V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU – URUGUAI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

ROSANE LEAL DA SILVA

MARCELO EDUARDO BAUZA REILLY

Copyright © 2016 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos.
Nenhuma parte deste livro poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Prof. Dr. Raymundo Juliano Feitosa – UNICAP
Vice-presidente Sul - Prof. Dr. Ingo Wolfgang Sarlet – PUC - RS
Vice-presidente Sudeste - Prof. Dr. João Marcelo de Lima Assafim – UCAM
Vice-presidente Nordeste - Profa. Dra. Maria dos Remédios Fontes Silva – UFRN
Vice-presidente Norte/Centro - Profa. Dra. Julia Maurmann Ximenes – IDP
Secretário Executivo - Prof. Dr. Orides Mezzaroba – UFSC
Secretário Adjunto - Prof. Dr. Felipe Chiarello de Souza Pinto – Mackenzie

Representante Discente – Doutoranda Vivian de Almeida Gregori Torres – USP

Conselho Fiscal:
Prof. Msc. Caio Augusto Souza Lara – ESDH
Prof. Dr. José Querino Tavares Neto – UFG/PUC PR
Profa. Dra. Samyra Haydêe Dal Farra Naspolini Sanches – UNINOVE
Prof. Dr. Lucas Gonçalves da Silva – UFS (suplente)
Prof. Dr. Fernando Antonio de Carvalho Dantas – UFG (suplente)

Secretarias:
Relações Institucionais – Ministro José Barroso Filho – IDP
Prof. Dr. Liton Lanes Pilau Sobrinho – UPF
Educação Jurídica – Prof. Dr. Horácio Wanderlei Rodrigues – IMED/ABEDi
Eventos – Prof. Dr. Antônio Carlos Diniz Murta – FUMEC
Prof. Dr. Jose Luiz Quadros de Magalhaes – UFMG
Profa. Dra. Monica Herman Salem Caggiano – USP
Prof. Dr. Valter Moura do Carmo – UNIMAR
Profa. Dra. Viviane Coêlho de Séllos Knoerr – UNICURITIBA
Comunicação – Prof. Dr. Matheus Felipe de Castro – UNOESC

D598
Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/UdelaR/Unisinos/ URI/UFSM /Univali/UPF/FURG;

Coordenadores: Marcelo Eduardo Bauza Reilly, Rosane Leal Da Silva – Florianópolis: CONPEDI, 2016.

Inclui bibliografia
ISBN: 978-85-5505-251-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Instituciones y desarrollo en la hora actual de América Latina

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Interncionais. 2. Direito. 3. Governança. 4. Novas tecnologias. I. Encontro Internacional do CONPEDI (5. : 2016 : Montevidéu, URU).

CDU: 34



Conselho Nacional de Pesquisa e Pós-Graduação em Direito
Florianópolis – Santa Catarina – Brasil
www.conpedi.org.br



Universidad de la República
Montevideo – Uruguay
www.fder.edu.uy

V ENCONTRO INTERNACIONAL DO CONPEDI MONTEVIDÉU – URUGUAI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

Vive-se sob o impacto crescente do desenvolvimento tecnológico. Diariamente incontáveis produtos e serviços são projetados e disponibilizados no mercado global de consumo e a cada novo lançamento se renovam as promessas de mais qualidade de vida, redução de distâncias, maior conexão e felicidade.

A indústria desenvolvedora de tecnologia não mede esforços na criação de produtos e aplicativos mais dinâmicos e inteligentes e, amparados em poderosas campanhas de marketing, criam e/ou antecipam desejos de consumo. Novos lançamentos se sucedem num curto espaço de tempo, ditados mais pelo ritmo frenético da obsolescência programada do que por qualquer real necessidade dos usuários. No outro lado da cadeia de produção, consumidores ávidos por novidades não medem esforços para a aquisição de um novo dispositivo eletrônico e, cativados pelo discurso publicitário, apostam nas promessas mercadológicas como verdadeiras fórmulas garantidoras de uma vida plena e feliz.

Não é diferente no segmento das Tecnologias da Informação e Comunicação (TIC), cujos produtos, aplicativos e serviços seduzem milhares de usuários em todo o mundo. Em nenhum outro período histórico foi tão fácil e rápido obter informação e o acesso aos bens culturais como livros, músicas e filmes também experimentou relativa democratização.

Ao lado da pluralidade de fontes de consultas, a tecnologia alçou o consumidor, antes reduzido a um papel mais passivo, à condição de produtor de conteúdos, fato que se revela atrativo, especialmente para os internautas mais jovens, denominados nativos digitais. E as anunciadas vantagens não cessam no campo da informação, pois as experiências comunicativas também se renovam sob a promessa de conexão global.

Para permitir a comunicação instantânea e sem fronteiras são criados dispositivos móveis e variados aplicativos que tanto possibilitam contatos reservados entre um número limitado de atores, quanto interações mais amplas e públicas, ocorridas nos inúmeros sites de redes sociais. E o ato de comunicar ganha novos matizes, pois ao lado da palavra falada e escrita novos signos são incorporados, encontrando nas imagens e símbolos aliados para dar vazão à liberdade de expressão e comunicação.

Todas essas facilidades introduzem modos próprios de ser e estar no mundo, típicos da era digital, e incorporam ao vocabulário cotidiano verbos como “publicar”, “curtir” e “compartilhar”. Quando esses verbos se transformam em ações, experiências de vida tornam-se insumos de um mercado que não cessa de se expandir. Grande parte dessa expansão ocorre graças aos dados pessoais dos internautas, captados durante as interações on-line, momento em que os usuários das TIC abrem mão de sua privacidade em nome de experiências compartilhadas nos mais variados ambientes virtuais. Ao lado da disponibilização voluntária de informações também são utilizadas técnicas mais veladas de captura dos dados pessoais, tanto realizadas pelo mercado quanto pelos Estados.

Em grande medida essa foi a tônica das discussões que se realizaram no GT Direito, Governança e Novas Tecnologias, realizado no dia 09 de setembro de 2016, na Universidad de la República Oriental del Uruguay, em Montevidéu, aos auspícios do V Encontro Internacional do CONPEDI.

A seleção dos trabalhos que compõem a presente obra foi realizada após criteriosa avaliação (com dupla revisão cega por pares), o que resultou na qualidade dos dezesseis artigos apresentados nesta obra. Ainda que com enfoques distintos, os artigos guardam em comum a preocupação com os impactos produzidos pelo uso crescente das tecnologias da informação e comunicação, quer isso se revele como um desafio para a regulação da internet, nos efeitos que vai produzir na sua regulação, quer se manifeste nas relações entre os particulares.

Para dar maior coerência aos debates ao longo da apresentação, ocorrida no dia 09 de setembro de 2016, os trabalhos foram divididos em três eixos temáticos, assim distribuídos:

1) Temas mais gerais, que situam o leitor sobre os desafios impostos à sociedade e Estado em decorrência do uso das tecnologias da informação e comunicação, tanto pelo aspecto da governança, quanto em razão dos processos de regulação, o que pode ser encontrado nos artigos: A governança do endereçamento da rede: breve análise comparativa; A regulamentação da internet à luz da violação à liberdade de uso; Apartheid tecnológico ou tragédia dos comuns: a América Latina na sociedade da informação; Crimes de informática e cruzamento de informação a partir de dispositivos móveis; Os contratos eletrônicos e os deveres anexos: aspectos da boa-fé objetiva e as novas tecnologias.

2) Os potenciais das tecnologias da informação e comunicação como instrumento para atuação política, tema que foi objeto de atenção nos trabalhos: A influência das novas tecnologias no processo democrático; As novas tecnologias da informação e o e-gov como instrumento de participação social; Em tempos de comunicação digital a transparência e o

acesso à informação como condições indispensáveis para o exercício da cidadania democrática.

