Similitude de Ocorrências de CSAM na Internet e o Registro Perante às Autoridades no Estado de São Paulo

Hericson dos Santos[1], **Jorge A. D. Barreto**[1], **Nicole V. Dalarmelina**[1], **Marcio A. Teixeira**[2], **Rodolfo I. Meneguette**[1]

[1]Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo (USP) São Carlos, SP – Brasil.

[2]Instituto Federal de São Paulo (IFSP) - Campus Catanduva
Catanduva, SP – Brasil.

{hericson.santos, jorge.barreto, nicole.dalarmenila}@usp.br

meneguette@icmc.usp.br, marcio.andrey@ifsp.edu.br

Abstract. *The scientific scope of this article is to draw a similarity between LE (Law Enforcement) records and the sharing of Child Sexual Abuse Materials (CSAM), one of the crimes carried out in the Child and Adolescent Statute, and its effective virtual distribution. For this intent, police monitoring software was used to monitor peer-to-peer networks, having as a methodological cut as occurrences, both of effective sharing of material and of LE occurrence records, observed only in the State from Sao Paulo. Finally, the study is able to demonstrate that police records faithfully reflect the location of occurrences, albeit in smaller numerical proportions compared to virtual ones.*

Resumo. *O presente artigo tem por escopo científico traçar a similitude entre os registros policiais relativos ao compartilhamento de materiais de abuso sexual infantil (CSAM), um dos crimes previstos no Estatuto da Criança e do Adolescente e a sua efetiva distribuição virtual. Para tal fim, foi utilizado um software policial de monitoramento sobre as redes de pares (P2P), tendo por recorte metodológico as ocorrências, tanto de compartilhamento de efetivo de material como de registo de ocorrência policial, observadas tão somente no Estado de São Paulo. Por fim, o estudo é capaz de demonstrar que os registros policiais refletem, de maneira fiel, a localidade das ocorrências, ainda que em proporções numéricas menores em relacão às virtuais.*

1. Introdução

A popularização da Internet como consequência direta da inclusão digital promovida por muitos países, inclusive no Brasil, com a expansão da banda larga de comunicação, as redes móveis e as novas tecnologias disponíveis nas mãos das pessoas se tornou algo inevitável. Hoje não há quem não tenha pelo menos um *smartphone*, mesmo nas camadas mais baixas da população [Freitas et al. 2015]. Esse fenômeno digital proporcionou

inúmeros benefícios para as pessoas, entretanto, também trouxe o incremento das mais variadas atividades criminosas, principalmente crimes contra a dignidade sexual de crianças e adolescentes.

A OMS – Organização Mundial da Saúde (1975, p.199), em seu manual de doenças, informa que o termo "pedofilia", no capítulo de transtornos mentais, no que tange às Neuroses, Transtornos de Personalidade e outros Transtornos Mentais Psicóticos, sob o código 302 – Desvio Sexual, subcódigo 302 é uma doença [OPAS 1980].

Já o ordenamento jurídico brasileiro [Lei 1990] vai no sentido contrário. Em diversos dispositivos legais trata o tema como crime, principalmente após o advento da Lei nº 8.069/1990 que instituiu o ECA – Estatuto da Criança e Adolescente, bem como as alterações trazidas pela Lei nº 11.829/2008 que acrescentou ao estatuto vários dispositivos definindo como crimes as diversas modalidades de condutas contra crianças e adolescentes cometidos por meios eletrônicos, notadamente na Internet.

Em relação ao que se entende pelo termo "pedofilia" é necessário expor duas linhas de pensamento distintos: a primeira, formada por especialistas da saúde e a segunda por operadores das ciências jurídicas. Enquanto uns defendem que "pedofilia"é uma doença; outros afirmam que esta conduta se trata, tão somente, de um desvio de caráter, devendo ser tratada como crime.

Num contexto contraditório como o exposto, as autoridades que investigam os crimes relacionados a esta conduta têm evitado utilizar o termo "pedofilia" para designar o crime, adotando a expressão "abuso sexual infantil". De maneira análoga, não se referem ao investigado como "pedófilo", mas sim como "predador" ou "abusador infantil".

No Brasil, o tema tomou notoriedade no ano de 2012, quando foi realizada uma audiência pública na Câmara dos Deputados em Brasília [dos Deputados 2003]. Na ocasião, várias autoridades, sociedades de proteção infantil e empresas de Internet foram ouvidas pelos parlamentares.

Após esta audiência, os principais buscadores de conteúdo e portais brasileiros se comprometeram a realizar ações no sentido de deixar de indexar palavras-chaves relacionadas à exploração sexual infantil. Assim, ao pesquisar o termo em inglês: *pthc – preteen hard core*, definido como o principal indexador na busca de CSAM na Internet, a ferramenta de busca retornará ao usuário avisos informando dessa prática criminosa, assim como as diversas operações policiais de repressão a estes crimes.

Apesar do cenário Brasileiro ter evoluído positivamente na *surface web* (internet indexada) após a referida audiência, ainda é possível realizar a busca por este tipo de material criminoso nas redes de compartilhamento P2P – ponto a ponto, na chamada *deep web* e na sua porção mais escura: a *dark web*. Estas são porções da Internet não indexadas pelos motores de busca convencionais.

O Napster, em 1999, foi o primeiro programa de compartilhamento de arquivos em redes P2P. Através dele seus usuários compartilhavam, basicamente, músicas no formato MP3, sendo o programa protagonista de uma disputa judicial envolvendo as principais

gravadoras e distribuidoras da indústria fonográfica mundial. Com esta disputa, o Napster foi retirado do ar em meados do ano 2000 pela justiça americana por infringir leis de direitos autorais, mas o seu legado persiste até hoje.

