assumem as estreitas relações humanas na vida cotidiana e no desenvolvimento tecnológico. Por um lado, temo inúmeros benefícios com esse advento. Por outro lado, se não expressivamente em maior grau, o aumento danoso da extensão dos crimes iniciados em eventos virtuais.

Segundo análise recente do IBGE, um em cada dez domicílios brasileiros acessa a rede por algum dispositivo móvel, tais como celulares, notebooks ou *tablets*.[3] Torna-se evidente o acesso cada vez mais precoce

[1] Doutor em Odontologia -Farmacologia pela Universidade Estadual de Campinas (1983) e livre docência pela Universidade de São Paulo 1986 Professor titular da Universidade do Estado do Rio de Janeiro UERJ. E-mail: massini@terra.com.br

[2] Mestranda na Medicina Laboratorial e Tecnologia Forense, da Universidade do Estado do Rio de Janeiro, UERJ. E-mail: mdsprado@gmail.com

[3] Para o IBGE, 85,6 milhões de brasileiros acima de 10 anos de idade (49,4% da população) tinham acessado a internet, pelo menos uma vez, num período de três meses.

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

por crianças e adolescentes e, nesse sentido, a Internet possibilita o contato com pedófilos.

A internet é um vasto território de compartilhamento de informações em escala global. O ambiente virtual promove problemas frequentes, tais como os crimes de estelionato, fraudes, injúrias, contra a honra, pirataria, pornografia infantil e sexual.

Este último é o objetivo geral do projeto proposto. Os capítulos seguintes proporcionarão análises dos conceitos, das definições e dos limites conceituais destes delitos. Por fim, após um breve estudo sobre aspectos relevantes do Direito Penal no Brasil, um levantamento do Direito Comparado, bem como as formas encontradas pelo Estado para a persecução destas condutas no ciberespaço.

Não obstante, espera-se contribuir com, além dessas que tem sido motivo de alerta e de necessária revisão da legislação brasileira, uma reflexão crítica ao aumento à insegurança jurídica nos cidadãos que dependem cada vez mais da rede.

TECNOLOGIA FORENSE

O ramo da tecnologia forense, ou computação forense, procura obter informações através de análise de dados de um computador, um sistema/rede ou qualquer dispositivo de armazenamento de dados, que seja alvo de investigação, por crimes ou delitos cibernéticos. Segundo Eleutério e Machado (2011) a Computação Forense busca evidências para a solução de um crime.

Tendo em vista que as provas digitais possuem requisitos específicos de validade como a sua admissibilidade, a sua coleta e preservação devem ser realizadas, conforme a autenticidade e integridade garantidos pelos princípios da ciência computacional. Características estas que podem ser verificadas pela análise das provas digitais pela perícia forense.

Segundo Domingos (2017) o papel da perícia forense é fundamental, sendo que o acompanhamento da mesma desde as buscas e apreensões é necessário para que a coleta das provas digitais seja mantida corretamente, com padrão nos procedimentos para garantir a credibilidade dos dados obtidos.

LEGISLAÇÃO

Leis que estabeleçam os direitos dos cidadãos usuários da Internet e deveres dos prestadores são fundamentais para que o Judiciário possa fazer frente a violações e riscos que a sociedade da informação possa sofrer com o impacto, segundo Jesus e Milagre (2016).

No Brasil, adotou-se primeiramente a legislação criminal onde são punidas condutas praticadas por intermédio ou contra sistemas informáticos. O direito dos cidadãos usuários veio retardamente com a Lei n. 12.965/2014 - Marco Civil da Internet.

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

O país tornou-se um dos maiores do mundo, em quinto lugar, com o maior número de fraudes virtuais[4]. Não somente está na rota dos crimes cibernéticos, mas os dados alarmantes mostram que a cada dez hackers no mundo, oito deles vivem no Brasil, segundo Jesus e Milagre (2016). Não obstante, na reportagem da época revelou que dois terços dos criadores de páginas de pedofilia na Internet eram de origem brasileira.

PROVA E FONTE DE EVIDÊNCIA DIGITAL

De acordo com Domingos (2017), a persecução penal de crimes efetiva se confirma pela participação internacional entre os países e suas instituições. Para que os delitos de violência e exploração sexual online não se percam faz-se necessário extensas medidas na obtenção das evidências à investigação e processamento deles.

As provas digitais podem ser encontradas em diversos dispositivos informáticos que se conectam à Internet tais como *smartphones, tablets,* relógios, plataformas de jogos, além da memória do computador pessoal do criminoso, relata Domingos (2017), o primeiro local onde os delitos de cunho pornográfico e/ou arquivos de imagens e vídeos ficam armazenados. Além destes, temos o armazenamento em nuvem, denominado *cloud computing*, arquivos que podem ser acessados remotamente e compartilhados para quaisquer lugares.

A obtenção das provas digitais para ser eficaz deve ser obtida o mais rápido possível, pois as vítimas, crianças, adolescentes, mulheres, podem ser "resgatadas" ao se interromper que um delito mais grave ocorra no mundo real, ou, que o criminoso que dissemina imagens particulares seja detido o mais breve possível, fazendo com que a vítima se sinta protegida diminuindo a proporção do dano pessoal.

CRIMES INFORMATICOS

Crime de informática, segundo Roque (2007), é "toda conduta, definida pela lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração". O criminoso se utiliza de dispositivos de informática para que suas práticas criminosas ou delitos sejam realizados.

A seguir, um breve levantamento dos principais artefatos, técnicas ou métodos informáticos relevantes para a prática de condutas que podem ser consideradas crimes de informática segundo Jesus e Milagre (2016).

Vírus

Espécie de *malware*. Um programa de computador que pode alterar dados ou sistemas, destruí-los e se replicar pela rede com o nome de *worm*.

[4] Disponível em: http://www20.opovo.com.br/app/opovo/dom/2016/01/23/noticiasjornaldom,3565860/crimes-ciberneticos-brasil-e-o-5-do-mundo-em-fraudes-digitais.shtml

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Trojan

Espécie e *malware*. Conhecido por "Cavalo de Troia" é um programa com instrução ou código malicioso ocultado por outro software que, uma vez instalado, permite que um computador fique vulnerável.

Sniffing

Técnica consistente em capturar pacotes de dados, transmitidos em redes TCP/IP.

Backdoor

Um código malicioso que permite acesso facilitado ao sistema ou máquina.

Spymare

Código ou programa malicioso instalado ou injetado em aplicativos cujas fontes são duvidosas.

Keylogging e screenlogging

Técnica para monitorar tudo o que é digitado pela vítima.

Defacement

Conhecido por "pichação de sites", usualmente, utilizada por *hackers* ou *crakers* em protestos. Prática equiparada a uma técnica.

