UNIVERSIDADE DO SUL DE SANTA CATARINA
MARCUS VINICIOS PIMENTA DA SILVA

A UTILIZAÇÃO DA INTELIGÊNCIA DE FONTES ABERTAS NAS OPERAÇÕES DAS FORÇAS ARMADAS EM PROVEITO DO PLANO DE SEGURANÇA PÚBLICA PARA O ESTADO DO RIO DE JANEIRO

Rio de Janeiro
2018

MARCUS VINICIOS PIMENTA DA SILVA

A UTILIZAÇÃO DA INTELIGÊNCIA DE FONTES ABERTAS NAS OPERAÇÕES DAS FORÇAS ARMADAS EM PROVEITO DO PLANO DE SEGURANÇA PÚBLICA PARA O ESTADO DO RIO DE JANEIRO

Projeto de pesquisa apresentado ao **Curso de Especialização em Segurança Privada**como requisito para a conclusão da Unidade de Aprendizagem de Metodologia da Pesquisa Científica e requisito parcial para a elaboração do Trabalho de Conclusão de Curso, sob orientação doprofessor Giovani de Paula

Rio de Janeiro

2018

RESUMO

Pelo acontecimento atual, e inédito, como um estado da federação sob intervenção do governo federal – e sob comando de um general do Exército – desde a Constituição de 1988, a intervenção é uma medida mais radical e abrangente do que o uso de militares das Forças Armadas em operações de GLO (Garantia da Lei e da Ordem), como vinha ocorrendo até hoje no Rio e como ocorreram 11 vezes nos últimos 12 meses em outros estados, como o Rio Grande do Norte e Espírito Santo, com base no artigo 142 da Constituição Federal e na Lei Complementar 97/1999. Essa pesquisa tem como objetivo maior verificar se, como nos EUA e Europa, o uso de fontes online e de redes sociais colabora no planejamento de futuras ações e operações, sabendo que elas não se objetivam em resolver situações, mas sim orientar passo mais assertivo nas atividades que se designam, economizando recursos e aumentando a efetividade. Levanta-se como problema de pesquisa se esse uso é adequado e segue os regramentos da legalidade. Para justificar esse estudo, se trazem contribuições, sob a ótica do Direito Constitucional, reflexões sobre o decreto presidencial citado e outras normas que regulam a proteção de dados. Por tratar-se de fato recente, a metodologia da abordagem utilizará fontes jornalísticas, acrescidas de bibliografias jurídicas e legislações anteriores, tendo como objetivo esclarecer os principais pontos do tema sob a égide da técnica legislativa e das Constituições (Federal e Estadual), sem deixar de apresentar hipóteses sobre os aspectos políticos, sociológicos e antropológicos da discussão. Utilizando conhecimentos teórico-empíricos, será realizada em conseguinte, uma especulação sobre a possível colaboração das fontes abertas, como as redes sociais, para contribuir na solução de casos processuais ou criminais, bem como nas operações que ocorrem nas favelas do Rio de Janeiro. Os resultados apresentam exemplos de uso da inteligência das fontes abertas em outras comarcas, e quais as leis e regras para uso e seus riscos no Brasil e no mundo. Em paralelo se discursará sobre o uso das redes e seus usuários, e os benefícios ou danos que podem acarretar quando se trata de dados pessoais em redes sociais. Conclui-se que a inteligência não somente é a captação e analise de dados negados, utilizando-se vigilâncias veladas ou informantes; mas também a simples investigação de fontes abertas como *Google Maps, Fabebook e Instagram*, as quais trazem uma série de percepções da realidade que muito ajudam na tomada de decisões operacionais.

Palavras-chave: Forças Armadas. Segurança Pública. Rio de Janeiro. Fontes de Inteligência. Redes Sociais.

SUMÁRIO

1 INTRODUÇÃO

O Brasil possui um Sistema de Inteligência que tem como fundamentos a preservação da soberania nacional, a defesa do Estado Democrático de Direito e a promoção da dignidade da pessoa humana, em cujas ações devem preservar os direitos e garantias individuais e demais dispositivos da Constituição da República Federativa do Brasil de 1988, bem como os tratados, convenções, acordos e ajustes internacionais. A Atividade de Inteligência contribui na produção de conhecimento voltado para a prevenção e segurança.

As novas tecnologias da informação e da comunicação impõem, no âmbito da atividade de inteligência, a necessidade de constante atualização, e as perspectivas da inovação e do empreendedorismo são fundamentais para que haja mudanças que permitam a evolução dos processos de construção, produção e gestão da informação e do conhecimento. Seguindo como importante, a segurança de dados se torna hoje um problema de difícil solução, e que a sociedade deve ter conhecimento da propaganda perigosa que faz diariamente sobre si nas redes sociais.

Como sempre fazemos, investigar modelos que funcionam ainda em países mais desenvolvidos no assunto sempre colabora com alguns planejamentos necessários, como é o caso da série que será descrita mais adiante, e que trás o pensamento de como proteger a sociedade se ela própria produz provas ou facilita os atos ilícitos acontecerem à elas, por não se informarem antes de fazer uso de tais atividades e postagens.