Os programas e aplicativos que atuam nas redes P2P não são ilegais, mas a troca de arquivos geralmente infringe normas e legislações internacionais, especialmente de direitos autorais e, no contexto do presente artigo, distribuição de material contendo cenas de abuso sexual infantil – *CSAM (Child Sexual Abuse Material)*.

Existem centenas de programas de compartilhamento de arquivos operando, basicamente, em cinco redes de protocolo de transferência P2P: umas operam no limite da *surface web*, enquanto outros já operam dentro da chamada *deep web*, utilizando, além do protocolo de troca de arquivos ponto a ponto, várias camadas de criptografia que dificultam o trabalho de identificação dos autores de crimes virtuais, notadamente aqueles contra a dignidade sexual de crianças e adolescentes.

Assim, este trabalho realiza o mapeamento do compartilhamento de materiais de CSAM, obtidos através dos registros policiais, e sua efetiva distribuição com os conteúdos que são compartilhados nas redes P2P. Para isso, utilizamos as bases policiais de monitoramento sobre as redes de pares (peer-to-peer), tendo como recorte metodológico as ocorrências de compartilhamento do efetivo material como também o registro de ocorrência policial. Com isso, é possível demonstrar a correlação dos registros policiais nas plataformas P2P com a localidade das ocorrências físicas de violência contra crianças.

O resto do artigo está organizado da seguinte forma: na Seção 2 são apresentadas algumas tecnologias P2P utilizadas para compartilhamento de arquivos, inclusive CSAM. Na na Seção 3 são descritos os trabalhos relacionados com os estudos e mapeamentos de CSAM. Na Seção 4 são discutidos os resultados do mapeamento dos dados compartilhados nas redes P2P com os atos realmente ocorridos. Por fim, na Seção 5 são apresentadas as conclusões finais e diretrizes para trabalhos futuros.

2. Fundamentação Teórica

As principais redes P2P em operação no mundo e que, frequentemente, são investigadas pelas autoridades e especialistas em crimes virtuais e perícia computacional são:

2.1. Gnutella/Gnutella2

Essa rede é a que mais possui programas clientes, sendo o *Shareaza* o seu principal expoente. Os dispositivos informáticos que se conectam à rede Gnutella são chamados de pontos [Adar 2000]. Ela utiliza o conceito de busca binária para proporcionar escalabilidade e eficiência durante o seu funcionamento. Através do seu algoritmo, a rede escolhe, dentre os pontos conectados, aqueles com características especiais (velocidade da conexão de internet do par, disponibilidade da conexão, quantidade de índices). Quando a rede se depara com pontos com estas características, ela os eleva à categoria de *ultrapeers* (ultrapontos), assim, toda pesquisa passará por algum ultrapeer que servirá de "catálogo de índices", ou seja, um ponto de apoio da rede Gnutella para aumentar a sua eficiência. Após o encontro da fonte a ser transferida, ou seja, o arquivo desejado, o handshake

(fechamento da comunicação), sua transmissão é feita ponto a ponto, entre solicitante e fornecedor.

2.2. Ares

Essa rede possui apenas um programa cliente: o *Ares Galaxy* [Galaxy 2020]. Os dispositivos informáticos que se conectam a ela são chamados de nodes (nós). Ela utiliza o conceito de busca binária, assim como a rede Gnutella, e também escolhe dentre os nodes aqueles com características especiais (velocidade da conexão de internet do par, disponibilidade da conexão, quantidade de índices), elevando-os à categoria de supernodes. Há uma grande diferença entre a Ares e as demais redes P2P, qual seja: quando um node é elevado a esta categoria, ele recebe uma lista de todos os arquivos que os nodes conectados a ele possui. Assim, o supernode formará um gigantesco catálogo de arquivos que é consultado durante uma pesquisa. Se um dos nodes conectado ao supernode se desconectar enquanto um dos seus arquivos é requisitado, dentre a lista que o supernode possui, a rede retornará que o arquivo não está mais disponível e procurará por outras fontes (outros nodes que possuam o mesmo arquivo). Essa movimentação da rede consome certo tempo, causando o que se conhece por tempo de latência da rede. Uma vez encontrado o arquivo, o supernode sai de cena e dá lugar à transferência direta dos arquivos.

2.3. eDonkey

O eDonkey possui como programas clientes as variantes do *eMule* e *eMule2000*. É chamada de rede híbrida, pois possui em sua arquitetura a estrutura de uma rede centralizada, onde um nó serve aos demais clientes [Heckmann et al. 2004], incorporando ao longo dos anos, o conceito de sistema de rede descentralizada com a introdução do DHT – (*Distributed Hash Table*) utilizada em larga escala pelas redes Bittorrent e na validação das transações de criptomoedas. Os dispositivos informáticos que se conectam a ela são chamados de *peers* (pontos). Ela utiliza o conceito de busca binária, assim como as demais redes já estudadas. Um fator importante desta rede é que ela exige que o ponto, durante o *download* (recebimento) do arquivo, também seja fornecedor de partes dele, sob pena de sua velocidade de download ser reduzida substancialmente

2.4. Bittorrent

O Bittorrent [Inc 2021] possui arquitetura de rede descentralizada utilizando o conceito de DHT. Um dos principais programas clientes é o uTorrent. Os dispositivos informáticos que se conectam a ela são chamados de peers. A transmissão é feita a partir de pequenos fragmentos do arquivo original na sua notação hash, alcançando o limite de velocidade da banda de internet do usuário. Diferente das outras redes, a busca por arquivos não é feita diretamente através de um dos programas que operam nesta rede, mas sim em sites convencionais disponíveis na internet. Estes sites disponibilizam as chamadas *seeds* (sementes), que são arquivos que possuem os metadados do arquivo "original", ou seja, informações necessárias para se fazer o download diretamente daquele usuário que possui o arquivo desejado. Atualmente é a principal rede de transferência de arquivos utilizada por usuários mundo afora.

