XII EPCC ENCONTRO INTERNACIONAL DE PRODUÇÃO CIENTÍFICA DA UNICESUMAR
19 a 21 de outubro de 2021
ISSN 2594-4991
ISBN 978-65-5615-456-5

UM ESTUDO SOBRE O IMPACTO DA INTERCONEXÃO DE BANCOS DE DADOS E OUTROS RECURSOS DE SOFTWARE NA CRIMINALÍSTICA

Michelle Maioli Caobianco[1]

[1]Graduada em Engenharia de Software, Campus São Vicente/SP, EAD - Universidade Cesumar - UNICESUMAR

RESUMO

No relatório ENASP de diagnóstico da investigação de homicídios o Brasil possui um índice de elucidação de crimes de 6%. Através do ponto de vista de Engenharia de Software esta pesquisa visa apresentar dentro do cenário da Tecnologia de Informações modelos e aplicações de ferramentas e recursos de software visando aumentar este índice. O ponto focal deste projeto é demonstrar a importância de ter um banco de dados interconectado, atualizado e precisos entre as agências. Além de analisar a influência de outros recursos como a padronização de evidências digitais, uso de Big Data e Inteligência Artificial na criminalística. Esta pesquisa possui caráter exploratório e descritivo, apresentando análises qualitativas e quantitativas obtidas via pesquisa de campo realizada com profissionais que atuam na área de perícia digital. Foi realizada uma extensa pesquisa bibliográfica e dos dados públicos disponíveis com a finalidade de sugerir soluções para a melhora do índice em questão.

PALAVRAS-CHAVE: Inteligência artificial; Big Data; Bancos de dados, Elucidação de crimes.

1 INTRODUÇÃO

O índice de resolução de Crimes no Brasil é um dos mais baixos do mundo. Conforme uma matéria publicada matéria publicada na Super Interessante/Mundo Estranho de Abril de 2018 este índice é de 6%, tais dados estão presentes no relatório ENASP de diagnóstico da investigação de homicídios no Brasil (CNMP, 2012). Vários fatores afetam este índice incluindo a falta de comunicação entre agências de inteligência e outros órgãos da polícia e a falta de interconexão de seus bancos de dados. Um banco de dados é basicamente um sistema computadorizado de manutenção de registros. O projeto visa apresentar soluções viáveis para melhorar a média brasileira de resolução de crimes, com o auxílio de ferramentas de software, a padronização da Evidência Digital, a interconexão de Bancos de Dados, Big Data e Inteligência Artificial. Usando como exemplo países onde tais recursos estão bem estabelecidos e consultando profissionais da área em território nacional pretende-se mostrar a importância destes recursos no aumento deste índice.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é apresentar de forma sucinta o uso de Big Data, integração de Bancos de Dados e outras ferramentas de software no combate ao crime e sua viabilidade no Brasil visando aumentar o índice de solução de crimes no país. Foi estudado quais recursos de Software são utilizados nos países cujos índices são mais altos, verificando quais deles já estão em uso no Brasil e qual a viabilidade de utilizá-los no território nacional.

1.2.2 Objetivos Específicos

A pesquisa científica deste trabalho tem como segunda etapa avaliar desde a adaptabilidade de novas tecnologias, já usadas em outros países, até quais são os desafios para a amplificação do uso das já presentes no país em todo o território nacional. O segundo e mais importante passo deste projeto é o estudo sobre a importância da interconexão

ISSN 2594-4991
ISBN 978-65-5615-456-5

entres os Bancos de Dados no Brasil e quais os impactos positivos desta prática sobre a resolução de Crimes no Brasil.

1.3 JUSTIFICATIVA

Este projeto visa demonstrar, a partir de uma análise, a enorme importância dos recursos e ferramentas de software na prevenção e combate aos diversos tipos de crimes. O fato desta análise ser feita a partir de informações coletadas diretamente dos próprios profissionais da área, também serve como um mapeamento mais atualizado e preciso de quais aspectos realmente afetam a elucidação destes crimes vinda de quem trabalha diariamente com estes recursos. Servindo como referencial para empresas privadas e para órgãos públicos sobre a necessidade de investimento no setor e os impactos positivos da implementação dos temas apresentados, além da melhora do índice de resolução de crimes sob o ponto de vista de Engenharia de Software.

2 REFERENCIAL TEÓRICO

2.1 EVIDÊNCIAS DIGITAIS

No mundo globalizado e moderno é mais que necessário falar de Evidências Digitais, como Kävrestad (2018) cita em seu livro sobre os Fundamentos Forenses Digitais o ser humano está a maior parte do tempo conectado, mesmo quando está *off-line*, sendo então numa sociedade moderna muito difícil ao cometer um crime não deixar algum tipo de evidência digital. Desde informações relevantes sobre o que aconteceu, como os acontecimentos antes e depois do crime ser cometido também podem deixar rastros digitais. Um enorme problema neste campo é a dificuldade da triagem. O professor, consultor de Investigações Digitais e palestrante Matthew Sorell da Universidade de Adelaide da Austrália cita porque deste problema ter se tornado um ponto nevrálgico nas investigações:

> Tem tanta evidência digital de tantas fontes que está se tornando impraticável analisar de forma completa tudo. Isso significa que uma técnica diferente é necessária porque o crescimento é exponencial, mas o potencial de crescimento dos laboratórios é linear. Extração seletiva, técnicas de triagem, amostragens e inteligência artificial foram propostas. E tem os desafios da inevitável contaminação ou degradação das fontes de evidência digital na cena do crime. Nós não temos o luxo, nem sequer a opção de ter evidências puras, sem contaminação e ter uma análise exaustiva. Temos que tomar decisões baseadas em risco para escolher a menos pior das opções para assegurar, adquirir e analisar as evidências digitais. (SORELL, 2019, tradução nossa).