A era da informação e do conhecimento exige que a sociedade e suas organizações ampliem suas estratégias e ações visando à construção de um ambiente social equilibrado e com o mínimo de conflitos, e as atividades de inteligência são fundamentais nesse processo. A Atividade de Inteligência (AI) é uma atividade do Estado e compreende a busca de conhecimento mediante um conjunto de procedimentos e rotinas específicas visando auxiliar o processo decisório voltado à defesa externa e interna e à manutenção da ordem, numa acepção weberiana de que o Estado detém os meios legais e materiais de dominação e controle e, por conseguinte, os atributos do monopólio legítimo do uso da força.

2 INTELIGÊNCIA EM FONTES ABERTAS:

A informação deve assumir, como linguagem técnica, um contexto muito amplo. As referências aos tipos de conhecimento e as fontes de produção da informação devem representar o resultado de um raciocínio, transmitir a certeza para quem a analisa, num significado contextualizado a respeito de um fato ou ação, suas conseqüências, tanto no passado quanto no presente.

Kent (1966) descreve inteligência sob três aspectos:

> - como produto: é a representação do resultado do processo de produção de conhecimento, atendendo a demanda do tomador de decisão, tornando o resultado obtido por meio do processo de inteligência, um produto de inteligência;
> - como organização: apresenta as estruturas funcionais, que tem como missão crítica a obtenção de informações e a produção de conhecimento de inteligência, podendo ser caracterizados como os operadores da inteligência;
> - como atividade ou processo: refere-se aos caminhos pelos quais certos tipos de informação são requeridos, coletados, obtidos, analisados e difundidos. Determinação dos procedimentos para a obtenção de determinados dados, em especial aqueles protegidos. (KENT, 1966).

Para Shulsky e Schimtt (2002), a inteligência compreende informação, atividades e organizações; e está relacionada à informação que é relevante para se formular e programar políticas voltadas aos interesses de segurança nacional e para lidar com ameaças, atuais ou mesmo potenciais, a esses interesses.

A respeito à atividade em si, a inteligência compreende a coleta, e a análise de informações e inclui as atividades destinadas a conter as diversas atividades de inteligência. Neste contexto Shulsky e Schimtt (2002) afirmam que a contra-inteligência estaria contida na inteligência e concluem que o termo se refere às organizações que exerçam a atividade, atribuindo a elas uma de suas características mais importantes, o secretismo, necessário à conduta de suas atividades.

Para diferenciar inteligência e informação, o Glossário da Organização do Tratado do Atlântico Norte - OTAN define em sua perspectiva, que a informação se refere aos dados brutos, que serão analisados para a produção de um conhecimento de inteligência, informação processada com vistas a subsidiar o processo decisório.

Para David Kahn (1995):

> A função predominante de otimização de recursos materiais e psicológicos seria uma das três características centrais da inteligência, observável na guerra e também na paz. As outras duas características seriam mais visíveis no âmbito estratégico e envolveriam, por um lado, o reconhecimento de o papel auxiliar da inteligência em relação à capacidade combatente e, por outro lado, a associação eletiva entre a defesa e a inteligência. (KAHN. David, 1995).

Segundo George O'Toole (1990), dessa "lei de Kahn" desdobram-se quatro corolários:

> - A ênfase na defesa tende a ser acompanhada pela ênfase na inteligência;
> - A ênfase no ataque tende a ser acompanhada pela ênfase na contra-inteligência para garantir segurança operacional e surpresa;
> - Em situações de impasse e equilíbrio de forças os dois lados tendem a enfatizar a busca de inteligência;
> - E as operações ofensivas que adquirem características defensivas tendem a aumentar a ênfase na inteligência. (O'TOOLE. George, 1990).

Por mais que as fontes abertas na investigação seja um termo comum ao meio policial, em serviço de investigação, ainda nem todos sabem que existem ferramentas de grande valia, que aliados em um trabalho de investigação ou estudo da vida pregressa de uma pessoa ou empresa, que podem encontrar informações diversas sobre a vida de uma pessoa ou o modo de operação de uma empresa na internet, como nas redes sociais, sendo elas um exemplo de fontes abertas.

Na busca da solução de um caso, policiais, detetives particulares e agentes de governo estão usando as fontes abertas na investigação diariamente, para buscar informações sobre a vida das pessoas ou de empresas, e cujas fontes podem ser encontradas nas fontes abertas, ou seja, que está em locais públicos, acessíveis sem necessidade de usar login e senha de seus investigados, o que dependeria de autorização judicial. Porém, a investigação policial deve se adequar à nova realidade dos avanços tecnológicos. Um dos caminhos para isso é a utilização de informações disponíveis em fontes abertas.

Barreto, Caselli e Wendt ressaltam a importância da coleta em fonte aberta tanto para a atividade de inteligência quanto para a investigação policial ao definir como:

> Qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em processos penais e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos federais, estaduais e municipais).

O investigador deve utilizar o serviço fornecido como ferramenta para acompanhamento dos golpes dos casos, seja para consulta no momento da lavratura do boletim de ocorrência, seja para agregar perícia na sua atividade investigativa. Esses dados obtidos em fontes abertas devem ser confrontados com outras fontes de consulta para somar valor na produção de provas ou de conhecimento de inteligência de segurança pública.