3) O terceiro eixo é composto por trabalhos que versam sobre novas formas de violação da privacidade e de dados pessoais, discutindo-se as estratégias para a sua proteção na sociedade em rede, temática que perpassa os trabalhos: A proteção de dados no e-processo: entre a publicidade do processo e a privacidade na era internet; A tutela da privacidade e a proteção à identidade pessoal no espaço virtual; A sociedade da informação como ambiente de transmissão de dados; Breves considerações sobre desafios à privacidade diante do big data na sociedade da informação; Os comunicadores instantâneos e o direito fundamental à privacidade nos ambientes corporativos; Privacidade e proteção de dados pessoais na era pós-Snowden: o Marco Civil da Internet mostra-se adequado e suficiente para proteger os internautas brasileiros em face da cibervigilância? Sociedade virtual do risco vs. Filosofia libertária criptoanarquista: livre manifestação do pensamento, anonimato e privacidade ou regulação, segurança e monitoramento da rede; Anotações sobre o marco civil da internet e o direito ao esquecimento.

Com nossos votos de boa leitura!

Profa. Dra. Rosane Leal da Silva - UFSM/Brasil

Prof. Dr. Marcelo Eduardo Bauzá Reilly - UDELAR/Uruguay

CRIMES DE INFORMÁTICA E CRUZAMENTO DE INFORMAÇÃO A PARTIR DE DISPOSITIVOS MÓVEIS

COMPUTER CRIMES: INFORMATION RETRIEVAL BASED ON MOBILE DEVICES

Cinthia O. A. Freitas [1]
Alonso Decarli [2]

Resumo

Os crimes de informática estão na ordem do dia e o volume de dispositivos móveis só tende a crescer na sociedade contemporânea. Os dados dos assinantes e de suas atividades por meio dos dispositivos móveis são por vezes uma fonte valiosa de provas em uma investigação. Questiona-se: como cruzar informações contidas em laudos periciais de dispositivos móveis distintos entre si? O artigo discute crimes de informática, legislação pertinente, computação forense e apresenta o SiCReT. Direito e Tecnologia proporcionam a busca de método para produção de provas que até então não tinham sido visualizadas antes da existência do SiCReT.

Palavras-chave: Novas tecnologias, Crimes de informática, Sociedades, Informação

Abstract/Resumen/Résumé

Computer crimes are the order of the day and the volume of mobile devices is growing in contemporary society. The data of subscribers and their activities through mobile devices are often a valuable source of evidence in an investigation. Question is: how to crossing the information contained in expert reports from different mobile devices? The article discusses computer crimes, relevant legislation, computer forensics and presents the SiCReT. Law and Technology provide a search method for producing evidence that hitherto had not been displayed before SiCReT.

Keywords/Palabras-claves/Mots-clés: New technologies, Computer crimes, Societies, Information

[1] Professora Titular da PUCPR para o curso de Direito. Professora Permanente do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Doutora em Informática pelo PPGIa da PUCPR.

[2] Mestre em Informática pela PUCPR. É professor substituto da UTFPR nas áreas de: Fundamentos de Programação e Informática Aplicada. Experiência profissional na área de Análise e Desenvolvimento de Sistemas.

1. INTRODUÇÃO

O volume de dados em formato digital gerado e armazenado vem crescendo exponencialmente com a evolução das Tecnologias de Informação e Comunicação (TIC) aplicadas nas mais diversas áreas e organizações. Gantz e Reinsel (2012, p. 1) estudaram o crescimento do volume de informações no planeta, apontando que de 2005 a 2020, o volume de dados digitais crescerá em um fator igual a 300, ou seja, passará de 130 hexabytes para 40.000 hexabytes ou 40 trilhões de gigabytes. Isto representa 5.200 gigabytes para cada homem, mulher ou criança em 2020.

Vive-se o "universo digital" tal qual denominado por Gantz e Reinsel (2012, p. 1), afirmando que de agora até 2020, o universo digital dobrará a cada 2 anos, lembrando que este universo compreende todo os dados digitais criados, replicados e consumidos. Melhor ainda, o universo digital é formado pelas imagens e vídeos em telefones celulares enviados ao YouTube, filmes digitais para TVs de alta definição, dados bancários em caixas automáticos, imagens de segurança, por exemplo em aeroportos e grandes eventos, como a Copa do Mundo de 2014 e as Olimpíadas de 2016, mensagens de voz veiculadas por linhas telefônicas digitais, e mensagens de texto (SMS ou WhatsApp), as quais se tornaram um meio generalizado de comunicação.

Para Kuechler (2007, p. 86) aproximadamente 80% dos dados digitais encontram-se armazenados em arquivos não estruturados, sendo que parte significativa destes dados encontra-se no formato de texto. Arquivos de dados não estruturados refere-se aos dados que, ou não tem um modelo de dados pré-definido ou não estão organizados de uma maneira pré-definida.

Cabe destacar que a dados estruturados constituem um fator de grande interesse às organizações, possibilitando agilidade nos processos de busca e de recuperação de informações. Assim, a transformação de grandes volumes de dados textuais não estruturados em informação útil fornece elementos para a reorganização, avaliação, utilização, compartilhamento e armazenamento do conhecimento gerado a partir do conjunto bruto de dados.

Neste universo digital estão os dispositivos móveis (*tablet*, celular, *smartphone*, entre outros) e o Brasil vem se destacando no uso de tipo de tecnologia. Na publicação do mês de julho de 2015 a Agência Nacional de Telecomunicações (ANATEL) relatou que o país alcançou a marca de 281,45 milhões de linhas ativas na telefonia móvel, apresentando dessa forma, uma teledensidade de 137,65 acessos por 100 habitantes (ANATEL, 2015). Em janeiro de 2016, o Brasil registrou 257,25 milhões de linhas ativas na telefonia móvel e teledensidade

de 125,31 acessos por 100 habitantes, demonstrando desaceleração na economia (ANATEL, 2016). De acordo com a IDC Brasil (2014), as vendas de celulares no ano de 2014 ultrapassaram a marca de 15.1 milhões de unidades, com crescimento de 49% na comparação com o mesmo período do ano de 2013.

Urge, portanto, considerar que o tratamento e uso da informação pela sociedade têm se modificado nas últimas décadas como consequência do surgimento de novos modelos sociais e econômicos alavancados pela Tecnologia de Informação e Comunicação. As TICs vêm promovendo mudanças de paradigmas tão importantes quanto à invenção da imprensa, ou ainda, quanto à própria revolução industrial. A crescente utilização de meios de comunicação, com alto grau de mobilidade, e também o uso cada vez maior da Internet, vem definindo outros espaços e explorando novas fronteiras para a sociedade contemporânea.

Neste novo espaço sem fronteiras definidas, encontram-se os crimes de informática, sejam estes praticados por meio de ou para aparatos informáticos, envolvendo: *hardware*, *software*, dados e sistemas organizacionais (NOGUEIRA, 2009). Entra em ação a área de Computação Forense.

A Computação Forense permeia as mais diversas áreas de perícia, seja trabalhando em conjunto com outras áreas, ou seja, preparando a evidência para exames, de modo que o reflexo do uso dos dispositivos móveis vem sendo percebido por meio da crescente demanda por exames periciais envolvendo dispositivos móveis.

Grochocki et al. (2013) apresentaram dados quantitativos demonstrando que no período de julho de 2012 a junho de 2013, a quantidade de celulares em estoque a serem periciados na Seção de Computação Forense do Instituto de Criminalística do Paraná passou de 5.300 celulares para 6.400 celulares, representando um aumento de 20,75% em um ano somente para celulares, sem contabilizar as demais categorias de dispositivos móveis (*tablet*, *notebook*, entre outros). Portanto, os dados dos assinantes e de suas atividades por meio dos dispositivos móveis são por vezes uma fonte valiosa de provas em uma investigação.