Rootits

Software que corrompe a interface de um sistema fazendo como que ajam de forma diferenciada de suas aplicabilidades.

DoS e DDoS

O *Denial of Service* (ataque de negação de serviços) sobrecarrega um serviço informático para indisponibilizá-lo com técnicas, tais como inundação e pacotes, problemas de protocolo, ataque de disco, problemas de codificação, DDoS (*Distributed Denial of Service*), *pingflood*, etc.

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

DNS poisoning

Alterar endereços de resolução DNS (*Domain Name System* – Sistema de Nomes de Domínios)

Brute force

Técnica para quebra de senhas e acesso a sistemas que consiste em tentar todas as combinações possíveis.

Ataque e dicionário

Quebra de senhas, que consiste em testar palavras do dicionário.

Rainbow table

Quebra de senhas criptografadas, que consiste em submeter os *hashs* a uma tabela de *hashs* já calculados para realização de comparações.

Scanning

Técnica para varrer diversos hosts procurando por portas abertas, vulnerabilidades e informações.

Connection back

Técnica ou aplicação que o criminoso passa a ter acesso a máquina da vítima.

SQL injection

Técnica consistente em alterar parâmetros ou instruções que são executadas sobre uma ou mais tabelas de um banco de dados, por meio da linguagem SQL (*Structured Query Language).*

Buffer overfow

Uma vulnerabilidade que ocorre quando uma variável de um programa recebe mais informações do que ela foi posta para suportar.

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

Botnets

Sistemas instalados por criminosos digitais em estacoes servidoras fazendo com que uma máquina se torne "zumbi".

Session hijacking

Conhecido por sequestro de sessão onde o invasor descobre uma conexão TCP ativa entre duas máquinas assumindo o controle.

Arp poisoning

Placas Ethernet efetuam uma solicitação ARP para que o sistema informe qual MAC *Address* (endereço físico de um computador) está vinculado a determinado IP. Pacotes da máquina da vítima é enviado para o MAC do atacante.

Exploração do Kernel

O Kernel é o núcleo de sistemas operacionais e quando a subversão dele acontece, o criminoso digital pode se tornar invisível à programas de segurança da informação, etc.

Watering hole attack

Devido à dificuldade em invadir sistemas de empresas maiores, o criminoso digital procura invadir sistemas de parceiros da empresa alvo.

CONDUTAS INFORMATICAS

Condutas ou comportamentos podem ser relacionados a potenciais crimes próprios, tendo a informática como bem jurídico atingido, elucida Jesus e Milagre (2017).

Aponta-se como as principais condutas analisadas: o acesso ilegítimo (acesso não autorizado), a interceptação ilegítima, a interferência de dados (dano informático intencional e ilegítimo), a interferência em sistemas (obstrução grave, intencional e ilegítima), o uso abusivo de dispositivos (produzir, vender, distribuir), a falsidade ou fraude informática (introdução, alteração, eliminação de dados), a burla informática (ato intencional e ilegítimo que cause danos), o furto de dados ou vazamento de informações (copiar ou mover indevidamente), a pichação informática ou *defacement* (altera layout de páginas indevidamente, o envio de mensagens não

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

solicitadas (spam), e, por fim, o uso indevido informático (ainda que autorizado).

Diversos comportamentos podem caracterizar um crime digital, entre outros, atualmente, destacamos os crimes contra a honra, a discriminação, as fraudes bancárias, e, principalmente, para este estudo a pornografia infantil[5], bem como a divulgação de imagens indevidas com fins de coerção ou humilhação à mulher.

LEGISLAÇÃO SOBRE A PORNOGRAFIA INFANTIL INFORMÁTICA

De acordo com Jesus e Milagre (2017) a Justiça Federal e a Policia Federal por não terem condições de atenderem a demanda que ocorreria com as mudanças das leis fizeram com que elas não prosperassem, infelizmente.

Procuravam incluir à competência da Policia Federal sobre os delitos praticados contra ou mediante rede de computadores, dispositivos de comunicação ou sistema informatizado, não obstante, trazer penas mais severas para o delito de pornografia infantil e ampliar a competência por evidente quebra de pacto federativo contemplado na Constituição Federal, sendo assim todas as infrações observadas no Projeto da lei passariam a Justiça Federal

TIPOS PENAIS PREVISTOS NO ECA (LEI N 8.069/90)

As hipóteses tratadas nos artigos de 241 a 241-D[6], relacionados a seguir, são os concernentes aos delitos informáticos próprios ou impróprios, ou seja, em que o crime pode ser praticado somente pelo meio Internet, bem como por intermédio dela ou outro meio.

> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. (Redação dada pela Lei nº 11.829, de 2008)
> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1o Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; (Incluído pela Lei nº 11.829, de 2008)
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
> § 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o

[5] Vale lembrar a diferença entre pedofilia e pornografia infantil. A pedofilia resulta da perversão sexual onde o adulto tem contato erótico om a criança ou adolescente, sendo que a pornografia infantil e a comercialização ou distribuição de fotos pornográficas ou eróticas com crianças ou adolescentes utilizando a internet como meio facilitador, segundo Rosa (2002).
[6] Disponível em < http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
§ 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
§ 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: (Incluído pela Lei nº 11.829, de 2008)
I – agente público no exercício de suas funções; (Incluído pela Lei nº 11.829, de 2008)
II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; (Incluído pela Lei nº 11.829, de 2008)
III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. (Incluído pela Lei nº 11.829, de 2008)
§ 3o As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido. (Incluído pela Lei nº 11.829, de 2008)
Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008)
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. (Incluído pela Lei nº 11.829, de 2008)
Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: (Incluído pela Lei nº 11.829, de 2008)
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
Parágrafo único. Nas mesmas penas incorre quem: (Incluído pela Lei nº 11.829, de 2008)
I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; (Incluído pela Lei nº 11.829, de 2008)
II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita. (Incluído pela Lei nº 11.829, de 2008)

CRIMES INFORMÁTICOS E A LEGISLAÇÃO NO MUNDO

Apesar de o Brasil tomar um rumo contrário, ao adotar primeiro a legislação criminal, objetivando punir condutas contra sistemas de informática, deixando em segundo plano os direitos dos usuários - com a Lei n.12.965/2014, denominando assim o Marco civil da internet, juntamente com o Chile – com a Lei n. 20.453/2011 são os países que apresentaram as mais avançadas regulamentações. Nesse sentido, visam a garantia de direitos civis, a promoção da cidadania e, por fim, o uso democrático da internet, segundo Segurado, Lima e Ameni (2014):

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

> Apesar das diferentes opiniões dos representantes da sociedade civil envolvidos no debate, podemos afirmar que ambos os países apresentam posições mais democráticas em relação ao caráter da regulamentação da internet, possibilitando que ela mantenha o princípio livre, aberto e colaborativo. Por outro lado, Espanha e França se apresentam como os defensores de maior controle dos acessos à rede, e, nos EUA, apesar das grandes barreiras jurídicas para impor o fim da neutralidade de rede, a Comissão Federal de Comunicações está preparando novas formas para acabar com esse princípio. A privacidade, a segurança e a vigilância encontram as posições mais retrógradas nos EUA, seguidos de França e Espanha.