O ciclo da inteligência apresenta-se em um processo repetitivo de cinco passos:

I. Planejamento e direção: abrangem o esforço inteiro de gerenciamento do processo e envolvem, em particular, determinar as exigências da coleta baseadas em pedidos dos clientes;
II. Coleta: recolhimento de dados “in natura” para encontrar o objeto dos requerimentos dos clientes, que podem ser derivados (obtidos) de fontes abertas ou secretas;
III. Processamento: é o tratamento dos dados “in natura” para convertê-los a um formato que os analistas de informação possam usar;
IV. Análise e produção: descrevem o processo de avaliação dos dados em sua confiabilidade, validação e relevância, integrando-os e analisando-os, e convertendo o produto deste esforço em um inteiro significativo, o qual inclui avaliações de eventos e de informações coletadas;
V. Disseminação: é a etapa em que o produto da Análise e Produção é distribuído para a audiência pretendida.

A atividade investigativa e/ou produção de conhecimentos na inteligência de segurança pública não podem desprezar os dados de livre acesso em razão dos avanços tecnológicos. Nesse contexto, inserem-se as fontes abertas como mecanismos para agregar valor na produção de conhecimento e/ou elementos informativos.

Open SourcesIntelligence (OSINT) é a inteligência de fontes ostensivas importante para qualquer sistema governamental de inteligência. Trata-se da obtenção de documentos oficiais por vias legais, da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia (jornais, rádio e televisão), da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, fontes disponíveis cujo acesso é permitido.

Quanto mais abertos os regimes políticos e menos restritos às medidas de segurança de um alvo para a circulação de informações, maior a quantidade de inteligência obtida a partir de programas de OSINT. Essas atividades especializadas de coleta absorvem entre 80% e 90% dos investimentos governamentais na área de inteligência nos países centrais do sistema internacional. A maioria desses recursos é dedicada às plataformas, sensores e sistemas tecnológicos de coleta e processamento de informações, especialmente os satélites no caso dos Estados Unidos, Rússia, China, França e outros poucos países que operam frotas desse tipo.

O volume de dados brutos e informações primárias coletadas é muito maior do que os relatórios efetivamente recebidos pelos usuários finais, os responsáveis pela tomada de

decisões e pela implementação de políticas. Segundo uma estimativa da década de oitenta, somente 10% das informações coletadas chega a sair dos muros dos sistemas de inteligência.

Tanto do ponto de vista dos modelos institucionais e procedimentos mais adequados e efetivos para a supervisão externa das atividades de inteligência, quanto do ponto de vista da reflexão sobre os problemas éticos e morais associados à espionagem internacional, essa é uma área de pesquisa sobre o impacto dessas atividades que tende a ser subestimada na literatura especializada. Isso é uma lacuna importante porque mesmo nos países mais democráticos, os mecanismos de supervisão congressual são muito recentes e ainda estão em fase de consolidação.

Conclui-se que a inteligência não garante de antemão a vitória na guerra, nem pode dizer o que vai ocorrer no futuro da política. Por mais que seja decisiva em momentos cruciais na guerra e na paz, em geral os governos contam com a atividade de inteligência para reduzir a incerteza nas suas decisões, para aumentar a segurança nacional e para posicionarem-se melhor no sistema internacional.

2.1 SCORPION SERVIÇOS DE COMPUTADOR, INC.:

Walter O'Brien (1975) é um empresário irlandês, tecnólogo da informação, produtor executivo, e personalidade e o fundador da CEO e da Scorpion Serviços de Computador, Inc. Ele é também a inspiração para um produtor executivo da série de televisão da CBS, Scorpion.

Aos 13 anos fundou o Scorpion Serviços de Computador para área de serviços de segurança. Após sua graduação na universidade mudou-se para os Estados Unidos. A Scorpion Serviços de Computador começou como um serviço de ajuda a TI e se expandiu para a segurança e gestão de risco, uma empresa de inteligência artificial. O'Brien descreve a sua empresa como um “grupo de pensadores para indivíduos com QI elevado".

Baseado na história real desse hacker irlandês, a série Scorpion (CBS) apresenta um grupo de gênios da tecnologia que passa a trabalhar para o governo americano combatendo ameaças virtuais com tecnologias e serviço de inteligência.

Em uma reportagem ao CBS Boston, O'Brien diz que usou a análise forense de vídeo para analisar centenas de horas de filmagem da Boylston Street após os atentados à Maratona. Ele diz que ajudou o FBI a se concentrar nos irmãos Tsarnaev. "Sistemas de reconhecimento de imagem que seriam o que eles usaram para os bombardeiros de Boston

para detectar comportamento suspeito ou quando alguém se comporta de maneira diferente de todos os outros". (HAUSER, 2014).

Essa série citada obteve uma significativa audiência, inclusive de assessores de órgãos governamentais, sendo usado como análise de viabilização de setores voltados as tecnologia das inteligências, e que sempre será objeto de estudo em todo o mundo.

2.2 GDPR: A NOVA LEGISLAÇÃO DE PROTEÇÃO DE DADOS PESSOAIS DA EUROPA:

Em 25 de maio de 2018 entrou em vigor a nova legislação européia sobre proteção de dados pessoais, mais conhecida como GDPR (*General Data Protection Regulation*). Pela relevância da utilização de dados para a movimentação da economia, segurança, educação, etc., notícias de que autoridades de diversos países iniciaram investigações para averiguar como tem sido coletados e tratados os dados pessoais de usuários de internet são intermináveis.