Logo se faz necessário um estudo sobre os métodos e recursos de software de triagem, que se mostram tão importantes quanto a aquisição e coleta da evidência digital.

2.2 BIG DATA E IA

Quando se fala em grandes volumes de dados já automaticamente surge diversas vezes o termo *Big Data.* No entanto, este termo é bem mais abrangente, como explica Taurion (2019), pois envolve outros fatores em sua composição, desde a variedade de dados até a análise destes quando as ferramentas típicas não dão conta de capturar, gerenciar e analisar volumes tão massivos de informações.

Complica ainda mais quando é necessário fazer o processamento e análise destes dados no âmbito da perícia digital. Isso se deve ao fato de que os bancos de dados relacionais não terem capacidade de lidar com um número massivo de dados de forma

ISSN 2594-4991
ISBN 978-65-5615-456-5

eficiente, pois o método amostral pode deixar passar detalhes que podem ser essenciais para a elucidação e até mesmo a prevenção de crimes.

Com o auxílio de Big Data, no entanto é possível fazer essa correlação e busca por padrões de forma a prevenir futuros crimes ou solucionar crimes já cometidos. Um dos métodos mais conhecidos de encontrar tais padrões se dá pelo processo de Data Mining, que age como um processo de mineração destes dados. Este consiste em limpar dados inconsistentes e sem sentido, fazer a integração dos dados que possam ser combinados, seleção, transformação, extração, avaliação e, por fim, a apresentação destes dados (HAN; PEI; KAMBER, 2012).

Tais avanços na tecnologia permitem que tempo seja economizado e que a eficácia aumente nas investigações. Entretanto outro nome tem ganho cada vez mais destaque no âmbito pericial digital: Inteligência Artificial (IA). Quando o FBI começou a implementar perfis de criminosos violentos, mal eles podiam imaginar que tal análise ia contar com o auxílio de tais recursos de software. Através do sistema de IA, uma investigação foi resolvida de forma pioneira em 1963 quando um perfil foi criado a pedido da polícia local para solucionar um caso sobre incêndios criminosos na região de Nova Inglaterra. O conteúdo não só continha uma descrição do suspeito em detalhes, como também onde ficaria sua residência de acordo com cálculos computacionais gerados através da Inteligência Artificial (ICOVE, 1986). Termo (IA) que é definido como a ciência e engenharia da criação de máquinas inteligentes (MCCARTHY, 1956, tradução nossa), mas na prática é algo muito mais complexo. Tal exemplo abriu um leque de possibilidades tanto na solução quando na prevenção de crimes.

Segundo Zeno Geradts, em sua palestra na *InterFORENSICS* de 2019 como Key Note Speaker, o uso da Inteligência Artificial no ramo forense tem se expandido. Ao lidar com Big Data uma preocupação é a redução do tempo gasto analisando grandes volumes de dados e encontrar somente os dados relevantes. No serviço chamado HANSKEN, criado pelo Instituto Forense Holandês para processar e analisar muitos terabytes de material apreendido, é aqui que a IA ganha um papel de destaque: automatizando esta análise de forma inteligente.

2.3 INTERCONEXÃO DE BANCOS DE DADOS

A tecnologia de lidar com dados massivos já existe, porém sozinha e sem o compartilhamento de informações, ou do uso da mesma base de dados entre as agências de inteligência, as consequências podem ser catastróficas. O maior e mais significativo exemplo disso foi em 11 de Setembro de 2001, quando os Estados Unidos tiveram o ataque terrorista mais significativo de sua história. Porém pouco se é falado sobre qual foi o grande vilão quando se trata de a tragédia poder ter sido evitada. Um memorando foi publicado por John Ashcroft frisando a relevância do compartilhamento de informações e recursos, assim como colaboração entre órgãos federais, estaduais e locais:

> Os ataques de 11 de setembro demonstram que a guerra ao terrorismo deve ser combatida e vencida em casa, bem como no exterior. Para atender a essa nova ameaça e evitar futuros ataques, agentes de segurança pública de todos os níveis de governo - federal, estadual e local - devem trabalhar juntos, compartilhando informações e recursos necessários, tanto para prender quanto para processar os indivíduos responsáveis e detectar e destruir células terroristas antes que elas possam atacar novamente (Ashcroft, 2001, tradução nossa).

Este grave problema ficou conhecido como uma falha em ligar os pontos no livro *After: How America Confronted the September 12 Era*, que relata que as agências de inteligência estavam descoordenadas e que tais ataques poderiam ter sido prevenidos se houvesse um esforço conjunto (Brill, 2013).