2.5. Freenet

A Freenet trata-se de uma rede desconhecida pela maioria do público, até mesmo para os maiores adeptos dos programas de compartilhamento P2P [Clarke et al. 2001]. Não se trata de um programa, e sim de uma rede tipicamente deep web. Barreto e Santos [Barreto and dos Santos 2019] escrevem que "O projeto Freenet foi criado pelo irlandês Ian Clarke no início dos anos 2000 com o objetivo de permitir ao usuário navegar, compartilhar arquivos e publicar freesites de forma totalmente anônima, através de canais criptografados, proporcionando segurança de dados." Para esta rede existe um cliente P2P, chamado Frost, que funciona semelhante aos programas acima, mas com o implemento da criptografia durante a transmissão dos dados.

3. Trabalhos Relacionados

É possível encontrar na literatura alguns trabalhos relacionados à utilização da tecnologia para a detecção de arquivos de CSAM compartilhado na internet, como em [Castrillon-Santana et al. 2018], onde é apresentada uma alternativa para detectar conteúdo visual que contenham pessoas "não adultas", e [Vetulani et al.], que descreve o desenvolvimento de um sistema que realiza a detecção de criadores de conteúdo de exploração sexual infantil em redes P2P.

Seguindo essa mesma linha, o trabalho [Wolak et al. 2014] utiliza dados coletados por meio de um software chamado "RoundUp" para medir um ano de atividade de tráfico de pornografia infantil por computadores dos Estados Unidos da América na rede P2P Gnutella. Por meio desse estudo, foram descobertos aproximadamente 244.900 (duzentos e quarenta e quatro mil e novecentos) computadores que compartilharam mais de 120 (cento e vinte) mil arquivos de CSAM conhecidos, somente durante o estudo, indicando que esses dados possam ser sistematicamente coletados e analisados para desenvolver uma compreensão empírica das características do tráfego de pornografia infantil em redes P2P.

Ainda em relação a redes P2P, o trabalho [Bissias et al. 2016] fornece detalhadas medições referentes à distribuição de material de CSAM em cinco dessas redes e mostra que foram realizadas aproximadamente 840 (oitocentos e quarenta) mil instalações de programas de compartilhamento de pornografia infantil por mês. [Westlake et al. 2017] destaca que webcrawlers conseguem fornecer dados de exploração sexual infantil válidos e que a distribuição desse conteúdo ainda é fortemente baseada em imagens.

Considerando os trabalhos citados acima e a problemática em relação à transmissão de CSAM em redes P2P que continua relevante até os dias atuais, este trabalho tem como objetivo comparar os dados de distribuição desse conteúdo com os casos que, de fato, chegam ao conhecimento das autoridades.

4. Similitude de Ocorrências de CSAM na Internet e o Registro Perante às Autoridades no Estado de São Paulo

Nessa seção descrevemos os passos para a obtenção dos dados das redes P2P, bem como a obtenção das ocorrências físicas, ou seja, dos boletins de ocorrências que envolvem atos

contra a violência sexual a menores e vulneráveis. Com base nesses dados realizamos uma correlação dos dados através de mapas de calor na qual permite analizar a Similitude de Ocorrências de CSAM na Internet e o Registro Perante às Autoridades no Estado de São Paulo.

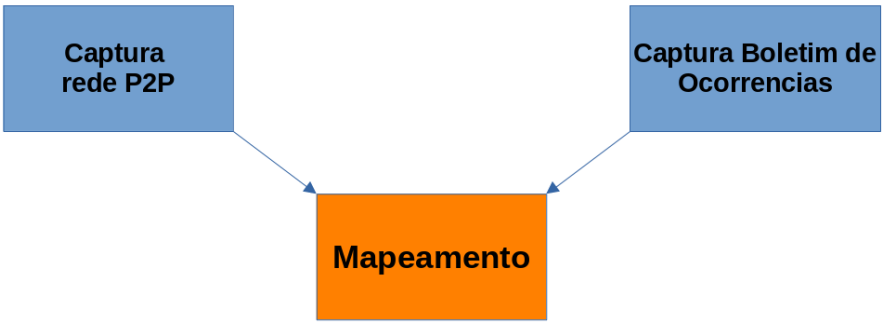


Figura 1. Diagrama de Obtenção de Dados

A Figura 1 descreve os componentes utilizados para a realização da similitude dos dados vindos e compartilhados das redes P2P com as ocorrências policiais. Assim, o componente P2P realiza a captura e processamento dos dados compartilhados nas redes P2P (dados virtuais). Na sequência, o componente ocorrências da qual foram extraídos os dados de boletins de ocorrências registrados na polícia (registros efetivos). E por fim, o componente Mapeamento que é o processamento dessas informações plotados através dos mapas de calor.

4.1. Captura rede P2P

Tomando apenas como mero exemplo, o mapa a seguir demonstra os dados disseminados de CSAM nas redes P2P que foram capturados das cinco redes descritas acima num intervalo de quinze minutos [06/06/2021 – 11:20AM a 11:35AM] no estado de São Paulo através um *software* de investigação utilizado pelas ICAC (*Internet Crimes Against Children) Task Force* ao redor do mundo, inclusive aqui no Brasil. Observe a distribuição de ocorrências de acordo com a cor da legenda de cada uma das redes que trafegam material de abuso sexual infantil. Essa distribuição é realizada pelo georreferenciamento do IP da conexão:

Observamos na Figura 2 uma grande concentração de conexões trafegando material de abuso sexual infantil na região da Grande São Paulo, mas também com conexões maliciosas distribuídas pelo interior do Estado. O ícone em azul mais escuro na Figura 2 representa as conexões utilizando a rede Bittorrent, que está em maior número: 123 (cento e vinte e três). Outro dado interessante é a existência de 2 (duas) conexões utilizando a rede Freenet, tipicamente *deep web*.