> (6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registraram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.
> (7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores econômicos e as autoridades públicas. (GDPR, 2016).

Os inúmeros índices de irregularidades com o uso dos dados de usuários de Internet podem ser vistos como fator de aceleração do movimento internacional de edição ou atualização das normas sobre proteção de dados pessoais. Os Estados Unidos tem anunciado interesse em editar nova norma para tratar de forma abrangente a proteção de dados pessoais.

Países que desejam se credenciar vaga na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), como o Brasil, estão acelerando a aprovação de umalei geral de proteção de dados pessoais.

A revisão da legislação européia sobre proteção de dados pessoais se iniciou com a constatação de que as regras existentes não estavam acompanhando as rápidas e intensas inovações tecnológicas após a mudança do milênio. Em razão disso, o órgão Supervisor de Proteção de Dados Europeu emitiu comunicado em 2011, recomendando a adoção de nova norma, mais abrangente e destinada a buscar padronização na proteção de dados pessoais na região.

A GDPR foi editada em 24 de maio de 2016 e estabeleceu um prazo de dois anos para que empresas, governo e sociedade civil tomassem conhecimento de seu conteúdo e passassem a implementar as medidas necessárias para o cumprimento de suas disposições. Suas normas, por tomarem a forma de um “Regulamento” ao invés de uma “Diretiva”, são integralmente obrigatórias para todos os países-membros, que poderão editar normas para regulamentar algumas de suas disposições.

Alguns acontecimentos podem ter acelerado a discussão da proteção de dados no Congresso Nacional. Em março de 2018, um escândalo envolvendo dados foi divulgado na imprensa: a utilização de dados pessoais de 50 milhões de pessoas pela empresa Cambridge Analytica na consultoria política do então candidato à presidência dos Estados Unidos, Donald Trump. O método teria sido utilizado para desenvolver ações para influenciar o cenário político americano e favorecer Trump. Os dados teriam vazado do Facebook.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS DO BRASIL:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (LGPD, 2018).

Como todas as leis desse país, o texto dessa lei tramitava a seis anos na Câmara dos Deputados e foi aprovado em 30 de maio de 2018. A redação atual é inspirada em regulações européias sobre o uso de informações pessoais como a Regulação Geral de Proteção de Dados (GDPR).

As informações serão coletadas e tratadas conforme dispõe a nova lei, especialmente em meios digitais, como dados pessoais de cadastro, número de telefone, endereço, estado civil, informações patrimoniais e até mesmo textos e fotos publicadas em redes sociais. As informações de menores acabam protegidos, pois seus dados não podem ser mantidos nas bases de dados das empresas sem o consentimento dos pais.

A lei prevê, ainda, a criação da Autoridade Nacional de Proteção de Dados, uma autarquia cuja principal função será fiscalizar o cumprimento da legislação e aplicar as sanções, e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. O descumprimento de qualquer uma das regras da nova lei poderá acarretar em multa de até 2% do faturamento da empresa responsável.

A proposta prevê ainda que o usuário seja informado quando o uso de seus dados for liberado para o cumprimento de uma obrigação legal ou pela administração. Por outro lado, as normas não se aplicam se as informações forem usadas por terceiro (pessoa física), para fins exclusivamente pessoais, ou se usado para conteúdos exclusivamente jornalísticos, artísticos ou acadêmicos.

Com essa resolução, a segurança nacional também poderá utilizar as ferramentas cibernéticas na função de seus propósitos, sabendo que já temos modelos utilizados em países com segurança exemplar.

> Art. 59. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e de atuação da Autoridade Nacional de Proteção de Dados; II – elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III – sugerir ações a serem realizadas pela Autoridade; IV – realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e V – disseminar o conhecimento sobre proteção de dados pessoais e da privacidade à população em geral. (LGPD, 2018).

2.4 INTERVENÇÃO FEDERAL NO ESTADO RIO DE JANEIRO:

A capital do Rio de janeiro há muito anos vem sendo palco de especuladores sobre o assunto segurança pública, apesar de que em outras unidades da federação as taxas de homicídios sejam inclusive maiores, segundo os dados do Fórum Brasileiro de Segurança Pública, é no Rio de Janeiro que os fracassos nas operações policiais ocorrem em maior número. A aposta pelo uso da força e apelo aos militares vem sendo constante no Estado desde 1992. As Unidades de Polícia Pacificadora (UPPs) representaram tentativa estruturante e de longo prazo, mas também falharam. As operações que aconteceram nas favelas da cidade serviram para encher os noticiários de imagens espetaculares do que para alcançar resultados efetivos.

No dia 16 de fevereiro de 2018 a democracia brasileira viu-se diante de um cenário dramático: o Rio de Janeiro passa a ter dois governadores em exercício em pleno ano eleitoral. Governador Luiz Fernando Pezão (MDB), que ficará responsável por todas as áreas

da gestão estadual exceto a de segurança pública. Sérgio Cabral solicitou o pedidoao presidente Michel Temer, que junto de seu correligionário de partido, decretou a intervenção federalno Rio.