ISSN 2594-4991
ISBN 978-65-5615-456-5

No relatório apresentado pela Comissão Nacional Sobre Ataques Terroristas é mencionado que a tragédia deve ser considerada como uma lição a ser aprendida sobre a importância de integrar a inteligência estratégica de todas as fontes de uma forma unificada (The 9/11 Comission Report, 2004). Em outro relatório feito para o Congresso Norte-Americano feito em 2003 cita que as melhorias na inteligência e compartilhamento de informações é essencial para combater o terrorismo (Gilmore *apud* BEST Jr, 2003, p. 17).

Cerca de 15 anos após o ataque foi publicada uma matéria na revista The Atlantic, escrita por Steven Brill, o mesmo autor do livro citado anteriormente, sobre o que mudou e se tal lição foi aprendida, relatando que atualmente as agências de segurança americanas compartilham das mesmas listas de observação e bancos de dados sobre ameaças, que são constantemente atualizados e que os orgãos federais e locais passaram a contribuir e compartilhar entre si em forças-tarefas conjuntas (REVISTA THE ATLANTIC, 2016).

Este banco de dados de sigla NCIC, *National Crime Information Center*, criado em 1967, contém também impressões digitais de DNA de 32 milhões de americanos (IDEA, 2011), 7 setores voltados para propriedades roubadas (barcos, carros etc) e 14 voltados para pessoas (pessoas violentas, imigrantes ilegais, suspeitos de terrorismo, agressores sexuais etc), o sistema contém também imagens que podem ser correlacionadas com os registros. Seus registros já continham dados sobre Gangues Violentas e Organizações terroristas antes da tragédia de 11 de Setembro, porém eram poucos registros, atualmente ele é o ponto central de informações coletadas sobre suspeitos de terrorismo segundo o site do FBI (2019).

O uso de sistemas como o NCIC que integram dados de segurança pública, poder judiciário e sistema prisional se tornou um marco em países desenvolvidos. O verdadeiro desafio é trazer este conceito para o território nacional, avaliar quais são as dificuldades de integrar as informações entre os órgãos e agências de inteligência.

Alguns estados brasileiros já estão fazendo um esforço para algo nesse padrão, mas é necessário a conversa entre estados e também entre os órgãos locais e federais. O Brasil já conta com um Banco Nacional de Perfis Genéticos, mas ainda estamos anos-luz de ter algo completo e categorizado como o modelo americano. Desde que foi implementado em 2012 ele conta com mais de 6500 perfis genéticos, sendo um número lastimável levando em consideração que em 2017 a populações prisional do Brasil era de 726 mil (REVISTA AGÊNCIA BRASIL, 2017), ou seja, não cobre nem os criminosos que estão atualmente encarcerados, muito menos os soltos por todo o território nacional.

O mais próximo que o Brasil tem no momento é o Sistema Nacional de Estatística de Segurança Pública e Justiça Criminal (SINESPJC), que é o sistema informatizado de informações de segurança pública e justiça criminal, o qual reúne informações sobre perfil da vítima, perfil do autor, número de ocorrências, entre outros. Porém o envio dessas informações é responsabilidade de gestores estaduais e mesmo tendo uma importância vital para uma base de dados sólida e confiável, não há um controle de qualidade das informações enviadas. Outros problemas citados são: a falta de periodicidade no envio das informações, o uso de metodologias diferentes no envio dessas informações e principalmente a falta de integração que geram o problema principal de nosso país ao tentar fazer um Banco de Dados nacional: a dificuldade no “cruzamento de dados das polícias civis e militares com os dados de outras bases federais e estaduais” (LIMA, 2016).

3 METODOLOGIA

A pesquisa tem natureza básica com caráter exploratório e descritivo, incluindo apresentação de análises qualitativas e quantitativas. Entre as abordagens utilizadas foi desenvolvida uma pesquisa baseada em dados coletados em pesquisa de campo, pesquisa bibliográfica, dados públicos disponibilizados em sites oficiais e entrevistas com profissionais da área.

ISSN 2594-4991
ISBN 978-65-5615-456-5

3.1 PESQUISA DE CAMPO

Através da pesquisa de campo no evento *InterFORENSICS* de 2019 pretendeu-se, com a aplicação de questionário, coletar a opinião dos profissionais de perícia digital do Brasil e do exterior para posterior tratamento e análise qualitativa.

3.2 PESQUISA BIBLIOGRÁFICA E DADOS PÚBLICOS

Com o estudo bibliográfico é possível entender a importância dos tópicos abordados tanto no âmbito nacional, quanto internacional. Desde livros, e-books atualizados sobre bancos de dados, IA, Big Data, até dados disponibilizados pelos sites oficiais para posterior tratamento e análise quantitativa.

4. MATERIAIS E MÉTODOS

4.1 COLETA DE DADOS

Para atender ao objetivo de analisar o quanto as ferramentas e recursos de software afetam o índice de resolução de crimes foi feita a coleta dos dados via um questionário através de uma pesquisa de campo contendo 10 perguntas sobre o tema com o intuito de coletar a opinião de profissionais da área de perícia digital. Este foi distribuído para os profissionais presentes no evento *InterFORENSICS* em maio de 2019. O evento possuía especialistas das áreas de perícia desde medicina legal até TI (Tecnologia da Informação), porém o questionário só foi entregue para os que atuam na área de perícia digital. Esta seleção inicial foi feita com a finalidade de obter respostas qualificadas além de uma visão global sobre o tema.