Neste cenário, o presente artigo tem por objetivo apresentar os crimes de informática relacionados aos dispositivos móveis, de modo a explicar o uso dos dispositivos móveis na sociedade contemporânea e a disseminação dos crimes de informática. E, então, adentrar a área de recuperação de informações neste tipo de tecnologia, focando o SiCReT – Sistema de Cruzamento de Registros Telefônicos, o qual se configura em um método de recuperação de dados de laudos periciais elaborados sobre dispositivos móveis em geral (celular, *tablet*, *smartphone*, entre outros). Tal sistema tem por objetivo maior a indicação da existência de

cruzamento de dados oriundos de laudos periciais distintos entre si e, por conseguinte, a existência de redes criminosas.

A questão é complexa, mas a união do Direito e da Tecnologia pode propiciar a busca por ferramentas de apoio aos Serviços de Inteligência e Policiamento Preditivo, evitando a subjetividade no exercício da atividade pericial e proporcionando a produção de provas e constatação de evidências forenses que até então estavam ocultas em documentos dispersos nas Sessões de Informática Forense

O artigo é resultado de projeto de pesquisa e seguiu duas vertentes de trabalho, sendo a primeira relacionada ao estudo bibliográfico e levantamento do estado da arte na área de recuperação de informações e, a segunda, voltada à pesquisa experimental desde a proposta do método computacional até sua implementação, testes e validação. Este artigo tem caráter explicativo, de modo a contemplar aspectos exploratórios e descritivos.

2. CRIMES DE INFORMÁTICA E COMPUTAÇÃO FORENSE

Inicialmente são apresentados os crimes de informática, definindo-os e categorizando-os, para posteriormente explicar a Computação Forense e os aspectos legislativos relacionados a estes crimes.

2.1. Crimes de Informática

Nogueira (2009, p. 63) apresenta uma tipologia de crimes de informática cometidos contra o computador, a saber: crimes contra o *hardware* – invasão para destruição ou danos aos equipamentos; crimes contra o *software* – invasão para destruição do sistema de dados, programas computacionais, sistema operacional e aplicativos; espionagem industrial – acesso não autorizado com o objetivo de furtar dados e segredos profissionais empresariais e pessoais, por exemplo, projetos, patentes, especificações de produtos, entre outros; invasão de site do Poder Público e do setor Privado – com a finalidade de apagar ou modificar dados, inserindo dados falsos.

Wendt e Jorge (2012, p. 18) definem crimes cibernéticos como “os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral)”. Os autores classificam os crimes cibernéticos em duas categorias: crimes cibernéticos abertos ou exclusivamente cibernéticos. Como crimes cibernéticos abertos, Wendt e Jorge (2012, p. 19) entendem:

> São aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele.

Exemplos de crimes cibernéticos abertos são: crimes contra honra, ameaça, estelionato, furto mediante fraude, racismo, apologia ao crime, falsidade ideológica, concorrência desleal e tráfico de drogas. Todos estes crimes podem ser praticados tanto no mundo real quando no mundo digital. Nestes casos, lança-se mão do Código Penal (BRASIL, 1940). Pode-se ainda citar o crime de pornografia infantil, incluído ao Estatuto da Criança e do Adolescente (ECA) por meio da Lei Nº 10.764/2003, arts. 240 e 241 (BRASIL, 2003) e, ainda da Lei Nº 11.829/2008, arts. 241-A até 241-D (BRASIL, 2008). Todos estes artigos tratam do crime de produção e divulgação de imagens de crianças e adolescentes em cenas de sexo explícito.

Os crimes exclusivamente cibernéticos são definidos por Wendt e Jorge (2012, p. 19) como sendo aqueles que "somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitam o acesso à Internet". Um exemplo deste tipo de crime é o aliciamento de crianças e adolescentes por meio da Internet, em salas de bate-papo (*chats*) ou redes sociais, devidamente previsto no art. 241-D do Estatuto da Criança e do Adolescente (ECA), Lei Nº 8.069 (BRASIL, 1990). Santin et al. (2012) apresentou o desenvolvimento de sistema computacional para detecção de aliciamento de crianças e adolescentes a partir da tratamento de mensagens instantâneas de texto. Há ainda o furto mediante fraude, já tipificado no Código Penal, e que em ambiente digital está relacionado a crimes financeiros, uma vez que os "criminosos descobriram que é muito melhor atacar o correntista, que é o pólo mais fraco, do que atacar o pólo mais forte, que é o banco" (WENDT e JORGE, 2012, p. 20).

A definição para crimes cibernéticos a partir do *National Crime Prevention Council* (NCPC, 2012, p. 2) considera

> A crime committed or facilitated via the Internet is a cybercrime. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam).

O NCPC (2012, p. 2) aponta que crime cibernético "*incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts*". Além disto, de um modo geral, pode-se considerar que os crimes cibernéticos alteram o meio

pelo qual são praticados, porém mantém características e peculiaridades dos crimes praticados sem o auxílio dos equipamentos eletrônicos. O NCPC (2012, p. 3) afirma que "*Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible.*"

Deve-se levar em conta também a definição do *United Nations Office on Drugs and Crimes* (UNODC, 2013, xvii) que apresenta crime cibernético como "*A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime*."

Os termos confidencialidade, integridade e disponibilidade são mencionados para explicar quais características do sistema informático são atacadas a partir deste tipo de crime. O UNODC (2013, xvii) explica ainda que

> Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the core of cybercrime acts.

Portanto, mesmo considerando o 'núcleo' dos atos criminosos em ambiente digital, isto não é suficiente para definir ou categorizar os crimes cibernéticos que são de natureza ampla e complexa. Assim, o UNODC (2013, xvii) entende que

> However, a 'definition' of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime' construct.

Nota-se que focar nas provas eletrônicas é a chave para entender os crimes cibernéticos e, para tanto não se necessita construir uma definição artificial para crimes cibernéticos, bastando trabalhar com os crimes de uma maneira geral. O universo digital não é uma terra sem lei como alguns imaginam, no tocante à esfera jurídica, o ambiente digital e computacional é regido pela legislação vigente no país.

2.2. Computação Forense e Aspectos Legislativos no Brasil

A área denominada de Computação Forense ou Forense Computacional (*computer forensics*) envolve a extração, identificação, preservação e documentação de evidências

digitais a partir de dados e informações armazenadas em mídias: magnéticas, ópticas ou eletrônicas (CRAIGER, 2007). Para Michaud (2001) a computação forense pode ser definida como uma peça do quebra-cabeça da investigação.

Assim, tal área do conhecimento se preocupa em estabelecer métodos e técnicas que de uma certa forma podem ser resumidos nos três A's descritos por Kruse e Heiser (2002): 1) Adquirir as evidências sem alterar ou causar danos aos dados originais, 2) Autenticar que as evidências coletadas são exatamente iguais aos dados originais e 3) Analisar os dados sem modificá-los.

Assim, entende-se que Computação Forense é o termo técnico utilizado para definir as perícias realizadas em aparatos eletrônicos. Ayers, Brothers e Jansen (2007, p. 27) explicam que "investigações digitais são comparáveis às cenas de crime, visto que técnicas de investigação com base na aplicação da lei têm sido utilizadas para a criação de procedimentos voltados às evidências digitais". Os autores destacam que os Princípios de Probatória consideram a prova digital em dois aspectos, a saber: a) os componentes físicos, periféricos e mídia, que podem conter dados e b) os dados extraídos a partir dessas fontes. De um modo geral, os tipos de evidências a serem coletadas durante a aquisição de provas digitais são os seguintes:

- Físicas: computadores (servidor, *desktop, laptop, notebook, tablet*), HD externos, *pen-drive* (*mp3-player*), CDs, DVDs, celulares, câmeras digitais, jogos e outros;
- Lógicas ou demonstrativas: dados, informações, arquivos, textos, imagens, vídeos, músicas, e-mails, entre outros que se encontram armazenados em suportes físicos, seja este eletrônico, ótico ou magnético.