Uma breve nota de alguns países do mundo em torno da temática dos crimes de informática, exemplifica Jesus e Milagre (2017).

Estados Unidos

Debates iniciados em meados da década de 1970 sendo promulgada a *Computer Fraud and Abuse Act* em 1986. Em 1994, a Lei dos Crimes Violentos, *Violent Crimes Act,* tipificou condutas como dano a dados e sistemas, disseminação e vírus e intercepção telemática.

Filipinas

Notoriamente, em 2012, fora aprovada pelo Senado a redação final da *Bill 2976: The Cybercrime Prevention Act of 2012.*

Emirados Árabes

Em 2012, fora promulgada a punição de condutas do uso da internet para fins de transmissão, publicação e promoção de atos pornográficos e/ou indecentes.

Inglaterra

A *Data Protection Act*, legislação de 1984 que já protegia dados pessoais no mundo da informática. Em 2014, a pena de prisão perpetua para crimes cibernéticos foi proposta no Parlamento das 11 novas leis – *Serious Crime Bill.*

MARCO CIVIL DA INTERNET

Considerado a "Constituição da Internet", a Lei n. 12.965/2014[7], visa a garantir os direitos e deveres dos usuários, dos provedores de conexão e de serviços em geral, ou seja, de todos os envolvidos na Internet.

Os principais pontos do objetivo da lei são a garantia de liberdade de expressão e de privacidade. O

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

Marco Civil da Internet tem como objetivo primordial oferecer segurança jurídica pois não havia até os dias atuais um específico instrumento regulatório da internet. O que decorria, no Brasil, a jurisprudência vinha sendo construída de forma aleatória e, diversas vezes, contraditória.

Em suma, a nova lei proporciona os fundamentos, princípios, objetivos e direitos na utilização da rede mundial de computadores, além de criar normas processuais para a proteção dos mesmos. Dessa forma, estabelece-se um marco legal que certamente uniformizará entendimentos, muitas vezes, controversos nos tribunais.

METODOLOGIA

Levantamento estatístico quantificador dos crimes sexuais na internet no estado do Rio de Janeiro (RJ). Tabulação de todos os registros, tais como reclamações e ocorrências discussão da legislação brasileira. Inclui-se a pesquisa bibliográfica, coleta de dados na Polícia Estadual, na delegacia própria do assunto e consultas à legislação nacional e à estrangeira.

Não obstante, uma análise dos boletins de ocorrência registrados na delegacia de repressão aos Crimes de Informática (DRCI) nos últimos dois anos (2013 e 2014) no estado do RJ. Acrescentou-se a este estudo os anos de 2015 e início de 2016.

RESULTADOS

O ciberespaço, definido como um mundo virtual e caracterizado pelo complexo de fluxos informacionais e de comunicação além-fronteiras, amplia a vulnerabilidade dos adolescentes, das mulheres, dos desatentos ao conjunto de informações danosas que tanto podem contribuir para sua própria vitimização, pela forma como deliberadamente se expõem, como podem ser enganados financeiramente por criminosos atrás de um computador ou links.

Os crimes na internet, ou cibercrimes, têm se tornado prática constante no Brasil. Os delitos vão desde os que afetam as pessoas individualmente até crimes que atingem a sociedade como a pedofilia e crimes de ódio.

Algumas crianças, que têm acesso precocemente à rede mundial, podem estar mantendo contatos com adultos que se identificam como pessoas da mesma faixa-etária a partir de perfis falsos, criados com a finalidade deliberada de estabelecer comunicação com crianças e adolescentes, e, a partir disso, ter acesso a imagens, informações e dados sobre sua intimidade. Infelizmente, esses crimes estendem-se a adultos, como as mulheres na maioria das vezes. Vítimas de ex-parceiros tem intimidade exposta indevidamente na internet.

[7] Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

Para muitos usuários das novas tecnologias da informação, o ciberespaço proporciona acesso à informação e entretenimento, construção de espaços coletivos inteligentes e oportunidades de estabelecer novos fluxos comunicacionais, facilitando o contato virtual entre pessoas espalhadas por diversas regiões do mundo. Para outros, entretanto, este ambiente equivale a um território sem lei, o que justificaria todo o tipo de conduta, já que seria um espaço à parte, subtraído de qualquer ingerência ou censuras sociais, o que possibilitaria desde a prática de atos que não seriam realizados em contatos de face a face em razão das regras de boa convivência, até o estabelecimento de redes invisíveis de criminalidade. É esta compreensão do ciberespaço como território sem lei que tem preocupado jurídicos e estudiosos do tema, pois a partir dela tem se proliferado os atos de violação aos direitos fundamentais de crianças e adolescentes, com destaque para os abusos de natureza sexual.