4.2 TRATAMENTO DE DADOS

Após a coleta foi feita a tabulação dos dados provenientes da pesquisa de campo e elaboradas tabelas e gráficos contendo as respostas gerais, somente dos brasileiros e somente dos estrangeiros. Esta etapa foi repetida para cada uma das perguntas elaboradas.

4.3 ANÁLISE DE DADOS

Foi feita inicialmente uma análise quantitativa dos dados. Mesmo sendo uma amostragem relativamente pequena o fato de serem profissionais qualificados que atuam com perícia digital que se torna um fator de peso para os resultados obtidos. Posteriormente foi feita a análise qualitativa para ilustrar e relacionar a opinião dos brasileiros e estrangeiros participantes de forma a responder a problemática da pesquisa e ilustrar a opinião destes quanto à real importância da área TI na criminalística.

4.4 RELATÓRIO QUANTITATIVO E QUALITATIVO

Participaram da pesquisa de campo 49 profissionais da área de perícia digital, sendo destes 37 do Brasil, 2 da Coréia do Sul, 2 de Omã, 1 da Ucrânia, 1 da Holanda, 1 da Malásia, 1 de Bangladesh, 1 dos Estados Unidos, 1 da Austrália, 1 da Singapura e 1 da Croácia. Foram feitas as mesmas 10 perguntas para todos os participantes em português para os brasileiros e em inglês para os estrangeiros. Foram abordados a interconexão de bancos de dados e sua importância, a familiaridade dos participantes com IA/Big Data, qual o foco

ISSN 2594-4991
ISBN 978-65-5615-456-5

que os recursos e ferramentas de software devem ter na criminalística, quais destes afeta mais o índice de elucidação de crimes, qual o grau de importância da padronização de evidências digitais e se fazem ou não uso da ISO 27037:2013(2012 para estrangeiros). Foi também disponibilizado um espaço discursivo para colocarem quais outras ferramentas e recursos acham importantes para a melhora do índice. Relatou-se uma unanimidade expressiva quanto à interconexão de bancos de dados e sua influência no índice de elucidação de crimes em todas as nacionalidades. Sobre o foco das ferramentas e recursos de software os brasileiros mostraram, em sua maioria, igualmente preocupados com ambas prevenção e solução de crimes. Os estrangeiros já se mostraram divididos nesta questão.

4.5 ESTUDO BIBLIOGRÁFICO

Foram analisados durante a pesquisa diversas vertentes que podiam influenciar o índice de elucidação de crimes no Brasil. Após a pesquisa de campo feita com os profissionais da área de perícia foi possível filtrar para dois pontos focais: a interconexão de bancos de dados e a prevenção de futuros crimes com as tecnologias estudadas. Baseada nessa premissa foi necessário estudar um modelo funcional de Banco de Dados interconectado em um país cujo índice de elucidação de crimes seja alto para assim definir uma base sólida como meta nacional. O modelo escolhido para análise foi o estadunidense *National Crime Information Center*, atualmente de acordo com o estudo realizado pela Statista os Estados Unidos possuem um índice de resolução de homicídios em torno de 62,3% (STATISTA RESEARCH DEPARTMENT, 2019). Não é um número muito expressivo, mas em contraste com os 6% do Brasil este ganha um contraste bem grande no diferencial de forma que tais países conseguem ter eficiência neste campo tão importante. Outro motivo por escolher tal país é o tamanho de seu território: locais como o Reino Unido cuja taxa é 90% também possuem um território e população muito pequenos, sendo assim mais fácil o monitoramento e eficiência de qualquer método aplicado. Conclui-se então que estudar um país cujo território apresenta características semelhantes ao brasileiro e ao mesmo tempo consegue ter eficiência é mais sensato.

Essa interconexão entre bancos de dados com a finalidade de elucidar crimes violentos é tão importante que o atual governo do presidente Jair Messias Bolsonaro lançou no dia 29 de agosto de 2019 um projeto de nome “Em frente, Brasil” justamente para adotar medidas conjuntas entre União, estados e municípios (PORTAL DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2019). Reconhecendo assim que a comunicação falha entre tais órgãos afeta diretamente o índice de elucidação de crimes no território nacional e a importância de tal interconexão entre eles. Quando esta pesquisa foi iniciada o mais próximo de uma iniciativa para melhorar tal comunicação era do SINESPJC como já citado anteriormente neste artigo. No entanto ao se relevar um projeto do governo atual focado nesta temática pode-se concluir que houve um início da valorização deste tema. Algo muito importante do aspecto técnico-científico, pois mostra que o governo está alinhado com as pesquisas e reconhece aonde é preciso melhorar para que o índice brasileiro alcance níveis aceitáveis.