Trabalha-se na busca de evidências tal qual o usuário vê ou utiliza o seu computador e demais equipamentos eletrônicos. É importante lembrar que evidências lógicas ou demonstrativas provêm de evidências físicas e que as provas digitais necessitam de suporte físico para existir. Deste modo, o *link* ou a ligação entre evidências físicas e lógicas é muito relevante para sustentar judicialmente a correta relação entre os suportes materiais e os dados digitais.

Muitas são as situações nas quais a Computação Forense se faz necessária e urgente, podendo-se citar: crimes praticados por computador, crimes via Internet, pornografia infantil, aliciamento de crianças e adolescentes na Internet, fraudes bancárias, e-mail caluniosos, direito autoral uso indevido ou não autorizado de *software*, músicas, filmes, jogos e muitos outros problemas. Deste modo, tais problemas necessitam da comprovação dos fatos que possam ser trazidos em juízo para as devidas responsabilizações.

Grochocki (2012, p. 20) demonstra que dentro dessa nova realidade existem alguns princípios do Direito Digital a serem considerados no exercício das atividades relacionadas à Computação Forense, a saber: as relações são não presenciais, as testemunhas são os equipamentos eletrônicos, as provas são eletrônicas e as fronteiras são informacionais e não territoriais, geográficas ou físicas.

Visando atender esta realidade fundada em dispositivos informáticos, em termos legislativos o Brasil vem avançando na tipificação dos delitos informáticos. Em 2012, foi sancionada Lei Nº 12.737, adicionando no rol de crimes já previstos no Código Penal a tipificação dos delitos informáticos, a saber (BRASIL, 2012):

- Invasão de dispositivo informático: invasão de computadores, roubo de senhas e de conteúdos de e-mail, e disseminação de vírus de computador ou códigos maliciosos (*malware*) para roubo de senhas (art. 154-A);
- Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 266);
- Falsificação de documento particular: falsificar um documento eletrônico em todo ou em parte (art. 298);
- Falsificação de cartão: o uso de dados de cartões de débito e crédito sem autorização do titular (art. 298).

Outro documento legislativo é o Marco Civil da Internet, Lei Nº 12.965 de 23 de abril de 2014, formado a partir de 3 objetivos: (i) adaptar e consolidar direitos fundamentais dos indivíduos a partir do contexto de comunicação eletrônica, (ii) delimitar de forma clara a responsabilidade civil dos diversos atores envolvidos nos processos de comunicação pela Internet, e (iii) estabelecer diretrizes convergentes para a atuação do governo, tanto na formulação de políticas públicas quanto em eventuais regulamentações posteriores (BRASIL, 2009).

Tais objetivos foram abertos em consulta pública pelo Ministério Público em 2009, visando construir colaborativamente tal instrumento. Os cidadãos puderam opinar sobre os seguintes temas, por exemplo: direito ao acesso, à liberdade de expressão e à privacidade, a não-discriminação de conteúdos e a resolução de conflitos relacionados à rede, entre outros. Deste modo, o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (BRASIL, 2014).

O estudo detalhado desta lei está além do escopo deste artigo, porém uma análise aprofundada pode ser encontrada em Carvalho (2014). Como já mencionado anteriormente,

deve-se ainda considerar o Estatuto da Criança e do Adolescente (ECA) e o Código Penal, bem como as leis que alteram ambos os dispositivos no tocante aos crimes cibernéticos.

3. RECUPERAÇÃO DE INFORMAÇÃO EM DISPOSITIVOS MÓVEIS

O foco deste trabalho está no que é denominado de dispositivo móvel, qual seja sua característica de mobilidade, sendo que esta capacidade permite mover fisicamente serviços computacionais juntamente com os usuários, tornando os dispositivos computacionais sempre presentes e permitindo acesso aos recursos oferecidos por sistemas computacionais independentemente da sua localização. Exemplos de características que são comuns aos dispositivos móveis atuais são: microprocessador, memória ROM (*Read Only Memory*), memória RAM (*Random Access Memory*), módulo de rádio, processador de sinal digital, alto falante, tela, sistema operacional, bateria, PDAs (*Personal Digital Assistants*), GPS (*Global Positioning System*), câmera, entre outros recursos.

É a partir deste tipo de dispositivo que se tem a formação das provas digitais, iniciando-se com a coleta dos dados digitais, a qual segue procedimentos técnicos da Computação Forense e, então, elaborando-se os laudos periciais. Estudou-se, portanto, a recuperação das informações dos laudos periciais com intuito de realizar o cruzamento de dados para então usufruir do que é denominado como Descoberta do Conhecimento (*Knowledge Discovery*).

3.1. Coleta de Dados Digitais a partir de Dispositivos Móveis

A coleta ou aquisição de dados digitais a partir de dispositivos eletrônicos (móveis ou não) considera, como mencionado anteriormente, as evidências físicas e lógicas. Além disto, a aquisição também pode ser assim categorizada, ou seja, aquisição física e aquisição lógica. A aquisição física tem vantagens sobre a aquisição lógica, uma vez que permite que os arquivos apagados e alguns dados restantes possam ser examinados, por exemplo, na memória não alocada ou em espaço do sistema de arquivos (AYERS; BROTHERS; JANSEN, 2007).

A Computação Forense preconiza que seja realizada a aquisição de dados física, por meio de procedimento denominado ‘imagem’. Este procedimento é assim denominado, ‘imagem’, pois realiza uma cópia *bit* a *bit* do conteúdo das evidências físicas. Estas cópias são realizadas tendo como origem o equipamento suspeito e como destino um HD externo. Exige-se a realização de ‘imagem’ visto que não se pode realizar uma análise forense diretamente no equipamento eletrônico original.

A realização do procedimento de ‘imagem’ necessita da utilização de ferramentas forenses, *hardware* e *software*, de modo a permitir que as cópias sejam duplamente garantidas. Isto significa que devem ser utilizados equipamentos denominados de *writer blocker*, ou seja, equipamentos que bloqueiam a escrita no equipamento origem durante o procedimento de ‘imagem’.

Tais equipamentos podem ser auxiliados por programas que efetuam propriamente este tipo de cópia. Existem diversos *hardware* e *software* que permitem aos peritos realizarem tais cópias. Não é o foco do presente artigo, comparar ou fazer a recomendação de *hardware* e *software*, uma vez que isto depende de diferentes fatores, tais como: recursos disponíveis, conhecimentos teórico-prático na utilização dos equipamentos e programas, conhecimento dos efeitos e implicações das ferramentas adotadas no sistema a ser analisado, uso de ferramentas consolidadas (sabe-se que existem juízes que tem reservas ao uso de ferramentas de código aberto (*open source*), mas por outro lado, as ferramentas com base em código aberto podem ser testadas e verificadas, ao ponto de se ter certeza que esta realiza o que afirma fazer), sendo que resultados das análises devem ser mantidos em dispositivos confiáveis e protegidos da tentativa de degradação intencional, entre outros.

Entre os equipamentos utilizados para coleta dos dados digitais a partir de dispositivos móveis, pode-se citar: *Cellebrite UFED* e *Microsytemation XRY*. Ambos realizam a extração de dados em padrão XML (*eXtensible Markup Language*), padrão este que permite descrever diversos tipos de dados, tendo como objetivo facilitar o compartilhamento de informações.

O *Cellebrite UFED* (*Universal Forensic Extraction Device*) *Touch Ultimate* é uma solução composta por *hardware* e *software* proprietário que permite a extração, decodificação, análise e geração de relatórios avançados, sendo que tal tecnologia suporta atualmente 7.900 dispositivos diferentes. Dentre os principais aplicativos que acompanham a solução destacam-se: *Phisical Analyzer*: ferramenta de decodificação, análise e relatórios, *Phone Detective*: *software* que identifica um telefone móvel no início de uma investigação e *Reader*: inicialização dos dispositivos em modo somente leitura, permitindo o compartilhamento de informações.