Essa intervenção confere plenos poderes de governador na área de segurança para o chamado "interventor federal". Ficou a cargo de Walter Souza Braga Netto, General de Exército e Comandante do Comando Militar do Leste, ser o chefe máximo das polícias Militar e Civil, Corpo de Bombeiros e da Administração Penitenciária fluminenses.

Cabe ao General tomar todas as medidas que achar necessárias para conter o crime no Rio, incluindo o domínio das facções criminosas de alcance nacional. Michel Temer, então Presidente do país, se defende em uma entrevista coletiva sobre sua tomada de decisão afirmando que "o crime organizado quase tomou conta do Estado do Rio de Janeiro. É uma metástase que se espalha pelo país e ameaça a tranquilidade do nosso povo".

Com a inédita intervenção federal decretada pelo Presidente Michel Temer (MDB), abre-se um novo capítulo na história das tentativas de estancar a violência no Rio e resolver um problema que possui raízes históricas e estruturais. Inédito porque, apesar do uso das Forças Armadas no Rio em outras ocasiões, é a primeira vez desde a redemocratização que o Governo Federal intervém diretamente no estadual, retirando destas suas competências na área de segurança pública e nomeando um interventor federal.

A história da criminalidade no Rio começa lá nos anos 70, quando a cocaína começa a se expandir. Nos anos 80 e 90 com o tráfico vai aumentando seu domínio pela cidade. E por seguinte aparece o fuzil nas mãos dos traficantes, e depois a polícia acompanha e adota o fuzil também. Seguiu-se por uma onda sequestros e as facções foram se consolidando nesse período. Chegamos aos anos 2000 com as UPPs, quando todas as esperanças se acenderam e todos acharam que tinham achado a solução dos problemas da população.

2.5 UPPS E MILÍCIAS:

Em janeiro de 2007 surge o texto que sugere solucionar e estruturar, em longo prazo, a segurança pública no estado. As Unidades de Polícia Pacificadora (UPPs) foram inauguradas no final de 2008 com uma operação no morro Dona Marta, no bairro de Botafogo. A estratégia consistia em expulsar o tráfico e instalar bases da Polícia Militar com agentes de preferência novos, sem antigos vícios da corporação, e treinados para manter uma relação de proximidade com os moradores do local.

Primeiro se fez uma ocupação policial da favela e, paralelamente, levou-se serviços públicos e obras de saneamento. Os tiroteios cessaram em comunidades, atividades econômicas floresceram e as taxas de homicídio diminuíram em todo o Estado, chegando a 28,7 mortes para 100.000 habitantes em 2012. A antropóloga Jaqueline Muniz, especialista de segurança pública da UFF, explica, em entrevista no jornal online EL País, escrita por Felipe Betim em 28 de fevereiro de 2018:

> Isso aconteceu porque a polícia parou de trocar tiro. Quem é o administrador da morte? O Estado. A polícia entrava para impedir disputas entre facções, mas ela depois passou de produzir o confronto e a ocupar o território. Mas o efeito disso é provisório, porque há um rearranjo da economia criminosa. (BETIM, 2018).

A primeira etapa, segurança em si apresentoufracasso, e a segunda etapa, parte de infra-estrutura, nunca chegou a se concretizar. A sociedade se manteve tensa, a relação polícia-morador não se restituiu como esperado, e logo alguns abusos se fizeram evidentes, como o caso do pedreiro Amarildo, que foi detido, torturado e morto por policiais da UPP da favela da Rocinha. Seu caso foi repercutido nacionalmente e internacionalmente.

A adequação das UPPs se mostrou fácil em favelas pequenas como o Vidigal e Dona Marta, mas de difícil aplicação em outras maiores como a própria Rocinha e o Complexo do Alemão, ambas com mais de 100.000 habitantes. Foi nesta última comunidade que, em 2010, uma ambiciosa mega-operação envolvendo a Polícia Militar e as Forças Armadas tentou expulsar o tráfico e instalar uma UPP. O plano para o Alemão nunca foi 100%bem sucedido: tiroteios e abusos continuaram sendo parte da rotina dos moradores, tendo se intensificado nos últimos dois anos.

As UPPs iniciaram seu foco nas favelas da região turística e nobre, e as da zona de classe média a pobre foram deixadas a própria sorte. Não demorou nada para que alguns agentes do Estado (policiais e bombeiros) resolveram adicionar a esse cenário de guerra fria as milícias. Esses agentes controlam determinado território e serviços como o fornecimento de gás. A princípio foi vista com bons olhos da população e políticos até a classificaram como ‘uma espécie de proteção comunitária’, porém o terrorismo era o regime que se fazia reinar dentro da política das milícias.

Uma professora, KSC tinha 32 anos em julho 2008, (não quer ser identificada) conta que morava em outro estado, foi tentar a sorte no Rio, no bairro de Vargem Grande, e pretendia viver na cidade pra sempre, porém não demorou três dias de sua chegada para receber a visita da milícia dentro de sua casa. Suas coisas ainda estavam em caixas por trabalhar muito, não havendo muito tempo para arrumar sua mudança. Nesse dia, três homens

grandes e fortes, com “cara de policiam mal” foram à sua casa, e ela teve de abrir suas caixas à noite para a milícia que a obrigara a fazer na hora. E ainda relatou as exigências que eles disseram que ela devia seguir para ficar “de boa” com eles: não fumar, não usar drogas ou bebidas alcoólicas, não receber homens após a meia noite, e se houver qualquer reclamação de vizinhos ou moradores da sua “comarca”, eles retornariam com mais severidade. Depois de ter ouvido isso, a professora encaixotou tudo e em dois meses retornou ao seu estado natal, para nunca mais se quer querer visitar o Rio de Janeiro.