Outro ponto que chama a atenção é que o NCIC foi estabelecido em 1967 nos Estados Unidos, digitalizando arquivos policiais e tornando-os disponíveis para o uso de diversas agências pelo país todo, facilitando a captura de criminosos que de outras formas facilmente se manteriam foragidos (FOREST, p.24,20170) e em pleno 2020 o Brasil ainda está na fase de início de projetos para unir e melhorar a comunicação entre as partes estadual, federal e local. No entanto a tecnologia avançou muito nos últimos anos o que facilita e agiliza a implantação, tendo como maior impedimento então somente a colaboração entre os órgãos, a extensão do território nacional e a burocracia para tais mudanças ocorrerem em escala nacional. Bancos como o NCIC são a prova de que mesmo em territórios extensos quando há a colaboração entre as polícias e o governo pode-se

ISSN 2594-4991
ISBN 978-65-5615-456-5

obter resultados incríveis através da computação. Os dados coletados de todo o território americano estão acessíveis para qualquer agente da lei que esteja em campo, não somente em determinados locais físicos para consultas. Um oficial da lei consegue de seu veículo acessar de prontidão dados sobre pessoas procuradas, histórico de antecedentes criminais, pessoas desaparecidas e até propriedades roubadas em um âmbito nacional. Essa facilidade resulta em um aumento da eficácia da força policial para agir com rapidez tanto em crimes violentos quanto outros crimes. Dados periciais e laudos também podem ser analisados numa perspectiva nacional facilitando a identificação tanto dos suspeitos quanto de crimes seriais.

Desde 1999 o NCIC passou por uma atualização e passou a ser chamado de NCIC 2000. Como consta no manual disponibilizado pelo governo americano, este banco de dados manteve a base do de 1967 e adicionou novas funcionalidades condizentes com o avanço da tecnologia computacional (NCIC 2000 OPERATING MANUAL, s.d). Grande parte do estudo realizado nesta etapa do projeto é baseado na versão atualizada deste banco de dados e seus manuais. Uma base sólida e organizada é essencial para qualquer banco de dados, neste banco cujos dados são sensíveis não poderia ser diferente. Nele estão contidas informações sobre pessoas procuradas, sobre pessoas desaparecidas, sobre pessoas ainda não identificadas, sobre propriedades roubadas, histórico criminal, sobre investigações em curso e sobre indivíduos identificáveis com a finalidade de prever, antecipar ou monitorar a atividade dos criminosos. No momento, o banco de dados serve agências de 50 estados americanos, além de também servir a Porto Rico, Canadá e ao distrito de Columbia.

Para manter os dados atualizados as agências que os colocam no sistema devem estar disponíveis 24 horas por dia para a confirmação destes. Em caso de a agência não ter disponibilidade de responder 24 horas por dia a mesma deve assinar um acordo com uma agência que possa fazer esta confirmação através de um “Holder of the Record Agreement” (Acordo de Detentor de Registro) e disponibilizar instruções e um telefone para contato caso necessário. Já a integridade do sistema é gerenciada pelo FBI, que faz o controle de qualidade destes registros e possui algumas funções automatizadas como deletar permanentemente registros obsoletos e rejeitar registros com erros comuns.

De acordo com o manual do NCIC 2000 os novos registros são feitos da seguinte forma: primeiramente os dados geralmente são inseridos no sistema por uma agência de origem (agência cujo mandato foi feito, ou onde a queixa foi prestada, etc.) em um terminal com acesso à rede. Os dados inseridos devem obedecer à critérios e padrões pré-estabelecidos para o tipo de registro a ser inserido. O sistema deve operar sem interrupções 24 horas por dia e 7 dias por semana. O sistema NCIC 2000 pode interagir com diversos tipos de hardware e de diversos fabricantes. Os únicos requisitos são de poder efetuar a comunicação via BiSync, TCP/IP ou protocolo SNA. (NCIC 2000 Operating Manual, s.d., tradução nossa.)

O sistema também possui um padrão de mensagens que aparecem para o agente consultando o sistema. Por exemplo, caso seja um estrangeiro ilegal a mensagem pede para não efetuar a prisão baseada apenas naquela informação e para contatar a Interpol e a imigração imediatamente, mas no caso de um criminoso violento o sistema exibe uma mensagem de cautela na abordagem.

Todos os terminais que usem o NCIC devem passar por uma auditoria que analisa precisão, segurança, plenitude e periodicidade de seus registros. Cada agência que insere dados no NCIC deve oferecer um treinamento aos agentes que forem inserir dados no sistema, além de ser responsável pelos dados que inserir. O FBI dá suporte para essas agências com a finalidade de juntos manterem um sistema íntegro e funcional. Este esforço conjunto aliado ao padrão para cada tipo de entrada, modificação e exclusão de dados é um dos fatores que torna o sistema robusto e confiável. Para auxiliar no controle de qualidade o FBI conta com um sistema de gerenciamento ERMS (Eletronic Records

ISSN 2594-4991
ISBN 978-65-5615-456-5

Management System), a sua equipe periodicamente checa o sistema para ver se as informações estão precisas e classifica os erros em duas categorias: erros sérios e erros não-sérios. Procedimentos padrão também são estabelecidos para lidar com cada tipo de erro. Em erros sérios, por exemplo, o registro é cancelado e uma mensagem administrativa é enviada à agência de origem.