O *Microsytemation XRY* realiza função semelhante de captura, podendo suportar até 10.036 dispositivos móveis distintos, sendo esta sua principal característica de modo a ser uma ferramenta utilizada em larga escala na área forense.

As ferramentas forenses adquirem informações dos dispositivos sem alterar o conteúdo, ou seja, em modo somente de leitura, e em geral geram *hash*, MD5 (*Message-Digest Algorithm 57*) ou SHA (*Secure Hash Algorithm8*), que garante a integridade dos dados

coletados dos dispositivos móveis. De um modo geral, a função *hash* tem por objetivo identificar univocamente cada conjunto de informações, ou seja, para cada documento criptografado gera-se uma cadeia alfanumérica única, sendo que o procedimento (ou algoritmo) de geração usa o conteúdo do documento para gerar tal cadeia (FREITAS; RICCI, 2012). Assim, se um documento for modificado e novamente criptografado, nunca conterá o mesmo *hash*, pois o conteúdo do documento foi alterado. A simples comparação dos valores dos *hashs* de dois documentos, permite a validação da autenticidade dos mesmos, visto que somente para *hashs* iguais têm-se documentos iguais. Tal característica é muito importante perante o Poder Judiciário, sendo que cabe ao perito garantir a integridade das provas digitais por ele coletadas ou a ele confiadas.

A partir de todo o conjunto de dados extraído pelas ferramentas de captura, pode-se então analisar quais dados permitirão a realização do cruzamento de informações provenientes de dispositivos móveis distintos. Deste modo, os dados digitais apresentam natureza diversificada, sendo oriundos em formatos distintos conforme as características técnicas de cada dispositivo.

Ainda não existe um padrão de informações que devem ser extraídas dos dispositivos e nem um formato padrão de armazenamento dos dados. Tem-se portanto uma variedade de dados que podem ser extraídos mas uma dificuldade de tratamento computacional frente a diversidade de formatos e estruturas de dados encontrados nos dispositivos móveis atuais. Todos estes dados são então apresentados nos laudos periciais, os quais integram as bases de laudos das Sessões de Informática Forense dos Institutos de Criminalística do Brasil.

Como exemplo, sabe-se *a priori* que, a partir de celulares e *smartphones* são importantes para o cruzamento os dados contidos nos contatos da agenda, nas chamadas (realizadas e recebidas) e mensagens instantâneas trocadas entre celulares distintos. Alguns modelos de *smartphones* fornecem dados de mensagens eletrônicas (*e-mail*), salas de bate-papo (*chat*), entre outros. DECARLI et al. (2014) apresenta o detalhamento dos dados de interesse a formação de um banco de dados a partir de dispositivos móveis com aplicação forense.

3.2. Recuperação de Informação

Em 1951, Calvin Mooers criou o termo Recuperação de Informações (*Information Retrieval*) de modo a explicar que essa área trata dos aspectos intelectuais da descrição da

informação e sua especificação para busca e, também, sendo que qualquer sistema, técnicas ou máquinas podem ser empregadas para realizar esta operação (MOOERS, 1951).

A Recuperação da Informação (RI) trata da representação, armazenamento, organização e acesso a itens de informação, tais como: documentos, páginas Web, catálogos *online*, registros estruturados e semi-estruturados, objetos multimídia, entre outros. A representação e a organização dos itens de informação devem fornecer aos usuários facilidade de acesso às informações de seu interesse (BAEZA-YATES; RIBEIRO-NETO, 2013).

De uma maneira simplificada, a partir de uma consulta efetuada pelo usuário, o objetivo maior do sistema de RI é recuperar informações que sejam úteis ou relevantes para o usuário e, que ao mesmo tempo, estejam relacionadas com a consulta realizada. A ênfase está na recuperação da informação, não na recuperação de dados. O principal objetivo de um sistema de RI é recuperar todos os documentos que são relevantes à necessidade de informação do usuário e, ao mesmo tempo, recuperar o menor número possível de documentos irrelevantes.

A tarefa é complexa, visto que determinar o que é ou não relevante ao usuário envolve conceito subjetivo e dependente de contexto. Por exemplo, a relevância pode mudar com o tempo, à medida que novas informações tornam-se disponíveis; com o local, a resposta mais relevante pode ser a mais próxima; ou até mesmo com o dispositivo, a resposta mais adequada pode ser um documento pequeno que seja mais fácil de ser acessado e visualizado. Nesse sentido, nenhum sistema de RI pode fornecer respostas perfeitas a todos os usuários o tempo todo. A Figura 1 mostra um processo clássico de Recuperação de Informação descrito por Salton & MacGill (1983).

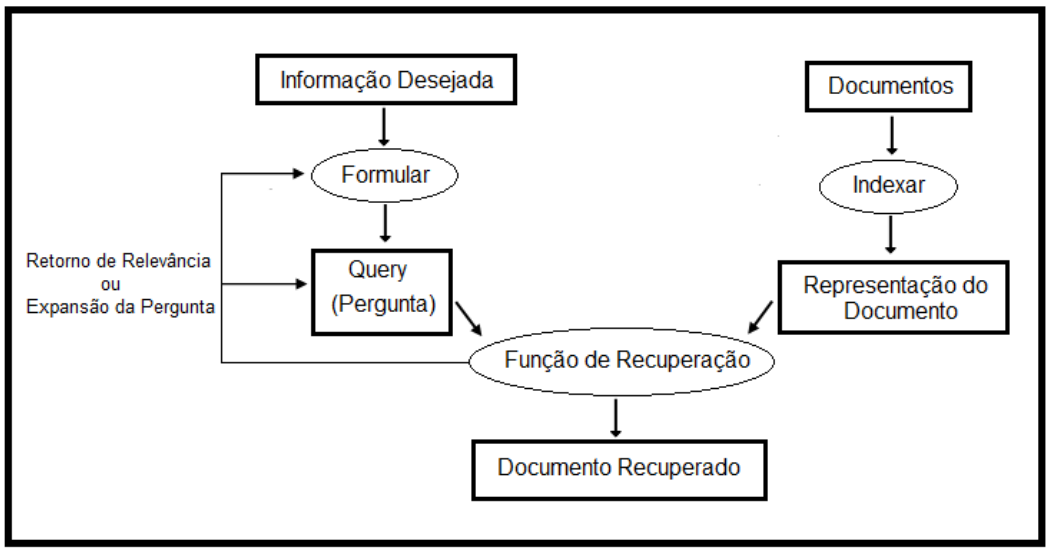


Figura 1: Processo Clássico de Recuperação de Informação.
Fonte: Adaptado de (SALTON e MCGILL, 1983)

Os sistemas de RI devem representar o conteúdo dos documentos e apresentá-los ao usuário de uma maneira que lhe permita uma rápida seleção dos itens que satisfaçam total ou parcialmente a sua necessidade de informação, sendo a consulta formalizada por meio de uma expressão de busca (FERNEDA, 2012). Já o processo de representação dos documentos tem por objetivo identificar e descrever cada documento por meio de seu conteúdo (FERNEDA, 2012).

Assim, RI envolve o *matching* do texto contido em uma consulta ou um documento com um conjunto de outros documentos. Frequentemente, essa tarefa gera uma resposta encontrando documentos em um conjunto de documentos que sejam relevantes para a consulta de um usuário (COPPIN, 2010). Os exemplos mais conhecidos de RI são os mecanismos de busca na Internet, sendo que a partir de uma consulta o usuário obtém uma lista de páginas relevantes que contém a consulta em seu conteúdo. Observa-se neste caso que os mecanismos de busca apresentam os resultados em forma de lista, sendo que este modelo não é adequado para representar dados digitais provenientes de laudos periciais de dispositivos móveis.