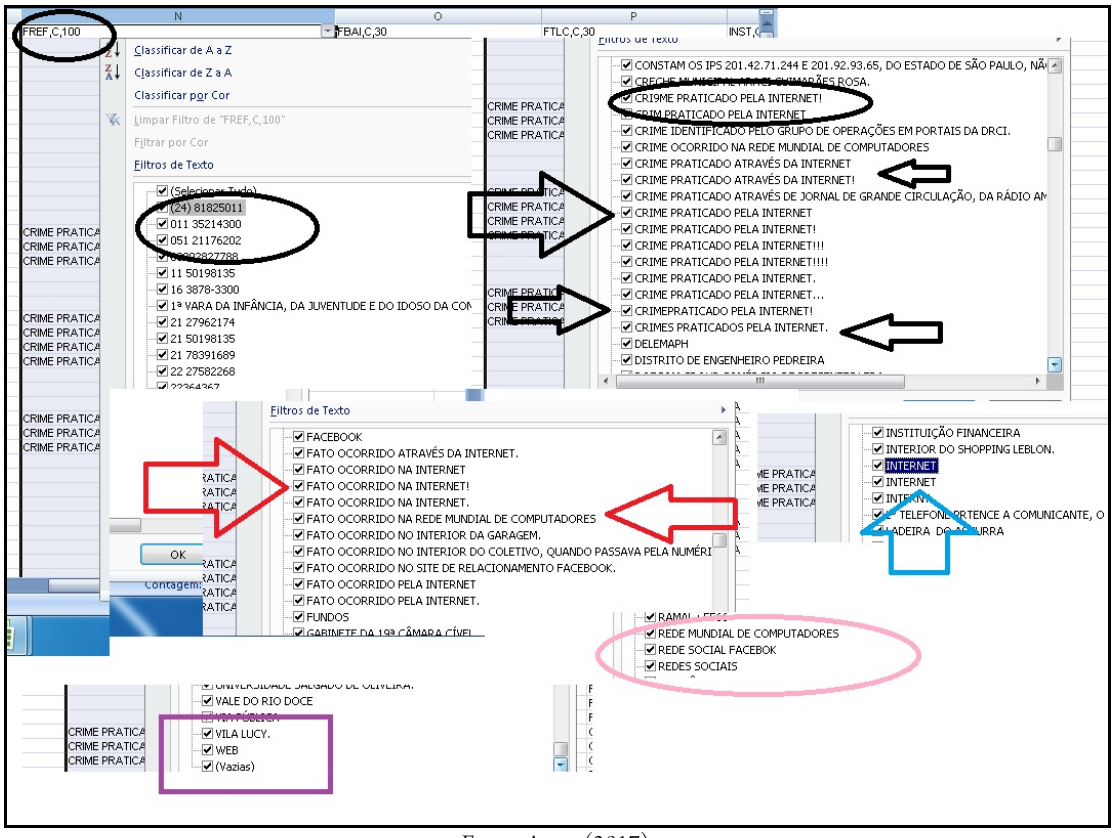
Não obstante, segundo dados do SaferNet Brasil, associação civil sem fins lucrativos e com alcance nacional, uma mulher a cada hora é vítima de crime sexual no Brasil. É o crime contra honra, quando denigre a imagem, que mais acontece, mas nem todas as pessoas denunciam, acalentando baixos índices nos levantamentos realizados, pois a maioria delas acredita que terá maior exposição caso a denúncia seja realizada e com isso não temos uma grande incidência de denúncias que possa refletir estatisticamente.

Atentando a esse fato e pela relevância que a mídia tem dado a esses crimes, solicitamos mais dados do último ano, de 2015 e início de 2016, para um levantamento mais eficaz desta pesquisa.

Os dados oferecidos pela central de informática do DRCI possuem problemas no cadastro. As referências não seguem padrões, conforme Figuras 1 e 2. Minuciosamente selecionei as denúncias de crimes de informática que ora eram cadastrados como web ora como internet, entre outros nomes relacionados à internet. Não obstante, muitos erros de digitação. Houve grandes melhorias na última coleta de dados observadas.

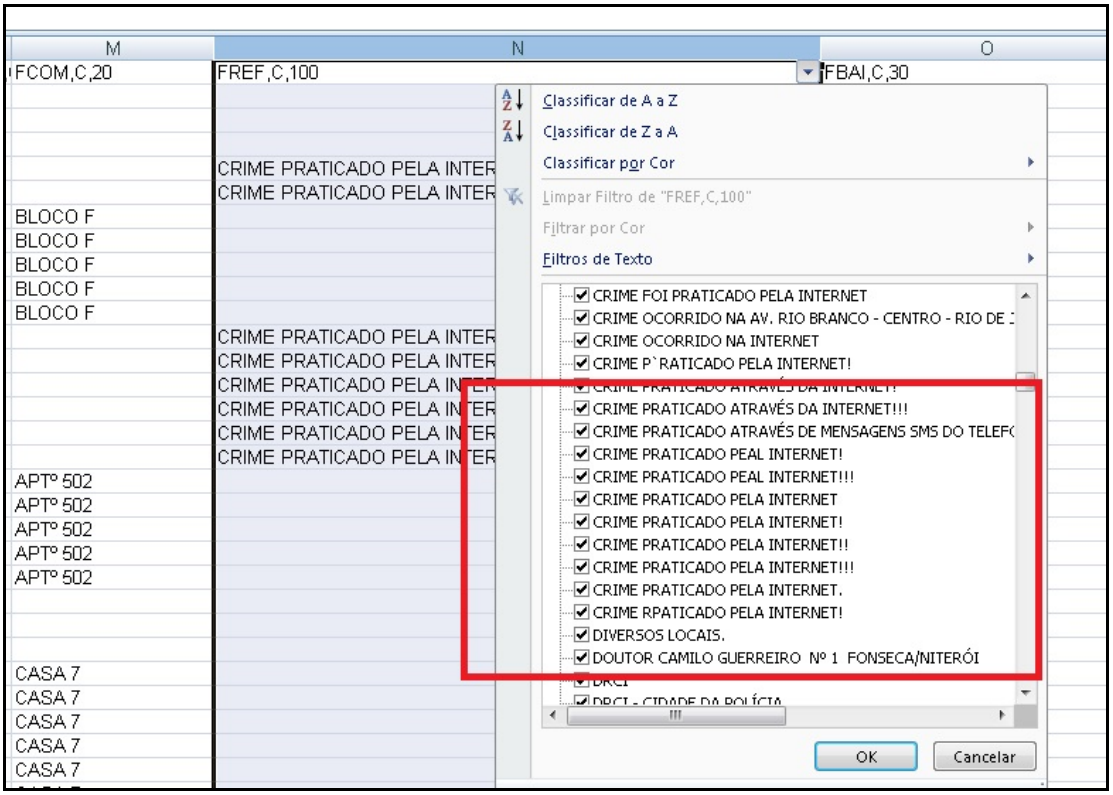
vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Figura 1: Cadastro 2013



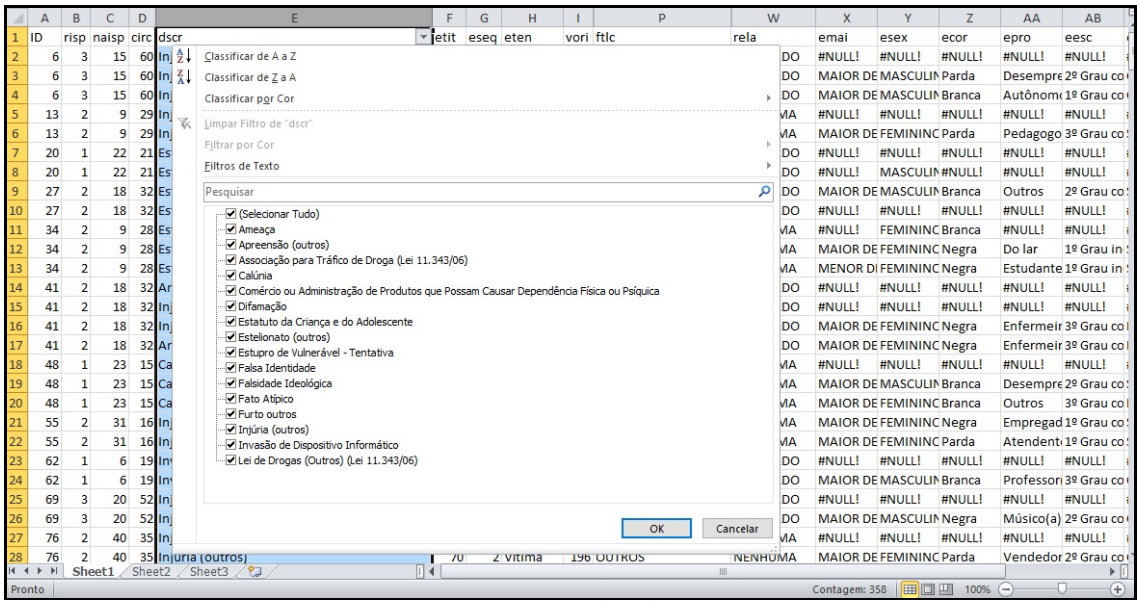
Fonte: Autor (2017).