A validação também faz parte do controle de qualidade, pois checa se o registro está completo e se a informação ainda está ativa. O NCIC faz uma checagem periódica que segue uma ordem pré-estabelecida: em janeiro eles checam os registros feitos em outubro do ano anterior, em fevereiro os registros de novembro e assim por diante. Todo o controle é padronizado e feito mensalmente. Também seguem uma sequência com prioridades baseados no tipo de dado a ser validado. A ordem que consta no manual é a seguinte:

1. Procurado/Membro de Gangue
2. Desaparecido/Sem identificação
3. Veículo/Placa/Parte/Barco
4. Arma
5. Títulos Financeiros Ordem Protetiva
6. Soltura Supervisionada
7. Registro de Agressor Sexual Nacional
8. Roubo de Identidade
9. Artigo Roubado
10. Pessoa Violenta

(NCIC 2000 Operating Manual, s.d., p.88, tradução nossa.)

Ao pensar na implantação de um Banco de Dados do porte do NCIC no Brasil é necessário também tomar como base os cuidados e restrições de acesso necessários pela sensibilidade das informações contidas. De acordo com a FAS (Federation of American Scientists, federação dos cientistas americanos) o NCIC possui alguns cuidados com a segurança tanto em sua base quanto nos computadores que possuem acesso ao mesmo. Tais cuidados são essenciais para prevenir o acesso não autorizado e também o uso não autorizado dos arquivos nele contidos. Os cuidados necessários utilizados pela NCIC (Portal da Federation of American Scientists, s.d.) e que seriam indispensáveis no Brasil são que:

- A central de dados deve ter seu acesso físico restrito e monitorado para impedir o acesso ao equipamento ou aos dados ali armazenados.
- Todo o acesso aos centros computacionais deve ser rastreado, supervisionado e monitorado pela central.
- Todo computador com acesso ao banco de dados deve ter instruções computacionais que restrinjam o acesso a qualquer outro dado ou histórico criminal fora o que for concedido acesso.
- Todo computador com acesso ao banco de dados deve manter um registro de acesso contendo todas as transações de dados e o registro específico de qual agência inseriu ou recebeu dados.
- Todas as transações devem ser monitoradas e revisadas em um período regular com a finalidade de detectar qualquer mau uso.
- As linhas e canais de comunicação para transmitir os dados devem ser de uso exclusivo e dedicado aos registros criminais. E estes devem ser fisicamente monitorados para que não sejam inseridos dispositivos clandestinos para interceptar ou inserir nada nos mesmos.
- Todos os terminais que tiverem acesso ao banco de dados devem ficar um local seguro e monitorado com acesso restrito a um número mínimo de profissionais autorizados. Deve-se ter também o controle e registro dos profissionais que fizeram requisição de acesso para prevenir o acesso de pessoas não autorizadas ou mau uso.

(Portal da Federation of American Scientists, s.d., tradução nossa).

ISSN 2594-4991
ISBN 978-65-5615-456-5

No entanto quando se possui um grande volume de dados como o NCIC é necessário falar sobre Big Data. Atualmente este banco de dados conta com mais de 13 milhões de artigos ativos e é acessado cerca de 12 milhões de vezes por dia pelas autoridades americanas. Como citado anteriormente nesta pesquisa o ataque terrorista de 11 de setembro foi um marco para os americanos aprimorarem não só o modo que eles coletam seus dados, mas também como estes devem ser compartilhados. Conclui-se então que ter o banco de dados por si só não é a única iniciativa para conter a atividade criminosa: é preciso ter uma estratégia entre as agências para que esta seja coletada e compartilhada de forma eficiente. Para resolver este problema os Estados Unidos criaram os Fusion Centers (Centros de Fusão que servem para compartilhar informações entre linhas federais e estaduais), Regional Information Sharing Systems (que coordenam dados coletados) e os Crime Analysis Centers (que analisam os dados coletados) para juntos também se coordenarem com as 17 Agências de Inteligência dos Estados Unidos (Ferguson, 2017). Levando em consideração o que foi passado em sala de aula na Unicesumar em Banco de Dados referente à Big Data é preciso inferir que trabalhar com enormes volumes de dados aumenta a dificuldade não só de trabalhar com as informações disponíveis, mas principalmente a de encontrar as informações necessárias (Carlos Danilo Luz, William Roberto Pelisari, 2018).

Big Data não é só um recurso para elucidar crimes já cometidos, seu uso pode ir além e ajudar a prevenir futuros crimes. Ao utilizar os dados já obtidos é possível reconhecer padrões e assim mobilizar os agentes da lei de acordo com tais cálculos. Nos Estados Unidos já está em uso por mais de 60 agências o PredPol (predictive policing) que clamam que seus dados podem melhorar a detecção de crimes de 10-50% em algumas cidades simplesmente por apontar e direcionar as viaturas para onde um crime está mais propenso a acontecer. Algo similar foi desenvolvido na Itália e batizado de X-Law, começou sendo utilizado em Nápoles, Prato e Veneza. Foi graças a este sistema que previram um roubo a um hotel pois a polícia já estava no local. A análise correta destes dados transforma Big Data em Smart Data (informação inteligente) fazendo com que o uso destes dados seja voltado para a redução de riscos e prevenção de crimes (PIZA; KAPLAN; KENNEDY; 2018).