4. O SISTEMA SiCReT

O Sistema de Cruzamento de Registros Telefônicos - SiCReT, surgiu da necessidade das Seções de Informática Forense dos Institutos de Criminalística utilizarem um procedimento computacional capaz de realizar o cruzamento de informações contidas nos laudos periciais de dispositivos móveis. Portanto, o SiCReT pode ser definido como uma ferramenta computacional capaz de realizar o processo de recuperação, detecção e visualização de cruzamentos existentes entre termos de interesse de um determinado conjunto de laudos periciais de dispositivos móveis distintos entre si, pertencentes ou não a um mesmo laudo pericial. Explica-se o uso do termo cruzamento associado às técnicas de Recuperação de Informação, de modo a apresentar os resultados em forma de grafos[1].

O SiCReT é composto por quatro fases, assim denominadas: composição dos conjuntos de documentos, representação de documentos, indexação de termos relevantes e, finalmente, apresentação e visualização dos resultados. Havendo ainda uma fase de pré-processamento, a qual é responsável por realizar a extração do conteúdo textual dos arquivos fornecidos como entrada de dados ao método. O SiCReT suporta às formas e formatos de

[1] Um grafo ou rede consiste em um conjunto de vértices (nós ou nodos) não vazio e um conjunto de pares de vértices denominados de arestas (HOROWITZ e SAHNI, 1987, 252-296p). Os grafos podem ser dirigidos ou não, ou seja, quando na aresta o sentido de ligação dos vértices é importante.

arquivos que armazenam documentos textuais existentes na atualidade, a exemplo de formatos como: HTML, XHTML, XML, *Microsoft Office document formats*, *OpenDocument Format*, PDF, EPUB, RTF e *Text formats*. Ao final do pré-processamento, é fornecida à primeira fase do método apenas o conteúdo textual contido no conjunto de arquivos de entrada.

A 1ª. fase do método considera o fato de que um determinado arquivo possa conter um ou mais laudos periciais de dispositivos móveis, aqui denominados de documentos. Ou seja, cada laudo pericial é considerado um documento a fim de representação computacional. Esta fase utiliza um conjunto de seccionadores, os quais proporcionam ao método um meio de detectar e definir o seccionamento do conteúdo textual do arquivo de entrada em um conjunto de documentos.

A 2ª. fase possibilita a representação dos documentos textuais no SiCReT e é dada por meio de um conjunto de termos resultantes da aplicação de indexadores baseados em expressões regulares, sendo que tal conjunto deve ser informado ao método como um de seus parâmetros de entrada, tal qual os arquivos contendo os laudos. O conjunto dos termos válidos extraídos do documento proporciona a composição do vocabulário do documento.

A 3ª. fase realiza-se o cruzamento das informações propriamente dito, ou seja, o procedimento de indexação das informações. Nesta etapa, é gerada uma estrutura de dados por meio da unificação de todos os termos que compõem os vocabulários, representando os seus respectivos documentos. Nessa estrutura de dados, os termos são individualizados e, conforme é verificada a incidência dos termos nos vocabulários, os respectivos documentos passam a fazer parte do conjunto de documentos referenciados pelo termo que está sendo analisado. A estrutura de dados resultante deste processo contém como chave de acesso os termos, por exemplo, um número de celular (XXXX-XXXX), sendo associados a cada chave os documentos (laudos) que contêm a incidência da referida chave.

Nesta estrutura de índices, observa-se que cada conjunto de documentos atribuído a um termo específico (número de celular igual a XXX1-XXX0) significa que existe um cruzamento de informações, ou seja, o termo foi encontrado e indexado em dois ou mais documentos. Podemos afirma nesses casos que o termo é responsável pela interseção entre os respectivos documentos. Já nos casos em que o termo tem incidência em apenas um único documento, o cruzamento de informações é inexistente, visto que o termo referenciado está contido em apenas um documento, portanto, não há cruzamento de dados entre laudos distintos.

A 4ª. fase, apresentação e visualização dos resultados, propriamente os cruzamentos de dados entre laudos periciais de dispositivos móveis, é realizada com o uso das informações contidas na estrutura de índices formado na 3ª. fase. A representação visual em forma de grafos permite que os usuários possam absorver rapidamente grandes quantidades de informações e construir mapas mentais das informações recuperadas, proporcionando maior capacidade de interpretação das informações visualizadas. Além disto, facilita a identificação de cruzamentos diretos e indiretos entre termos de interesse a partir dos laudos indexados.

Para testes e validação do método proposto utilizou-se uma base de 200 arquivos da Seção de Informática Forense do Instituto de Criminalística do Paraná da Polícia Científica do Paraná – Curitiba, devidamente descaracterizada, ou seja, de forma anônima sem que se possa identificar nomes ou pessoas. Esses arquivos possuem informações referente aos laudos periciais, anexos de laudos e arquivos complementares, todos em formato ODT (*OpenDocument Text*) que é o formato padrão de documentos do *Open Office*.

A partir desta base de 200 arquivos foram detectados 516.592 termos, contendo 7.913 termos relevantes (registros telefônicos) a partir de 8.725 termos recuperados em um total de 46.034 ocorrências de termos recuperados. Para melhor entendimento, explica-se:

- Termos: parte de dados detectada em um documento, por exemplo: palavras, registros telefônicos, entre outros;
- Termos Relevantes: termos de interesse que foram recuperados, ou seja, termos correspondentes aos registros telefônicos;
- Termos Recuperados: conjunto composto por termos relevantes recuperados somados aos termos que não correspondem a registros telefônicos, ou seja, resultado incluindo os "falsos positivos".

A Figura 2 mostra os resultados obtidos a partir de toda a base de dados, contendo 28 cruzamentos. Observa-se que existem cruzamentos entre laudos e seus respectivos anexos (em um total de 21), o que é esperado que seja devidamente recuperado pelo sistema, porém não configuram cruzamentos relevantes à atividade pericial. Assim, ao se excluir tais cruzamentos, são recuperados somente os cruzamentos relevantes em um total de 7 cruzamentos entre laudos periciais de dispositivos móveis distintos, conforme Figura 3.

Outro experimento realizado a partir da mesma base de dados foi a consulta a partir da raiz dos termos, ou seja, tendo sido especificado que a raiz é representada pelos 8 dígitos base dos registros telefônicos. Exemplificando, a raiz do registro telefônico +55 (41) xxxx-xxxx ou (41) xxxx-xxxx, é somente o conjunto de algarismos xxxxxxxx.

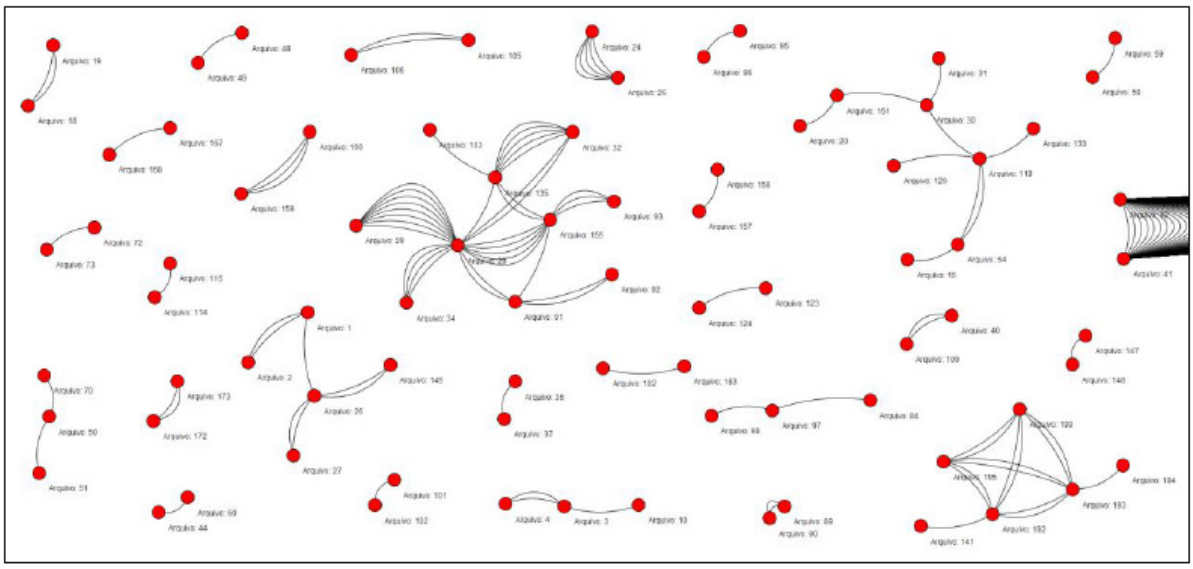


Figura 2: Resultado completo a partir da base de 200 arquivos (28 cruzamentos)