No Brasil, estes autores (H, SANTOS e J.A.D, BARRETO) são dois dos cinco representantes policiais que detém permissão de uso e treinamento de outros policiais, promotores e juízes no Brasil, América Latina e Caribe para operarem as ferramentas que auxiliaram na observação dos dados deste estudo. Trata-se de uma grande aliada no rastreamento de CSAM ao redor do mundo e aqui no Brasil. Sua principal fonte

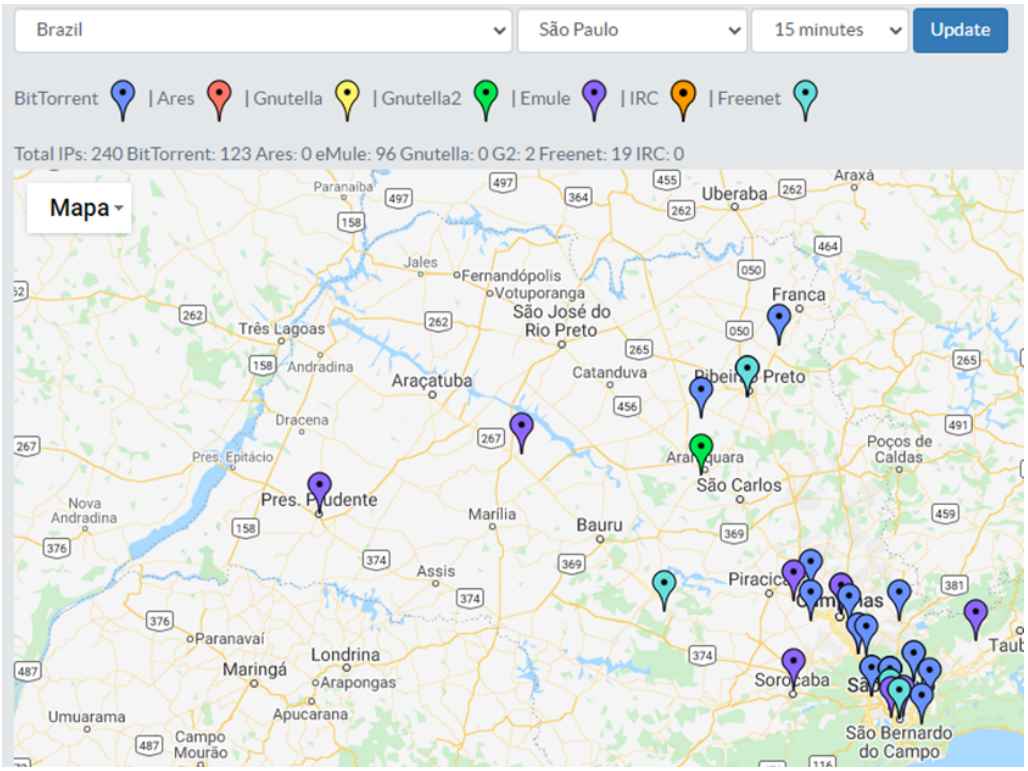


Figura 2. Compartilhamento de CSAM no Estado de São Paulo

de informação são as próprias LE (Law Enforcement), ou seja, as Forças Policiais que utilizam a plataforma alimentando-a com o resultado das apreensões de arquivos através da codificação hash.

A Figura 3 descreve as conexões que trafegam material de abuso infantil no Estado de São Paulo nos últimos 30 (trinta) dias, ou seja, entre o período de 07 de maio e 06 de junho de 2021. Pode-se observar uma disseminação muito grande de conteúdo espalhado em todo o estado de São Paulo, ou seja uma pandemia digital na distribuição de CSAM.

Importante frisar que as marcações (ícones) constantes nas Figuras 2 e 3 representam tão somente o ramal de conexão de Internet que opera na região, ou seja, *links* dos provedores de Internet. Assim, essa disseminação pode ser ainda maior quando considerarmos conexões individuáis de cada um dos usuários desses provedores.

Quando alisado um único ponto do provedor (Figura 4 podemos observar a expansão da disseminação desse conteúdo. Assim, em um único ponto do mapa é possível verificar a conexão possui 255 (duzentos e cinquenta e cinco) arquivos notáveis, que é a nomenclatura utilizada pelo *software* para classificar os arquivos de abuso sexual infantil em geral. Esse suspeito utiliza as redes Gnutella (G), eDonkey (E), Ares (A), OpenFasttrack (O) e DirectConnetc (D). Estas duas últimas redes são redes P2P mais antigas, com poucos adeptos.

Vale ressaltar que todos esses pontos estão cometendo algum dos crimes classificados pelo jurídico brasileiro que são:

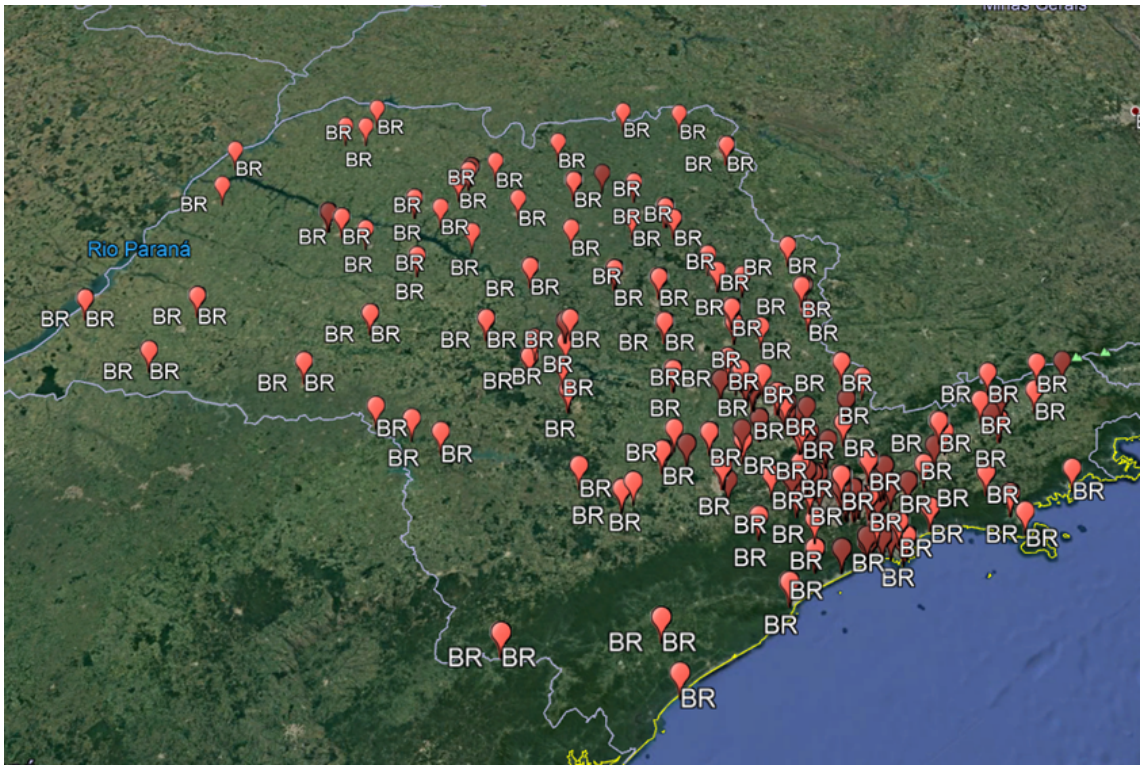


Figura 3. IPs no Estado de São Paulo que compartilharam materiais CSAM

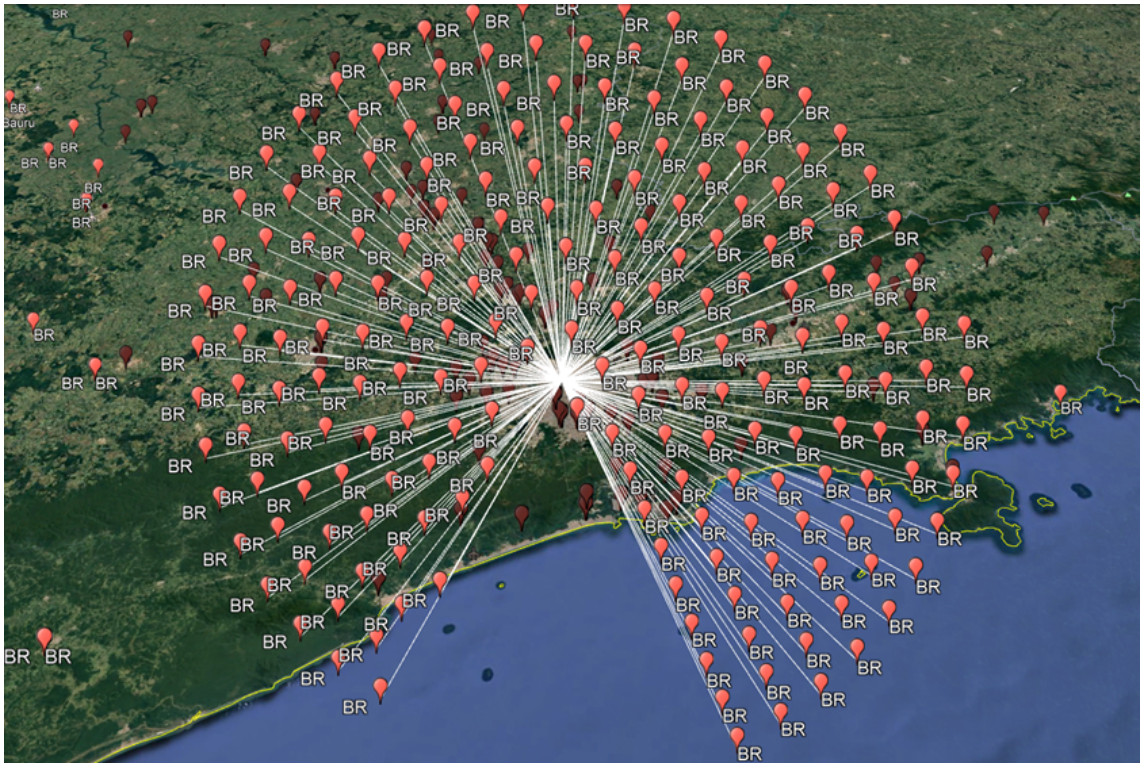


Figura 4. Expansão da informação de um ponto de conexão de uma provedora de Internet que dissemina conteúdos CSAM

- **Compartilhar**: a conduta de compartilhar CSAM é definida como crime pelo Estatuto da Criança e do Adolescente no artigo 241-A em 7 (sete) verbos diferentes: oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar. Estes verbos são sinônimos de compartilhar, essência das redes P2P, com pena de reclusão de 3 (três) a 6 (seis) anos.
- **Armazenar**: o fato de disponibilizar arquivos de CSAM em redes P2P pressupõe que o suspeito os tenha armazenado em algum dos seus dispositivos informáticos. Essa conduta caracteriza o crime previsto no artigo 240-B do ECA: adquirir, possuir ou armazenar. O título legal prevê pena de reclusão de 1 (um) a 4 (quatro) anos. Trata-se de um crime afiançável.
- **Produzir**:trata-se de um dos crimes mais graves do ECA, capitulado do artigo 240, onde o legislador se preocupou em criminalizar a produção de CSAM com os seguintes verbos: produzir, reproduzir, dirigir, fotografar, filmar ou registrar. A pena prevista é de 4 (quatro) a 8 (oito) anos de prisão.
- **Simular**:encontra-se muito na internet as famosas montagens envolvendo pessoas em atos sexuais. O ECA procura proteger a criança através do artigo 241-C, com pena de 1 (um) a 3 (três) anos de reclusão. Trata-se de um crime afiançável.
- **Aliciar**: trata-se do crime de iniciar a criança na vida sexual. O diploma legal trouxe os seguintes verbos: aliciar, assediar, instigar ou constranger no seu artigo 241-D. Atualmente representa uma das maiores ameaças para as crianças e adolescentes na internet. Trata-se do crime de *grooming*. O abusador, nominado como *Groomer* pelos investigadores, se faz passar por um adolescente em redes sociais, buscando se relacionar com meninas ou meninos entre as idades de 9 (nove) a 13 (treze) anos, em média. Durante o "namoro virtual", ele solicita imagens íntimas das crianças para disponibilizar nas redes P2P, mas principalmente na deep web