A prevenção e elucidação de crimes chega em patamar diferenciado quanto se combinam Big Data e Inteligência Artificial. O Netherlands Forensic Institute (Instituto de Ciências Forenses da Holanda) desenvolveu um sistema que analisa dados utilizando Deep Learning, que são modelos computacionais que aprendem com os dados recebidos, quase como funcionaria no cérebro humano (GOODFELLOW, 2016). O uso de tal tecnologia vai desde softwares de reconhecimento facial até o ponto focal desta pesquisa que é a análise de grandes quantias de dados (como e-mails, imagens, áudios, vídeos e outros) e o uso destas técnicas pode ser importante não só para a solução de crimes, mas também a prevenção dos mesmos (GERADTZ, 2018). O Brasil pode se beneficiar de tais tecnologias quando tiver um banco de dados interconectado, atualizado e com dados confiáveis. Sendo a prevenção de crimes um segundo passo na escala evolutiva que deve iniciar com o essencial já apresentado neste projeto.

No entanto não basta ter uma base sólida de dados, recursos inteligentes e não ter profissionais capacitados para utilizarem os mesmos. Ao ter a solução implantada os policiais devem ser treinados e orientados a consultar o sistema em qualquer abordagem. Em Nova Jersey nos Estados Unidos um policial que fazia sua patrulha parou um motorista por estar com apenas um farol do carro funcionando e ao checar o sistema descobriu que o mesmo era procurado por assassinato e assalto à mão armada em outro estado 9 anos antes (LYFORD; WOOD; 1983). Este exemplo só demonstra que além do sistema interconectado, também é preciso que os agentes da lei sejam instruídos a sempre utilizar o mesmo até nas abordagens mais simples.

ISSN 2594-4991
ISBN 978-65-5615-456-5

5 RESULTADOS E DISCUSSÕES

Durante a pesquisa de campo ocorrida no evento *InterFORENSICS* 2019 que reuniu profissionais do Brasil e de outros 35 países das mais diversas áreas da pesquisa foi possível entrar em contato com diversos especialistas em perícia digital. Participaram do questionário 45 pessoas com o questionário físico e 4 outros pelo questionário digital, totalizando 49 participantes. Participaram profissionais atuantes da área de perícia digital do Brasil e outros 10 países, cuja coleta de dados se mostrou muito importante para uma melhor análise do problema apresentado neste projeto e sobre as soluções do ponto de vista dos mesmos.

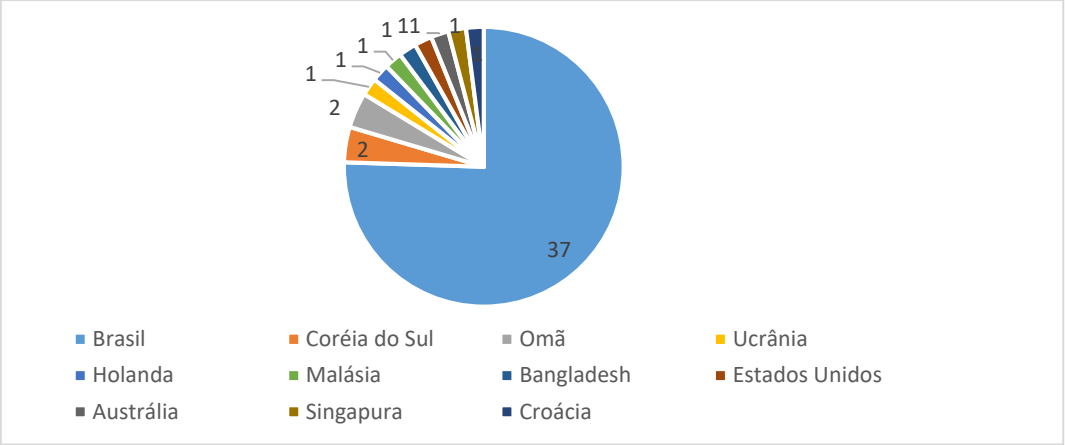

Gráfico 1: Participantes
Fonte: Autor.

Independente dos países de origem foi possível ver unanimidade entre os participantes em duas questões: se o uso de ferramentas e recursos de software afeta positivamente o índice de elucidação de crimes e se a interconexão de bancos de dados também afeta diretamente o mesmo. Constatou-se que todos os participantes concordam que ambos afetam o índice de elucidação, o que comprova a importância da área de TI para uma melhora no mesmo.

6 CONSIDERAÇÕES FINAIS

Em uma sociedade moderna cuja grande parte da interação entre as pessoas produzem dados que podem ser essenciais na solução de crimes é natural que a TI se torne cada vez mais importante da perspectiva forense. Bancos de dados interconectados, agências de fusão e compartilhamento de dados policiais se tornaram essenciais para os órgãos policiais se tornarem eficientes tanto no combate quanto na prevenção de crimes.

Existem diversos fatores que influenciam a eficiência de um país conseguir solucionar seus crimes mais violentos, mas pelo aspecto da TI é possível aprender com os erros e acertos de outros países para implementar soluções nacionais. Com uma base sólida de dados, posteriormente o país pode ir além e também utilizar estes para a prevenção de crimes e monitoramento inteligente. O caminho é longo, porém seguindo os exemplos e soluções apresentados neste projeto, unindo as forças entre o Governo Federal, as Agências de Inteligência e a força policial, é possível trilhar um caminho mais rápido e objetivo para o sucesso.