Figura 2: Cadastro 2014



vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Figura 3: Cadastro 2016



Fonte: Autor (2017).

Para o ano de 2013 obtivemos resultados parciais de 2106 vítimas de algum tipo de crime reportado, sendo que destas 471 denúncias registradas no DRCI eram sobre crimes de informática. Das 368 vítimas, 179 são do sexo feminino. Observamos que 152 são do sexo feminino e maiores de idade. Com relação ao objetivo geral desta pesquisa, infelizmente, deparamo-nos com 25 denúncias relativas aos crimes sexuais. Observar as figuras 4, 5 6 com seus gráficos detalhados abaixo.

Figura 4

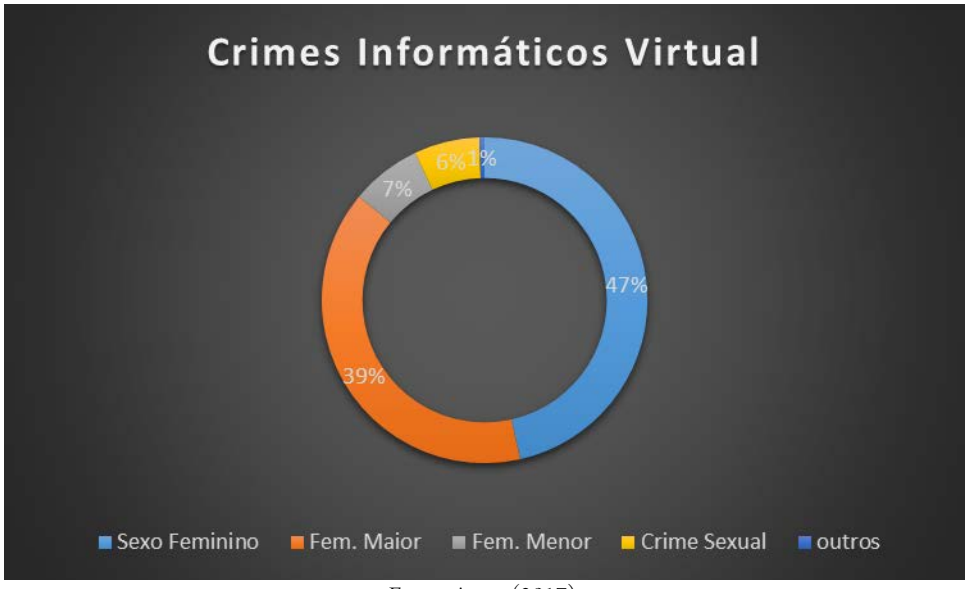
Fonte: Autor (2017).

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Figura 5

Fonte: Autor (2017).

Figura 6



Fonte: Autor (2017).

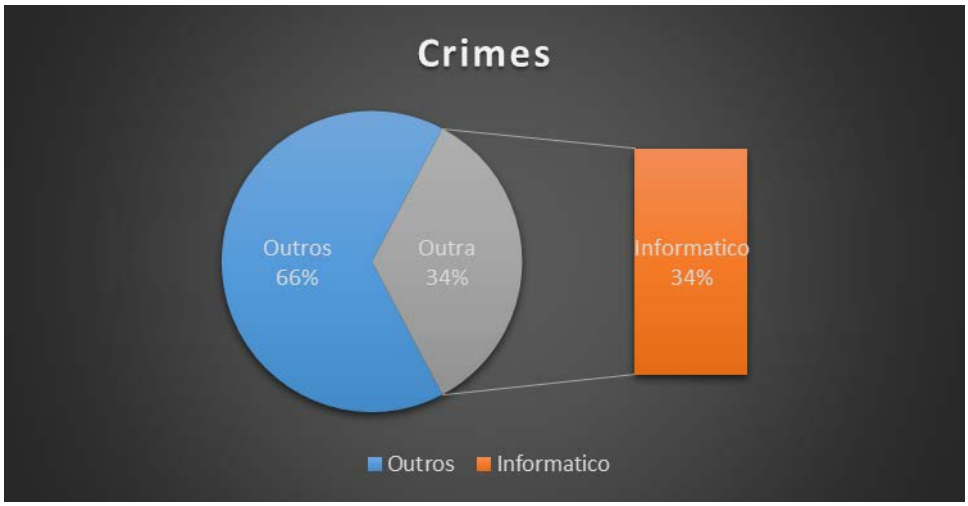
Para o ano de 2014 ocorreu um declínio de 10 denúncias, num total de 15 relativas à ordem de crimes sexuais. Posteriormente, tentaremos elaborar estudos sobre os motivos pelos quais as denúncias não foram registradas até esse ano. Dessa forma, fazem-se necessários maiores dados de outros anos para respaldar conclusões sobre a base de dados do DRCI.

Para finalizar o ano de 2014, foram 1640 vítimas de algum tipo de crime. Dessas, 983 são do sexo feminino. Não obstante, ocorreram 565 denúncias de crimes cibernéticos. Das 210 vítimas de algum crime virtual,