Todos estes crimes são consequência de um crime ainda mais grave, o qual é previsto no artigo 217-A do CPB – Código Penal Brasileiro e não mais no ECA. Cuida o diploma legal do estupro de vulnerável, crime gravíssimo. Os arquivos de CSAM só existem porque uma criança real foi abusada por um predador real no mundo real.

4.2. Análise dos Boletins de Ocorrência

Para a análise dos boletins de ocorrênca, foi realizado uma busca nos sistemas da Polícia Civil do Estado de São Paulo, autoridade judiciária legal encarregada de investigar os crimes descritos no capítulo anterior, entre o período de 01/01/2021 e 01/06/2021, ou seja, 6 (seis) meses, sendo possível compilar as seguintes informações:

Os dados tabulados na Tabela 1 são acessíveis através de sistemas de fontes fechadas disponíveis apenas para Policiais Civis autorizados, incluindo os autores deste artigo (H, SANTOS e J.A.D, BARRETO), no entanto podem ser acessíveis a qualquer pesquisador através da Lei de Acesso à Informação (Lei nº 12,527/11).

Ao todo, foram registradas 311 (trezentas e onze) ocorrências na Polícia Civil de São Paulo com vistas a apurar os crimes relacionados com o Estatuto da Criança e do Adolescente.

Tabela 1. Registro de crimes por categoria [Fonte: Detecta SSP]

CONDUTA	ARTIGO	OCORRÊNCIA
Produção	240 do ECA	15
Compartilhamento	241-A do ECA	59
Armazenamento	241-B do ECA	68
Simulação	241-C do ECA	4
Aliciamento	241-D do ECA	145

Infere-se dos dados mostrados na Tabela 1 a quantidade ligeiramente igual entre os crimes de "Compartilhamento" e "Armazenamento" de CSAM por parte dos investigados, os quais, somados, não atingem o total de ocorrências relacionadas com o Aliciamento, isto porque este último tipo de crime vem crescendo cada vez mais, em consequência da facilidade de acesso que as crianças atualmente possuem a aplicações, como jogos e redes sociais, e o cenário pandêmico acelerou mais essa conectividade de crianças cada vez mais jovens.

Os crimes previstos nos artigos 241-A e 241-B, principalmente, necessitam de investigação proativa automatizada por parte das autoridades policiais, ou seja, utilizar de ferramentas capazes de reconhecer a ilicitude dos arquivos trafegados através da codificação *hash*, colocando suas respectivas conexões em uma verdadeira "lista-suja" para que as autoridades decidam pelo melhor momento de se tomar uma decisão.

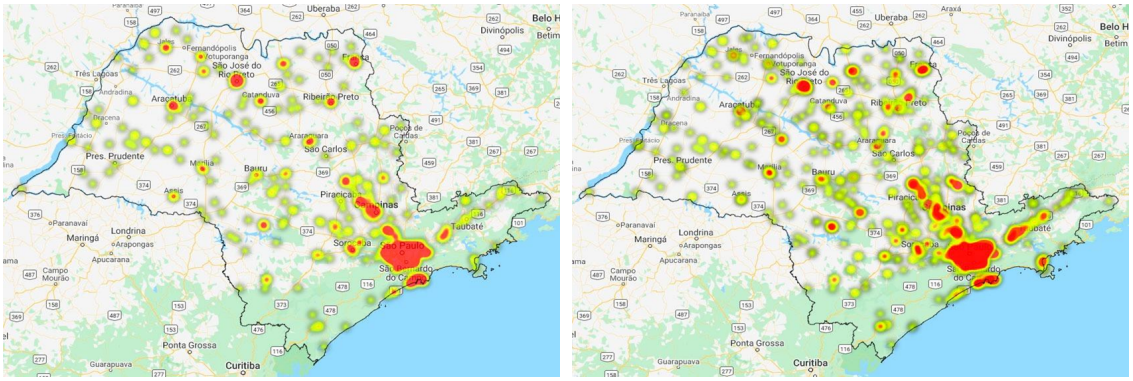
Em contrapartida, o crime de "Aliciamento" previsto no artigo 241-D do ECA necessita da observação contínua dos investigadores, chamada pela doutrina policial de ronda virtual, e dos próprios pais em relação a seus filhos, principalmente com relação às suas interações nas redes sociais, pois é ali que agem os aliciadores e abusadores denominados *Groomers*.

Os *Groomers*, ao adquirirem CSAM de suas vítimas, comercializam o material em cyberespaços da *deep web*, principalmente através da rede TOR *(The Onio Route)*. Após algum tempo, esse material passa a ser encontrado nas redes P2P convencionais (Gnutella, Ares, eDonkey e Bittorrent), de onde dificilmente sairão um dia.

4.3. Mapeamento

Para a realização do mapeamento foram utilizadas as informaços vindas da Tabela 1 constam apenas os crimes de maior incidência ligados intimamente com a transmissão de CSAM através das redes P2P. Abaixo, na Figura 5, o mapa de calor plotado de acordo com o endereço de ocorrência real dos fatos registrados na polícia.