Cabia a milicianos, por exemplo, autorizar ou não a distribuição de panfletos de campanha ou comícios em determinados bairros. Muitos deles inclusive eram deputados estaduais ou vereadores. As milícias foram alvo de uma CPI na Assembléia Legislativa do Estado do Rio de Janeiro em 2008, comandada pelo deputado estadual Marcelo Freixo, e muitos milicianos chegaram a ser presos e condenados. Mas as milícias nunca deixaram de existir.

Para se ter uma ideia de como nenhuma dessas alternativas mudou o cenário, em 2016 nos Jogos Olímpicos a sensação da população era de segurança nas ruas do Rio enquanto acontecia o evento, o Exército e a Força Nacional patrulhavam as ruas, mas era nas favelas que a polícia agia incessantemente e a violência não cessou durante um minuto.Em2017, o Governo Temer enviou mais uma vez os militares, porém os gastos na Rocinha serviram apenas para apreender algumas armas.

O fracasso das UPPs e as operações policiais de caráter paliativo voltaram aos noticiários, com aumento da taxa de homicídios em 2017. Após tantos fracassos, em 2018, com uma intervenção federal que, embora de caráter inédito, tem muitas semelhanças com outras medidas tomadas ao longo das três décadas passadas.

2.6 AS PUBLICAÇÕES EM REDES SOCIAIS:

Redes Sociais, hoje em dia, são *websites* e portais de relacionamento existentes e disponíveis hoje na Internet, porém, por definição, uma rede social é uma estrutura composta por pessoas conectadas por um ou mais tipos de relações que partilham valores e objetivos em comum. Nesse contexto podemos dizer que redes sociais existem a milhões de anos, desde a era das pedras, onde o home se sentava na fogueira no fim de dia para se aquecer e alimentar com seus pares.

> As redes econômicas serão estabelecidas [...]. Afinal, antes que uma colônia poderia se tornar valiosa e um anexo de uma economia europeia, tinha que ter tendido uma rede de comunicações e transportes. (DE UGARTE, 2007).

As redes sociais nos permitem encontrar emprego, fazer amizades, e namoros através das relações entre as pessoas conhecidas nesse meio, mas um problema existente nessas redes é que muitas vezes, as conexões são desconhecidas.

De acordo com De Ugarte (2007), com a Era das Redes Distribuídas, nascida da conexão de milhões de pontos hierarquicamente iguais através da Internet, qualquer indivíduo pode potencialmente, encontrar, reconhecer e comunicar-se com qualquer um. (DE UGARTE, 2007).

> Este mundo distribuído está dando à luz um meio de comunicação à sua imagem e semelhança: a blogosfera, o conjunto de ferramentas on-line de publicação e comunicação pessoal. (DE UGARTE, 2007).

O perigo nas redes sociais na internet é de asinformações serem repassadas sem sua autorização para outras instituições ou de um atacante comprometer este servidor e obter acesso a todas as informações pessoais, e orienta-se que não se façam transações financeiras*on-line* ao menos que se tenha certeza da idoneidade da instituição que mantém o site.

Quando o usuário é atento e sabe exatamente o risco que corre ao postar informações nessas redes, ele se protege de quaisquer problemas que poderiam tentar fazer com seu nome e dados. É extremamente importante avaliar com cuidado que informações estarão disponíveis nos sites de redes de relacionamentos - principalmente aquelas que poderão ser vistas por todos - e quais comunidades participam. Estas informações podem não apenas ser utilizadas por alguém mal-intencionado, mas também para atentar contra a segurança física do próprio usuário. (CERT.br, 2006).

Um exemplo, uma foto divertida hoje compartilhada no Facebook, pode se tornar uma foto comprometedora no futuro. A falta de percepção existente por parte dos usuários sobre o impacto que o compartilhamento destes conteúdos e outros podem provocar, mesmo que a conta do usuário seja removida da rede são inacreditáveis. Não há retorno. Numa perspectiva empresarial e profissional, estas redes sociais podem ser uma ameaça, uma vez que hoje em dia, as empresas recorrem freqüentemente às redes sociais como uma forma complementar de verificar o perfil dos candidatos.

Num estudo recente realizado pela Sophos 2010, no qual estiveram envolvidas cerca de 500 empresas em que responderam a um inquérito, cerca de 60% consideraram que o

Facebook apresenta-se como uma das principais ameaças à segurança e privacidade da informação das suas organizações (Facebook 60%, Myspace 18%, Twitter 17% e Linkedin 4%). Esse estudo chegou a conclusões assustadoras sobre o comportamento dos utilizadores no Facebook, em relação aos dados que revelam. Assim, conclui-se que:

- ✓ 46% dos utilizadores do Facebook aceitam pedidos de amizade de estranhos;
- ✓ 89% dos utilizadores da faixa etária dos 20 divulgam a sua data de aniversário;
- ✓ Quase 100% dos utilizadores divulgam o seu endereço de email;
- ✓ Entre 30-40% dos utilizadores listam dados sobre a sua família e amigos.