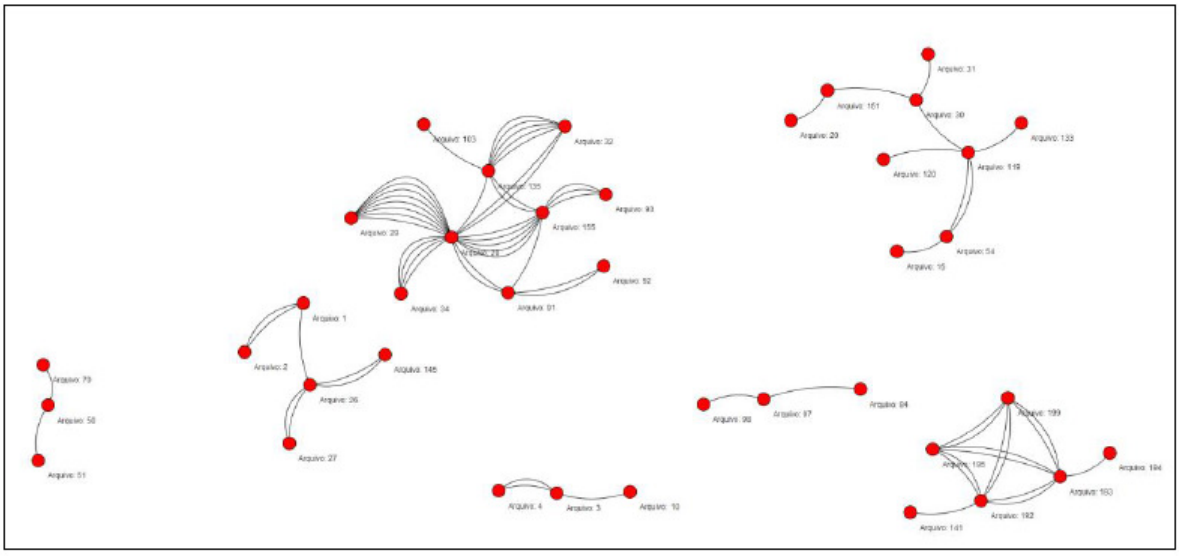


Figura 3: Resultados relevantes à atividade pericial (7 cruzamentos)

A Figura 4 apresenta o resultado obtido contendo um total de 42 cruzamentos, sendo que 35 cruzamentos não são relevantes e que, finalmente, 07 cruzamentos se mostraram relevantes. Vale observar que as configurações dos cruzamentos se apresentam diferenciadas quando se compara as Figuras 3 e 4 entre si. Isto é explicado, visto que muitas pessoas ao cadastrarem em suas agendas os números para chamada de celulares ou fixos, não colocam todas as informações, como código do país e de área. Portanto, ao se reduzir o termo de busca à raiz dos registros telefônicos, pode-se localizar outros cruzamentos que não foram encontrados quando se exigia a completude das informações. Os resultados obtidos nos experimentos alcançaram uma precisão de 91% na recuperação de informações.

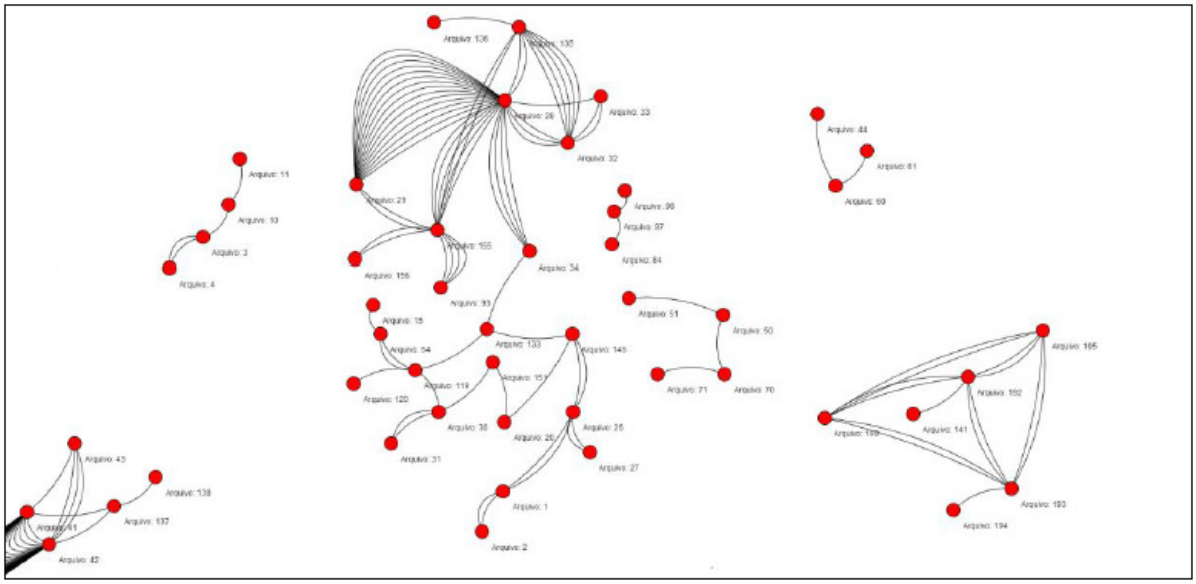


Figura 4: Resultados relevantes à atividade pericial a partir da raiz dos registros telefônicos (7 cruzamentos)

Cabe destacar que os resultados são apresentados em forma de grafos, visto ser a representação gráfica mais adequada à atividade pericial, uma vez que o perito pode expandir tanto as arestas quanto os nós e, então, obter mais detalhes, por exemplo: se é uma chamada realizada ou recebida, se tem envio de mensagens de texto, se existe recebimento de mensagens de texto, datas, horários, entre outros. Estes resultados nunca haviam sido visualizados pelos peritos da Seção de Informática Forense do Instituto de Criminalística do Paraná, nem de outro IC no Brasil. É o que se denomina de descoberta do conhecimento a partir da recuperação de informações relevantes. Estes cruzamentos estavam ocultos e puderam ser revelados a partir da implementação do sistema SiCReT. Dessa forma, foi gerado um conhecimento que ninguém havia observado até então.

O cruzamento entre laudos distintos é de grande interesse por representar novas evidências forenses, demonstrando o fluxo de informações a partir de dispositivos móveis, inicialmente não relacionados a um mesmo cenário ou cena de crime.

5. CONSIDERAÇÕES FINAIS

Os crimes de informática estão na ordem do dia. Tecnologia, velocidade e mobilidade são características dos crimes atuais. Cabe a proposição de ferramentas computacionais de modo a permitir que tanto a Direito, no que diz respeito à legislação, quanto a Tecnologia, no que se refere ao trabalho pericial, possam unir esforços e contra atacar este tipo de crime.

Neste contexto, o artigo apresentou a Recuperação de Informações em documentos textuais não estruturados, assim como todos os Sistemas de RI, a qual tem por objetivo fazer

com que o usuário encontre rapidamente a informação que está precisando, sem que seja necessário analisar todas as informações existentes em uma base de informações.