Com essas informações foram gerados dois mapas de calor. O primeiro mapa registra os pontos na qual a polícia cívil de fato capturou o disipositivo na qual estava disseminando informações CSAM sendo os pontos mais escuros locais de maior ocorrencia (Figura 5(a)). O segundo Mapa de calor apresenta o fato ocorrido, ou seja, o estupro de vulneráveis (artigo 217-A do CPB) registrados na Polícia Civil de São Paulo (Figura 5(b)). Embora o artigo 217-A do CPB não se trate de um crime virtual ou cometido através da



(a) Incidência de casos registrados na Polícia Civil de São Paulo

(b) Estupro de vulneráveis registrados na Polícia Civil de São Paulo

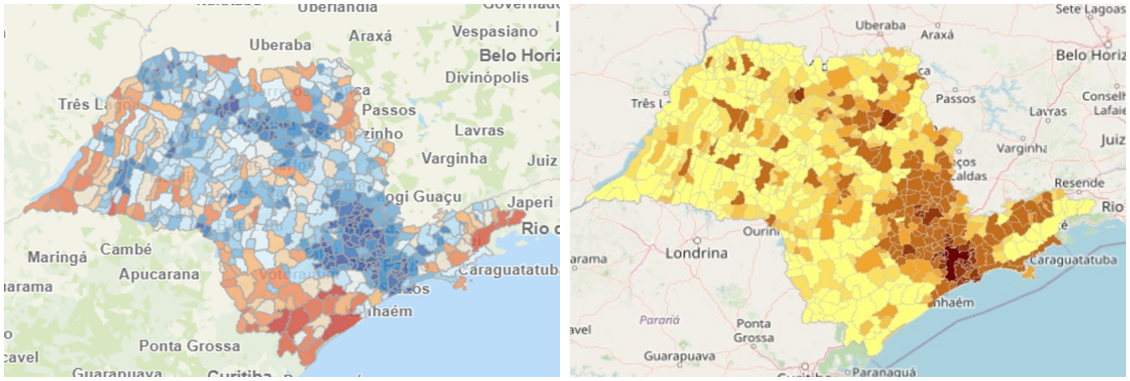
Figura 5. Mapa de calor.

Internet, muitas vezes as autoridades policiais chegam aos autores desse tipo de abuso através de investigações que se iniciaram no meio virtual. Diversas operações policiais como a Peter Pan e Hacker do Bem (maio, 2016), Peter Pan II (setembro, 2016 – preso o maior compartilhador do Brasil) e as várias fases da operação internacional Luz na Infância coordenada pelo Ministério da Justiça e Segurança Pública desde 2017, assim como a operação Black Dolphin (novembro, 2020), esta última investigando o maior Grommer em atividade da deep web brasileira, conseguiram não só identificar centenas de vítimas, assim como os seus abusadores.

Na Figura 5, podemos observar uma maior concentração de ocorrências de compartilhamento e atos violento na região metropolitana de São Paulo. Isto se dá, principalmente, pela maior concentração de pessoas na região plotada do mapa de calor (em vermelho), ou seja, por uma maior densidade populacional. A Figura 6(b) mostra a densidade populacionado extraído do *site* DataGeo [DataGeo 2021], que representa os municípios do Estado de São Paulo de acordo com a distribuição populacional. As regiões identificadas em tons da cor marrom mais escuro representam as regiões mais populosas do Estado.

Observamos na região inferior do mapa, onde constam cidades importantes do interior do Estado (Presidente Prudente, Assis, Bauru e Marília) possuem muito menos ocorrências registradas que cidades como Araçatuba, São José do Rio Preto, São Carlos, Piracicaba e Campinas, também do interior. Na qual tais regiões também apresetaram um menor número de conectividade com a Internet, observado na Figura 6(a) na qual mostra a consulta ao site da ANATEL – Agência Nacional de Telecomunicações [de Telecomunicações 2021], que é a agência reguladora máxima das telecomunicações no Brasil, obtivemos acesso, através de fontes-abertas disponíveis, ao mapa da cobertura de Internet do Estado de São Paulo.

Podemos observar no mapa da Figura 6(a) as regiões em tons de azul e marrom representando a área territorial de cada um dos 645 municípios do Estado. A primeira variação de cor, ou seja, em tons de azul, indica as regiões com maior cobertura de sinal de



(a) Cobertura de Internet no Estado de São Paulo (b) Densidade Demográfica do Estado de São Paulo

Figura 6. Mapa poulacional e de conectividade da ANATEL

Internet, coincidindo com os maiores e mais importantes municípios paulistas. É possível traçar até uma linha imaginária partindo da Baixada Santista, passando pela Grande São Paulo, seguindo para o Interior (Campinas, Ribeirão Preto e São José do Rio Preto) e municípios limítrofes. Em contrapartida, as regiões em tons de marrom e cores mais claras são aquelas cuja cobertura do sinal de Internet é menor, e isso tem relação direta com a densidade demográfica dessas mesmas regiões.

Dado o mapa de calor fica claro a similitude entre o compartilhamento de conteúdo em P2P com o fato real consumado, a violência.

4.4. Discussão

Observou-se que a difusão de material de abuso sexual infantil ou CSAM é um problema global, podendo ser nominado como uma pandemia digital. No Brasil e no Estado de São Paulo isto não é diferente. As autoridades têm realizado várias operações policiais para reprimir as mais variadas modalidades de crimes virtuais envolvendo a produção, compartilhamento e armazenamento desses arquivos na internet, principalmente através de redes P2P, deep web e redes sociais, sempre apoiadas por métodos e ferramentas que permitem automatizar o trabalho.