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

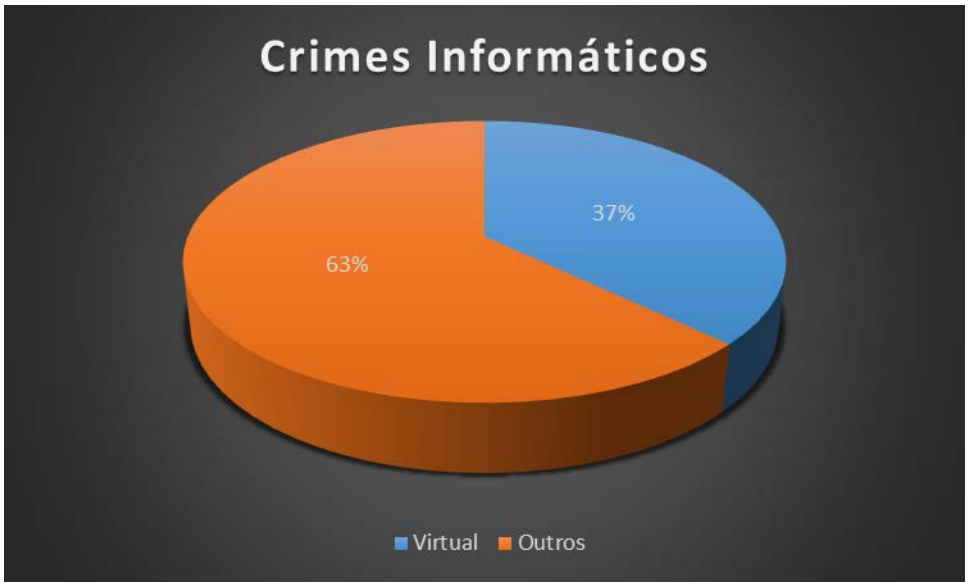
135 são do sexo feminino e 109 maiores de idade. Denúncias com menores de idade e do sexo feminino foram de 26. Conforme mostram as figuras 7, 8 e 9 a seguir.

Figura 7



Fonte: Autor (2017).

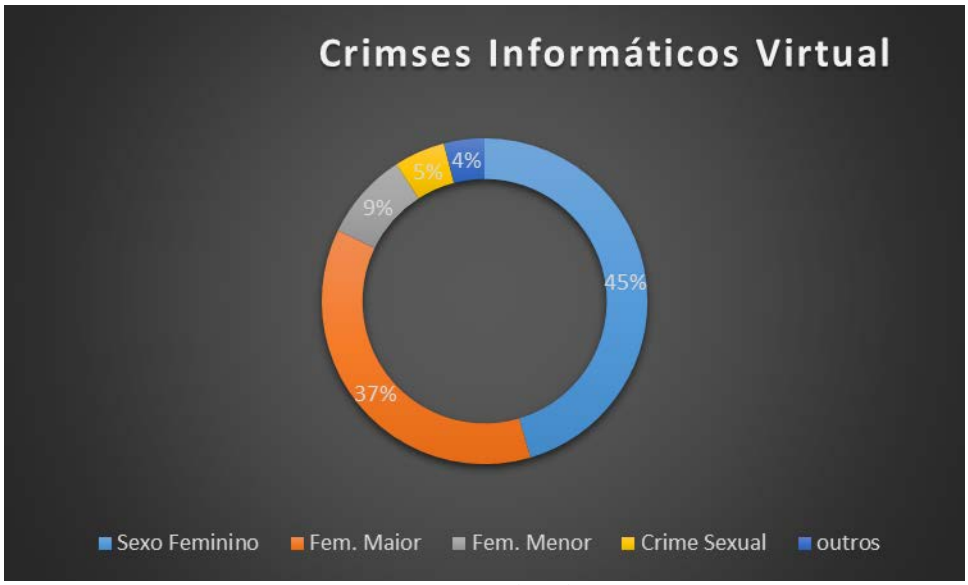
Figura 8



Fonte: Autor (2017).

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

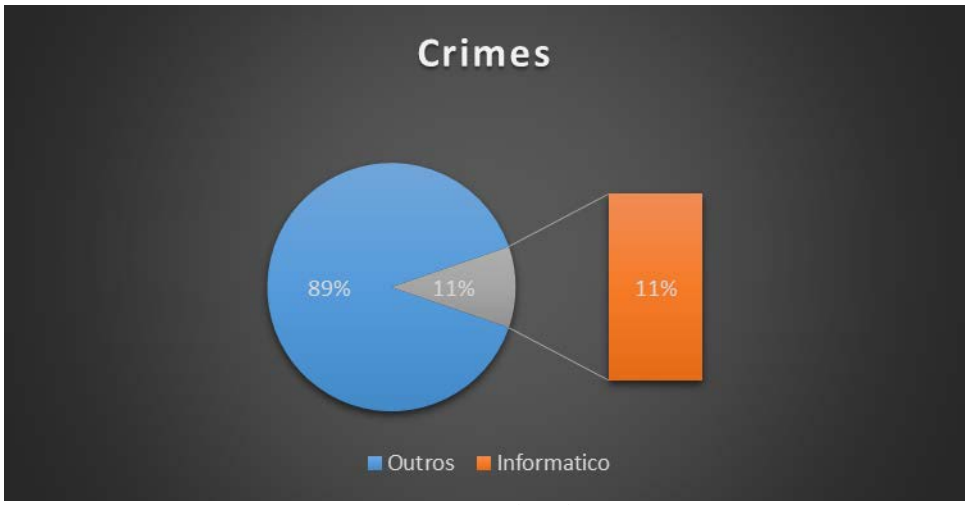
Figura 9



Fonte: Autor (2017).

Em 2015, resultados parciais de 1552 vítimas mostram algum tipo de crime reportado, sendo que destas 164 denúncias registradas no DRCI eram sobre crimes de informática. Destas 64 estão no ambiente virtual e 38 são do sexo feminino que estão envolvidas nos crimes sexuais. Observamos que 11 são do sexo feminino e menores de idade. Com relação ao objetivo geral desta pesquisa, infelizmente, deparamo-nos com 25 denúncias relativas aos crimes sexuais. Os dados são demonstrados nas figuras 10, 11 e 12, abaixo.

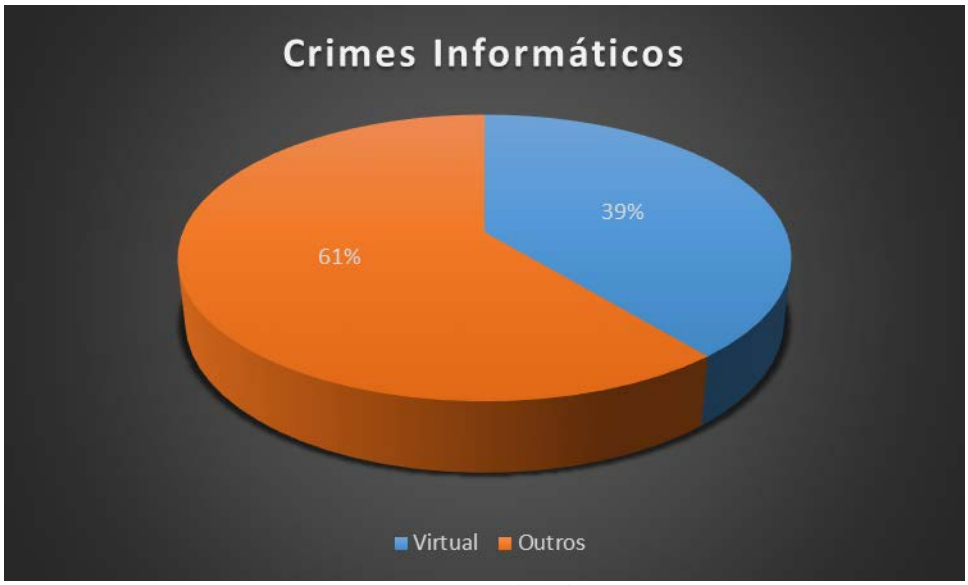
Figura 10



Fonte: Autor (2017).