Os usuários estão disponíveis para compartilhar tanto da sua própria informação pessoal no Facebook, fazendo com que o risco de ocorrência de ataques de roubo de identidade ou de engenharia social aumentem consideravelmente. Recentemente foi relatada a história da esposa do diretor do MI6 do Reino Unido, que tinha colocado no seu perfil no Facebook detalhes sobre a sua residência e sobre os seus amigos, colocando a própria segurança nacional em risco. A utilização da inteligência de fontes abertas para a segurança privada, ouno uso militar e policial se justifica mediante o discurso de que depende da futilidade do cidadão em aparecer nas mídias e redes sociais que os direcionam aos riscos diversos, vexatórios e morte.E em se tratando de personalidades públicas e assuntos sigilosos governamentais ou empresariais, a utilização de dados pela razão de justiça e segurança auxilia na tomada de solução para um objetivo de um bem maior.

Especialistas recomendam algumas dicas para se beneficiar das redes sociais de forma racional, e acima de tudo a percepção de quais dados deve compartilhar e que tipos de conteúdo disponibilizar - e para quem. Um conjunto simples de indicações pode melhorar em muito a privacidade dos usuários e reduzir o risco de exposição às possíveis ameaças. Estas indicações podem ser resumidas:

- ✓ Usar corretamente as listas de amigos;
- ✓ Remover-se dos resultados de pesquisa do Facebook;
- ✓ Evitar o tagging (marcação) em fotos e vídeos;
- ✓ Proteger ou restringir os álbuns de fotografias;
- ✓ Evitar que as histórias apareçam no feed de notícias dos seus amigos;
- ✓ Proteger-se contra histórias publicadas por outras aplicações;
- ✓ Tornar a sua informação de contato privada;
- ✓ Evitar postagens que possam ser embaraçosas;

- ✓ Tornar as suas relações privadas.

As ameaças não estão resumidas à privacidade dos usuários e são cada vez mais perigosas.

2.7 O PAPEL DAS MÍDIAS SOCIAIS EM CRIMES ONLINE:

Desde sua criação, a web e as mídias sociais têm tido grande papel nos crimes ocorridos. Em algumas vezes esses crimes não passam de simples mal entendido, porém em outras, são casos sérios, nos quais a rede foi usada como evidência ou flagrante.

Por compartilharem informações entre comunidades, e estarem cada vez mais presentes na rotina das pessoas, pode ser acompanhadas 24 horas por dia, sete dias por semana, devido à mobilidade da Internet, e acesso às mídias por telefone celular, ou outros dispositivos móveis. Porém, como já vimos, no que se diz respeito à segurança dos usuários, verifica-se que por se tratar de mídias relacionadas à maior rede de computadores.

Pode-se afirmar que existem vantagens no uso da Internet como meio de se interagir socialmente utilizando mídias sociais, com inúmeras opções para entretenimento, busca de informações e networking. O desafio está em manter a consciência e mensurar não só a quantidade de informações e dados a se disponibilizar na *Web*, como também a qualidade, tendo em mente as consequências do que aquele conteúdo compartilhado pode causar para os envolvidos.

2.8 OS DADOS PODEM SER UTILIZADOS PELAS EMPRESAS:

Segundo pesquisa divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2013 para 2014, mais de 85 milhões de pessoas estão conectadas à rede mundial e para acessar as redes sociais e se cadastrar em provedores de e-mails, é preciso passar dados pessoais a algum desconhecido. As informações compartilhadas na internet ficam armazenadas em uma central de dados online, conhecida como nuvem. Da nuvem vai direto pra tela do celular ou de qualquer outro dispositivo que permita o acesso a internet.

As redes sociais podem se tornar uma grande armadilha quando o assunto é emprego, no entanto o uso das redes é como um fenômeno social atual, que propicia a interação entre os homens e, conseqüentemente, a realização de diversas trocas entre estes, inclusive a troca comercial. Esse favorecimento de intercâmbio entre as atividades empresarial/comercial e o

desenvolvimento da sociedade, se deu com essa evolução dos meios de comunicação progredindo incansavelmente na atividade comercial no cenário atual.

É com convívio em sociedade que é construída a interação existente entre os homens, a qual se refere à troca simultânea de dois ou mais indivíduos em contato. São evidenciadas diversas modalidades de trocas em uma comunidade (de conhecimentos, dados, informações, produtos, comercial, e etc.).

A troca comercial advém de um passado que sempre utilizou de mercantilismo para realizarem suas relações, obterem suas necessidades essenciais dos seres humanos e da impossibilidade de satisfação das mesmas mediante o simples uso da força de trabalho individual, tendo em vista a gama de interesses complexos existentes e a diversidade dos instrumentos necessários para alcançá-los. Foi por meio de convívio em sociedade que se tornou possível a realização de trocas de produtos entre os membros da comunidade, ou seja, o indivíduo passa a se concentrar na produção de materiais que pode desenvolver com maior facilidade e passa a trocá-lo por outros produtos de outros membros, trazendo benefícios e satisfação para ambas as partes envolvidas.

> “No início do desenvolvimento do comércio moderno, os produtos eram intercâmbiados diretamente nos postos de troca, sendo que na época as moedas não tinham a credibilidade financeira para serem universalmente aceitas. Era a fase do escambo.” (NOVAES, 2007).