Com o intuito de fornecer meios de processamento e otimização das atividades realizadas por peritos, descreve-se um método para Cruzamento de Registros Telefônicos a partir de dados extraídos de laudos periciais de dispositivos móveis. O SiCReT é capaz de recuperar e descobrir relacionamentos, redes criminosas, a partir de laudos periciais elaborados para dispositivos móveis distintos entre si e, ainda, capaz de relacionar os cruzamentos entre laudos de dispositivos não provenientes de um mesmo cenário, cena de crime ou operação de busca e apreensão.

Os resultados obtidos nos experimentos permitem afirmar que a aplicação do método proposto na base de dados especificada conseguiu detectar as intersecções previstas entre os documentos por meio de termos de interesse contidos nos mesmos, ou seja, os registros telefônicos.

Foi observado que a visualização dos resultados gerados, especialmente em formato de grafos, permitiu aos usuários analisar rapidamente grandes quantidades de informações detectando e visualizando os cruzamentos de informações de interesse entre laudos distintos.

Os resultados gerados, a partir de documentos dispersos nas Sessões de Computação Forense mostraram que o sistema fornece uma ferramenta de apoio aos Serviços de Inteligência e Policiamento Preditivo, evitando a subjetividade no exercício da atividade pericial e proporcionando a produção de provas e evidências forenses que até então não tinham sido visualizados antes da existência do SiCReT.

REFERÊNCIAS

ANATEL. **Julho de 2015 fecha com 281,45 milhões de acessos móveis**. 2015. Disponível em: <http://www.anatel.gov.br/institucional/index.php?option=com_content&view=article&id=621:julho-de-2015-fecha-com-281-45-milhoes-de-acessos-moveis&catid=104&Itemid=354> Acesso em: 25 maio 2016.

ANATEL. **Brasil fecha janeiro de 2016 com 257,25 milhões de acessos**. Disponível em: <http://www.anatel.gov.br/institucional/index.php/noticias/noticia-dados-01/1022-brasil-fecha-janeiro-de-2016-com-257-25-milhoes-de-acessos-moveis-2> Acesso em: 25 maio 2016.

AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. **Computer Security - guidelines on mobile devices forensics**. NIST - Special Publication 800-101, 2007. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>. Acesso em: 10 maio 2016.

BAEZA-YATES, Ricardo; RIBEIRO-NETO, Berthier. Recuperação **de Informação: conceitos e tecnologia das máquinas de busca**. Bookman Editora, 2013.

BRASIL. **Lei Nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: 24 de abril de 2014, Brasília-DF, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 10 maio 2016.

BRASIL. **Lei Nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União: 3 de dezembro de 2012, Brasília-DF, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 10 maio 2016.

BRASIL. Ministério da Justiça. Marco Civil da Internet – seus direitos e deveres em discussão. 2009. Disponível em: <http://culturadigital.br/marcocivil/tag/convite/> Acesso em: 10 maio 2016.

BRASIl. . **Lei Nº 8.069**, de 13 de julho de 30 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União: 27 de setembro de 1990, Brasília-DF, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069Compilado.htm> Acesso em: 10 maio 2016.

BRASIL. **Decreto-Lei Nº 2.848**, de 7 de dezembro de 1948. Código Penal. Diário Oficial da União: 31 de dezembro de 1940, 1940. Disponível em: <http://presrepublica.jusbrasil.com.br/legislacao/91614/codigo-penal-decreto-lei-2848-40> Acesso em: 10 maio 2016.

BRASIL. **Lei Nº 10.764**, 12 de dezembro de 2003. Altera a Lei nº 8.069, de 13 de julho de 1990, que dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União: 13 de dezembro de 2003, Brasília-DF, 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.764.htm> Acesso em: 10 maio 2016.

BRASIL. **Lei Nº 11.829**, 25 de novembro de 2008. Altera a Lei Nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Diário Oficial da União: 26 de novembro de 2008, Brasília-DF, 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm> Acesso em: 10 maio 2016.

CARVALHO, Ana Cristina Azevedo P. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014.

COPPIN, Ben. **Inteligência Artificial**. Rio de Janeiro: Editora LTC, 2010.

DECARLI, Alonso; GROKOSKI, Cícero Lemos; PARAISO, Emerson Cabrera; GROCHOCKI, Luiz Rodrigo; FREITAS, Cinthia Obladen de Almendra. **Banco de Dados de Laudos Periciais de Dispositivos Móveis**. In: XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg'2014), 2014, Belo Horizonte. Anais do

XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Belo Horizonte: Sociedade Brasileira de Computação, 2014. v. 1. p. 559-571.
FERNEDA, Edberto. Introdução aos modelos computacionais de recuperação de informação. Rio de Janeiro: Editora Ciência Moderna, 2012.

GANTZ, John; REINSEL, David. **The digital universe in 2020: Big Data, nigger digital shadows, and biggest growth in the far east**. IDC iView - Analyze the Future, 2012.

GROCHOCKI, Luiz Rodrigo; VRUBEL, Alexandre; ZAGO, Raphael ; DECARLI, Alonso; FREITAS, Cinthia Obladen de Almendra. **SICReT - Sistema de Cruzamento de registros Telefônicos**. In: XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2013, Manaus. Anais do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg). Manaus: Sociedade Brasileira de Computação, 2013. v. 1. p. 527-536.

GROCHOCKI, Luiz Rodrigo. **Direito Digital**. Escola de Governo, Estado do Paraná. Palestras – 2012, 2012. 52 slides, color. Acompanha texto. Disponível em: <http://www.escoladegoverno.pr.gov.br/modules/conteudo/conteudo.php?conteudo=581> Acesso em: 10 maio 2016.

HOROWITZ, Ellis; SAHNI, Sartaj. **Fundamentos de Estruturas de Dados**. Tradução: Thomasz R. Rawicki. Rio de Janeiro: Campus. 1987.

IDC. **Estudo da IDC Brasil mostra recorde nas vendas de smartphones no terceiro trimestre de 2014**. 2014. Disponível em <http://www.idcbrasil.com.br/releases/news.aspx?id=1777> Acesso em 25 maio 2016.

INPI – Instituto Nacional de Propriedade Intelectual**. Método de Cruzamento de Dados de Laudos Periciais de Dispositivos Móveis – SICRET**. Revista da Propriedade Industrial - Seção I. Nº 2350, de 19 de Janeiro de 2016. p. 167.

KUECHLER, William L. **Business applications of unstructured text**. Communications of the ACM, v. 50, 2007, p. 86-93.

KRUSE, W.G.; HEISER, J.G. **Computer forensics: incident response essentials.** Indianapolis: Addison-Wesley, 2002.

MICHAUD, D.J. **Adventures in computer science**. SANS Institute, 2001.

MOOERS, C.N. **Zatocoding applied to mechanical organization of knowledge**. American Documentation, v. 2, 1951, p. 20-32.

NOGUEIRA, Sandro D'Amato. **Crimes de Informática**. Leme: BH Editora e Distribuidora, 2ª. ed., 2009.

RICCI, Henrique Cavalheiro; FREITAS, CInthia Obladen de Almendra Freitas. **Os Títulos de Crédito Eletrônicos e sua (In)Compatibilidade com os Princípios do Direito Cambial: por uma mudança de paradigma frente aos documentos eletrônicos**. Revista Jurídica CESUMAR. Mestrado, v. 12, p. 439-461, 2012.

SANTIN, Priscila Louise Leyser ; FREITAS, Cinthia Obladen de Almendra; PARAISO, Emerson Cabrera; SANTIN, Altair Olivo. **Modelagem de Aliciamento de Menores em Mensagens Instantâneas de Texto**. In: XII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2012), 2012, Curitiba. Porto Alegre: Sociedade Brasileira de Computação, 2012. v. 1. p. 288-301.

UNODC - *United Nations Office on Drugs and Crimes*. **Comprehensive Study on Cybercrime**. 2013. Disponível em <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> Acesso em: 10 maio 2016.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012.