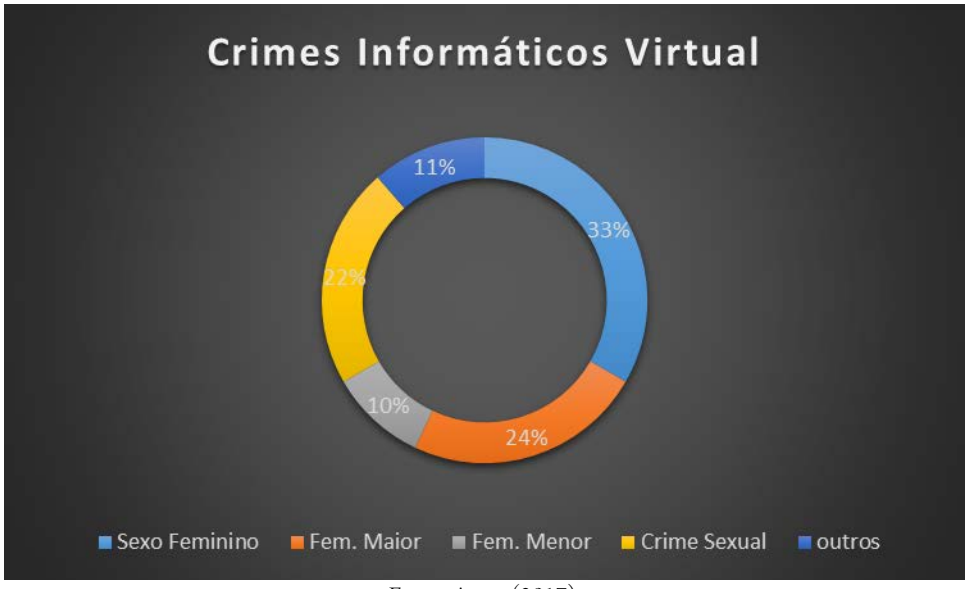
vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Figura 11



Fonte: Autor (2017).

Figura 12

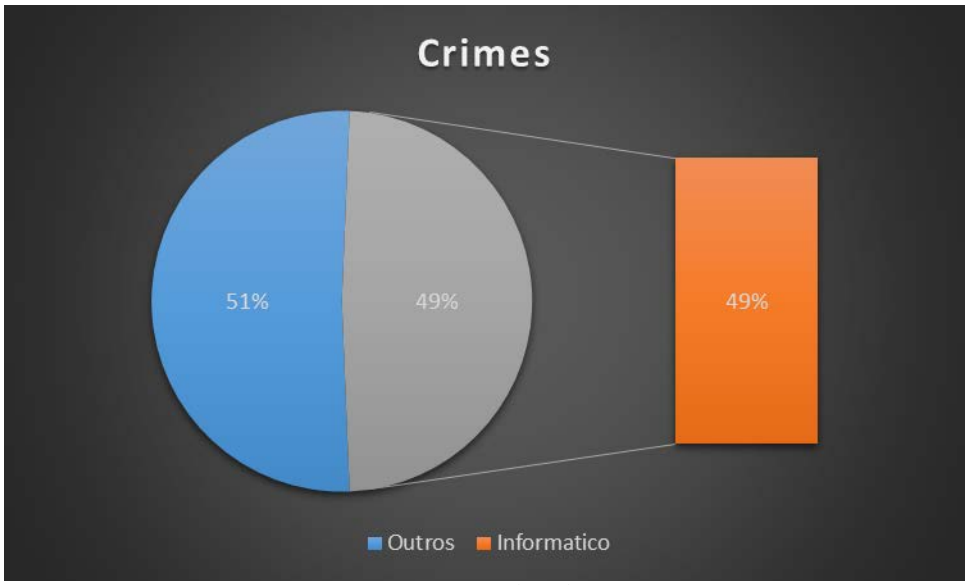


Fonte: Autor (2017).

Por fim, os últimos resultados apurados, em janeiro de 2016, constam 156 denúncias de crimes sendo 76 relacionadas à crimes sexuais e de informática. Destes, 11 ocorreram em ambiente virtual e 3 com vítimas do sexo feminino, todas maiores de idade. Não fora especificado a ordem de crime sexual. Por fim, seguem as figuras 13, 14 e 15, e os gráficos da última coleta de dados.

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Figura 13



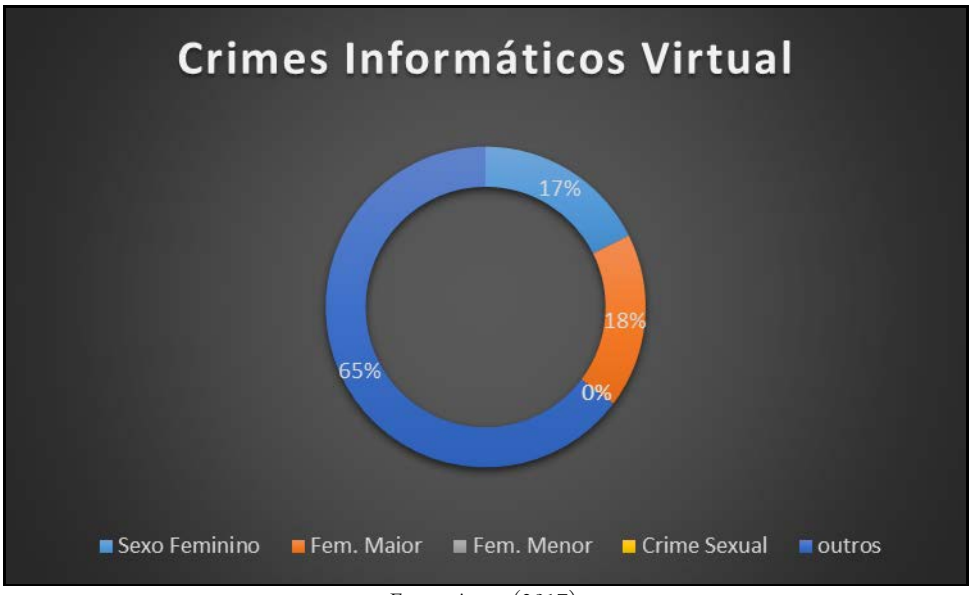
Fonte: Autor (2017).