Muitos dos casos são resultados de investigações proativas realizadas, justamente, utilizando a observação dos dados trazidos pelas ferramentas de investigação; outras investigações, no entanto, são resultados da chamada ronda virtual, onde o agente busca informações manualmente em sites e redes sociais; isso ocorre muito para se investigar o crime de grooming (aliciamento).

Dos mapas apresentados nas figuras trazidas neste texto (Figuras de 2 a 4) em comparação com os mapas de calor trazidos pela Figura 5, observamos uma similitude entre o que as ferramentas automatizadas produzem e disponibilizam para as policiais e o que é registrado na prática.

O grande desafio das autoridades é aumentar a eficiência em relação ao grande número de casos que as ferramentas apresentam para a investigação e a demanda suportada pelas equipes de investigação.

A relação de sobreposição envolvendo os mapas de distribuição de CSAM (Figura 5 (a)) e de estupro de vulnerável (Figura 5 (b)) com os mapas de cobertura de Internet (Figura 6 (a)) e densidade demográfica (Figura 6 (b)) demonstram que as experiencias obtidas pelos agentes de campo e os registros das ocorrências através de operações policiais, de fato, refletem a similaridade dos crimes virtuais e físicos.

Muitos abusadores são encontrados pesquisando na Internet imagens, vídeos e até mesmo tutoriais de como praticar o abuso infantil, culminando com a postagem dos arquivos por eles produzidos. Encontramos suspeitos que se denominam consumidores desses materiais, alegando nunca terem abusado sexualmente de uma criança. Os agentes apontam também para a existência dos predadores "vintage" que abusam fisicamente de suas vítimas, mas não registram tais atos.

A similaridade desses comportamentos indica que essas pessoas possuem uma necessidade de se expressarem; de buscar novas informações; de se comunicarem e, por fim, acabam usando a Internet como mola propulsora para garimpar informações e novas vítimas online e por que não, até fisicamente.

Naturalmente que uma maior eficiência na repressão dos tipos de condutas descritas ao longo deste estudo passa pelo constante aprimoramento dos agentes responsáveis pelas investigações, assim como ferramentas cada vez mais robustas. Outro fator muito importante a se considerar para se alcançar resultados melhores é o constante aprimoramento da legislação que tutela os direitos das crianças e adolescente, assim como as que permitam o uso de técnicas diversas para se investigar estes crimes, pois só com o comprometimento de todas a sociedade seremos capazes de proteger nossas crianças.

5. Conclusão

Nesse artigo foi apresentado a similitude entre os registros policiais relativos ao compartilhamento de materiais de abuso sexual infantil (CSAM), um dos crimes previstos no Estatuto da Criança e do Adolescente e a sua efetiva distribuição virtual.

Fica evidente que a uma correlação entre os pontos na qual são disseminados as informações com os pontos na qual há a violencia carnal.

Como trabalho futuro visa a otimização dos postos policiais no estado da melhor forma a minimizar a quantidade de víolencia real, assim como a própria disseminação de CSAM.

Agradecimento

Os autores agradecem às Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) processo número #2020/07162-0 pelo apoio financeiro para o desenvolvimento desta pesquisa.

Referências

Adar, Eytan; Huberman, B. A. (2000). *Free Riding on Gnutella*.

Barreto, A. and dos Santos, H. (2019). *Deep Web: Investigação no submundo da internet*. Brasport.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., and Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child abuse & neglect*, 52:185–199.

Castrillon-Santana, M., Lorenzo-Navarro, J., Travieso-Gonzalez, C. M., Freire-Obregon, D., and Alonso-Hernandez, J. B. (2018). Evaluation of local descriptors and cnns for non-adult detection in visual content. *Pattern Recognition Letters*, 113:10–18.

Clarke, I., Sandberg, O., Wiley, B., and Hong, T. W. (2001). *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, pages 46–66. Springer Berlin Heidelberg, Berlin, Heidelberg.

DataGeo (2021). Infraestrutura de dados espaciais ambientais do estado de são paulo – idea-sp. Acessado em: 1 de junho de 2021.

de Telecomunicações, A. N. (2021). Panorama: Cobertura das localidades e obrigações. Acessado em: 1 de junho de 2021.

dos Deputados, C. (2003). Departamento de taquigrafia, revisão e redação. *AudiênciaPublica. Sobre PEC25/95. Sessâo*, (229.1):30–0.

Freitas, D. J., Marcondes, T. B., Nakamura, L. H., and Meneguette, R. I. (2015). A health smart home system to report incidents for disabled people. In *2015 International Conference on Distributed Computing in Sensor Systems*, pages 210–211.

Galaxy, A. (2020). *P2P File Sharing since 2002*.

Heckmann, O., Bock, A., Mauthe, A., and Steinmetz, R. (2004). The edonkey file-sharing network. In *GI Jahrestagung*.

Inc, B. (2021). *BitTorrent*.

Lei, N. (1990). 8.069, de 13 de julho de 1990. dispõe sobre o estatuto da criança e do adolescente e dá outras providências. *Diário Oficial da União*, 16.

OPAS, O. M. U. (1980). Manual da classificação estatística internacional de doenças, lesões e causas de óbito. In *Manual da classificação estatística internacional de doenças, lesões e causas de óbito*, pages 815–815.

Vetulani, Z., Geoffrois, E., Czarnecki, W., and Kochanowski, B. Language resources for public security applications: Needs and specificities. *Language Resources for Public Security Applications*, page 1.

Westlake, B., Bouchard, M., and Frank, R. (2017). Assessing the validity of automated webcrawlers as data collection tools to investigate online child sexual exploitation. *Sexual Abuse*, 29(7):685–708.

Wolak, J., Liberatore, M., and Levine, B. N. (2014). Measuring a year of child pornography trafficking by us computers on a peer-to-peer network. *Child Abuse & Neglect*, 38(2):347–356.