ISSN 2594-4991
ISBN 978-65-5615-456-5

REFERÊNCIAS

ASHCROFT, John. Cooperation with State and Local officials in Fight Against Terrorism. **Memorando de John Ashcroft para todos os chefes de departamentos e agências federais**, nov. 2001. Disponível em: https://fas.org/irp/agency/doj/agdirective5.pdf. Acesso em: 6 Jun. 2019.

BEST JR., Richard A. The intelligence community and 9/11: Congressional Hearings and the Status of the Investigation. **United States Congressional Research Service**, 2003. RL31650. Disponível em:https://fas.org/irp/crs/RL31650.pdf. Acesso em: 7 jun. 2019.

BRILL, Steven. **After**: how America confronted the september 12 era (English edition). Simon & Schuster, 2003. 736 p. Disponível em:https://ler.amazon.com.br/kp/embed?asin=B000FBJFGO&preview=newtab&linkCode=kpe&ref_=cm_sw_r_kb_dp_ZaS.Cb28CA9PG. Acesso em: 3 jun. 2019.

BRILL, Steven. Is America any safer? Has it worked?. **The Atlantic**, set. 2016. Disponível em: https://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/. Acesso em: 7 jun. 2019.

COUTELLE, José Eduardo. Qual a porcentagem de crimes solucionados pela polícia no Brasil? **Super Interessante**. 2017. Disponível em:https://super.abril.com.br/mundo-estranho/qual-a-porcentagem-de-crimes-solucionados-pela-policia-no-brasil/. Acesso em: 2 jan. 2019.

Federal Bureau of Investigation. **National Crime Information Center (NCIC)**. Federation of American Scientists. s.d. Disponível em:https://fas.org/irp/agency/doj/fbi/is/ncic.htm. Acesso em: 4 jan. 2020.

FERGUSON, Andrew. **The rise of Big Data policing**: surveillance, race, and the future of law enforcement. NYU Press, 2017. 272 p.

ICOVE, David J. Automated Crime Profiling. **FBI Law Enforcement Bulletin**, 1986. Disponível em: https://www.researchgate.net/publication/258512766_Automated_Crime_Profiling. Acesso em: 6 jun. 2019.

IDEA. **The Debatabase Book**. 5. ed. International Debate Education Association, 2011. 236 p.

KENNEDY, Leslie W.; PIZA, Eric L.; CAPLAN, Joel M. **Risk-based policing**: evidence-based crime prevention with Big Data and Spatial Analytics. Univ of California Press, 2018. 168 p. Disponível em:https://play.google.com/store/books/details?id=_sNwDwAAQBAJ&rdid=book-sNwDwAAQBAJ&rdot=1&source=gbs_atb&pcampaignid=books_booksearch_atb. Acesso em: 2 Fev. 2020.

KÄVRESTAD, Joakim. **Fundamentals of digital forensics**: theory, methods, and real-Life applications (English edition). 1. ed. Springer, 2018. Disponível em: https://ler.amazon.com.br/?asin=B07G2XZN8M. Acesso em: 8 Jun. 2019.

ISSN 2594-4991
ISBN 978-65-5615-456-5

LIMA, Vladmir Braga de. **Ferramentas de tecnologia da informação e comunicação na segurança pública:** uma análise sobre o Portal Sinesp e suas ferramentas. Araranguá, 2016. TCC (Especialização Tecnologias da Informação) - UFSC. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/181418/TCC%20Pos%20-%20Vladmir_Revisado%281%29.pdf?sequence=1&isAllowed=y. Acesso em: 8 jun. 2019.

LYFORD, George; WOOD JR., Udy. **National Crime Information Center**: your silent partner. 1983. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/fbileb52&div=23&id=&page=. Acesso em: 3 Jan. 2020.

National Crime Information Center (U.S.). **National Crime Information Center**: the investigative tool: a guide to the use and benefits of NCIC. U.S. Department of Justice, Federal Bureau of Investigation, National Crime Information Center, 1984. 37 p. Disponível em: https://play.google.com/store/books/details?id=7W2-AUOjDqsC&rdid=book-7W2-AUOjDqsC&rdot=1. Acesso em: 4 jan. 2020.

National Comission on Terrorist Attacks Upon the United States, THE 9/11 COMMISSION REPORT. Final Report of the National Commission on Terrorist Attacks Upon the United States. 2004. Disponível em: https://govinfo.library.unt.edu/911/report/911Report_Exec.htm

SORELL, Matthew. Entrevista concedida a Michelle Maioli Caobianco. São Paulo, 24 maio. 2019.

STATISTA. **Crime clearance rate in the United States in 2018, by type**. STATISTA. 2019. Disponível em: https://www.statista.com/statistics/194213/crime-clearance-rate-by-type-in-the-us/. Acesso em: 4 jan. 2020.

TAURION, Cezar. **Big Data**. 1. ed. BRASPORT, 2013. 102 p. Disponível em: https://play.google.com/store/books/details?id=GAVLAgAAQBAJ&rdid=book-GAVLAgAAQBAJ&rdot=1&source=gbs_vpt_read&pcampaignid=books_booksearch_viewport. Acesso em: 4 jun. 2019.