Figura 14

Fonte: Autor (2017).

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

Figura 15



Fonte: Autor (2017).

CONSIDERACOES FINAIS

A partir dos estudos, aqui propostos, pretendeu-se alcançar os objetivos apresentados no projeto. Dessa forma, espera-se um mapeamento inédito e estratégico no estado do Rio de Janeiro sobre os crimes sexuais na internet.

A coleta de dados não fora expressiva mesmo com o aumento de denúncias referentes aos crimes sexuais pelo uso da internet nos últimos anos. Entendemos a necessidade de expandir além dos últimos dois anos para três anos e pouco, finalizando este em janeiro de 2016.

As denúncias referentes aos crimes sexuais pelo uso da internet têm-se aumentado nos últimos meses. Diversos fatores estão relacionados a esse episódio. Os meios de comunicação têm dado maior espaço para estes crimes e midiaticamente pela virilizacao dos espaços virtuais coletivos, mediante interesse do público de massa.

Com os resultados obtidos, esperamos que se utilize de respaldo para trabalhos futuros concernentes à questão tão crucial nos dias atuais. Almeja-se uma maior atenção a estes crimes pontuais, e, que a legislação se atente às resoluções incisivas destes problemas na nova era da informação.

SEXUAL CRIMES AGAINST SEXUAL DIGNITY THROUGH THE USE OF THE INTERNET - A CRITICAL REVIEW OF BRAZILIAN LEGISLATION

Abstract
This work presents to the reader the consolidation of the understanding about sexual crimes with the use of the internet, as analyzed and legally by Brazilian legislation. The contribution of technological advances is undeniable. However, the uncontrolled growth of Internet access has facilitated the practice of illegal activities, such as the

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944 - 964
DOI: 10.12957/rqi.2018.29848

dissemination of child pornography, fraud, sexual crimes, etc. The objective is to make an analysis of the law compared to the international legislation on the subject of computer crimes and at the same time to discuss the incidence of this type of crime in the state of Rio de Janeiro (RJ). In this work a statistical quantification survey of the sexual crimes in the internet in the state of Rio de Janeiro (RJ) and the tabulation of all the records by the analysis of the reports of occurrence registered in the police station of repression to the Crimes of Informatics (DRCI) in the last three (2013, 2014, 2015 and early 2016). In this work, we obtained a non-expressive data collection even with the increase of denunciations related to sexual crimes by the use of the Internet in recent years. It is hoped that with the results of the survey, it will be used to support future work concerning the crucial question nowadays.

Keywords: Internet; Technology; Forensic Computing; Sexual Crime; Legislation.

REFERÊNCIAS

ANDRADE, Maria Margarida. **Introdução à metodologia do trabalho científico**. São Paulo: Atlas; 151 p. 1997.

ASCENSÃO, Jose de Oliveira. **Direito da Internet e da Sociedade da Informação**. Rio de Janeiro: Forense. 2002.
ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: http://jus.com.br/artigos/2250. Acesso em 9 jan. 2015.

BRASIL, Associação brasileira de normas técnicas. **NBR 6023:** informação e documentação: referências: elaboração. Rio de Janeiro; 24 p. 2002.
_____Presidência da República**. Lei n.8089/90, de 13 julho 1990**. Brasília, 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L8069.htm. Acesso em 26 jul. 2017.
_____Presidência da República. **Lei n.12965/2014, de 23 abril 2014**.Brasilia, 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 26 jul. 2017.
_____Universidade do Estado do Rio de Janeiro. Rede Sirius – Rede de Bibliotecas UERJ. **Roteiro para apresentação das teses e dissertações da Universidade do Estado do Rio de Janeiro.** 2. ed. rev. atual. e ampl. Rio de Janeiro; 142 p. 2012.

CABRAL, BF. **Direito comparado: os órgãos de segurança pública e a persecução criminal no Brasil e nos Estados Unidos.** Jus Navigandi, Teresina, ano 14, n. 2150, 21 maio 2009. Disponível em: http://jus.com.br/artigos/12905. Acesso em 8 já. 2015.

CASEY, Eoghan. **Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.** 3 th ed. EUA: Elsevier. 2011.

CAVALCANTE, Ana Mary C. **Crimes Cibernéticos. Brasil é o 5º do mundo em fraudes digitais**, 24 janeiro 2016. Disponível em: http://www20.opovo.com.br/app/opovo/dom/2016/01/23/noticiasjornaldom,3565860/crimes-ciberneticos-brasil-e-o-5-do-mundo-em-fraudes-digitais.shtml. Acesso em 25 jul. 2017.

CRESPO, Marcelo Xavier Freitas. **Crimes Digitais.** 2. ed. São Paulo: Saraiva. 2011.

vol. 11, nº. 02, Rio de Janeiro, 2018. pp. 944- 964
DOI: 10.12957/rqi.2018.29848

DOMINGOS, Fernanda Teixeira Souza. [et al.]. **Crimes Cibernéticos. A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual infantil online.** 1 ed. Porto Alegre: Livraria do Advogado. 2017.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** 1.ed. São Paulo: Novatec. 2011.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional - Teoria e Prática Aplicada**. 1. ed. EUA: Prentice Hall Brasil. 2007.

JESUS, Damásio de; MILAGRE, Jose Antonio. **Manual de crimes informáticos.** 1 ed. São Paulo: Saraiva. 2016.

JEWKES, Yvonne; YAR Majid. **Handbook of Internet Crime**. EUA: Routledge. 2010.

SILVA, Rita de Cassia. **Direito penal e sistema informático.** São Paulo: Revista dos Tribunais. 2003.

SILVA, Mario Camarinha da; Brayner, Sonia. **Normas técnicas de editoração: teses, monografias, artigos e papers**. 3. ed. Rio de Janeiro: Editora UFRJ. 1995.

SOUZA, Artur de Brito Gueiros; JAPIASSÚ, Carlos Eduardo Adriano. **Curso de direito penal: parte geral.** Rio de Janeiro: Elsevier. 2012.

ROQUE, Sergio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador**. 1 ed. São Paulo: ADPESP Cultural. 2007.

ROSA, Fabrizio. **Crimes de Informática**. 2. ed. Campinas: Bookseller. 2002.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandu; AMENI, Cauê. S. **Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França**. Hist. Cienc. Saúde - Manguinhos, Rio de Janeiro, v. 22, supl. p. 1551-1571, dec.2015. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-59702015001001551&lng=en&nrm=iso>. Acessado em 31 jul 2017.

SYDOW, Spencer Toth. **Crimes Informáticos e Suas Vítimas**. São Paulo: Saraiva. 2015.

Trabalho enviado em 01 de agosto de 2017.
Aceito em 11 de novembro de 2017.