Com a evolução e o desenvolvimento da sociedade, a atividade comercial foi se tornando mais intensa, à medida que foi sendo necessário diversificar os materiais, uma vez que a produção para consumo próprio já não era suficiente e as riquezas passaram a ser produzidas com fins de permuta. Nessa medida, com o desenvolvimento dessa atividade, a permuta de um produto por outro foi sendo substituída por itens intermediadores – gado, peixe – que serviam como moeda e, gradativamente, o homem desenvolveu mecanismos que facilitaram o fluxo de mercadorias (MEDEIROS, 2011).

As empresas perceberam a valia da globalização e a revolução tecnológica, que possibilita obter receitas fora do país sede. Sendo assim, se torna um importante meio de divulgação dos produtos e serviços oferecidos pela organização empresarial em escala global, tornando-se uma ferramenta de marketing. O Marketing pode ser entendido como processo usado para determinar que produtos ou serviços se comunicam com seus consumidores, assim como avaliar a estratégia que utilizará nas vendas do negócio.

Segundo Peter Drucker (1980):

> O marketing é colocado como uma força poderosa a ser considerada pelos administradores focados no mercado, na medida em que se ocupa da arte de como atrair consumidores, identificando a necessidade e criando a oportunidade de negócio. Nessa medida, considerando que a rede social permite o estabelecimento de trocas instantâneas entre os membros, esta passa a ser uma importante ferramenta em termos de atração de consumidores e, conseqüentemente, realização de vendas. (DRUCKER. Peter, 1980).

Os membros das redes sociais possibilitam a integração entre diferentes povos e entre diferentes culturas, onde influenciam uns aos outros virtualmente. Da mesma forma que a pessoa física cria seu perfil e demonstra se identificar com determinados assunto, as empresa também podem divulgar seu perfil, agregando pessoas que estão predispostas a esse assunto em questão e aumentarem suas chances de negócios bem como influenciar diretamente o consumidor e estabelecer um modelo ou padrão de consumo associado ao produto da empresa.

No caso de as empresas desejarem saber sobre quem contratar, as empresas utilizam as redes sociais para averiguarem o perfil do possível candidato e suas qualificações na sociedade. Para a segurança privada, tal aspecto é fundamental, pois se podem averiguar desvios de conduta do candidato a vigilante, por exemplo.

O convívio social estabelecido entre empresa e o consumidor gera ganhos para a empresa, haja vista o número de compradores que são alcançados por meio da rede social e a rápida troca de informações *online*. É por meio das redes sociais que a empresa saberá informações urgentes e importantes que são divulgadas acerca das opiniões dos consumidores sobre o atendimento da empresa, mercadoria, serviço prestado e etc.

A rápida velocidade que a rede social trafega a informação tornando acessível a todos os usuários em todas as partes do globo terrestre, ampliando a exposição dos produtos e serviços das organizações em escala mundial, ela possui uma ausência de monitoramento e controle das informações veiculadas, acarretando inconveniências desastrosas às empresas, tendo em vista que a imagem da organização pode desmoronar no ritmo em que se desenrola a comunicação no ambiente virtual.

O que no passado estava restrito a uma área específica devido aos limites geográficos, agora as informações, com a evolução tecnológica, podem transcender fronteiras e alcançar o mundo todo, pois são transmitidas via *web* em tempo real. Portanto, a divulgação de informações negativas a respeito da empresa na rede social pode causar conseqüências degradantes à imagem empresarial.

Sendo assim, cabe às empresas promoverem a concentração na proteção de bens ativos, no que se refere à reputação da organização perante a sociedade. Devem

constantemente se ocupar em manter atualizado o status social, bem como devem permanecer atentas aos dados divulgados acerca dos produtos e serviços que oferece que estão circulando na rede.

2.9 O GOVERNO E A UTILIZAÇÃO DE DADOS:

O governo utiliza tanto essas bases de dados das empresas que despertou a atenção dos pesquisadores do Projeto Privacidade, por saberem que esses dados podem ser usados de forma arbitrária, pois somente o *Google e o Facebook* são que decidem se vão liberar uma informação pertencente a um usuário e que foi pedida pela justiça, e eles tendem a analisar cada pedido separadamente. Por essa razão, gestores de todo o mundo criaram regras e leis a serem seguidas, para a proteção de dados, bem como a liberação dos mesmos, quando solicitados por meios jurídicos.

Na investigação policial deve-se agregar o uso de fontes abertas para dar uma maior celeridade ao procedimento investigativo, possibilitando ao investigador respostas rápidas e precisas, pois a polícia não deve ficar adstrita a depoimentos e exames periciais, conforme previsto no Código de Processo Penal.

Imediatamente às informações disponíveis em determinada aplicação de internet, não há necessidade de burocratizar a busca por meio de expedição de um ofício que, em algumas situações, levaria bastante tempo para se ter uma resposta. É o caso, por exemplo, da expedição de um documento para saber se o investigado recebe o benefício da bolsa família ou se é servidor de ente da federação. Logo de início haveria a dúvida para saber a quem enviar, como solicitar e quanto tempo demoraria a resposta. Para essas duas situações basta à simples consulta, no primeiro caso, ao Portal da Transparência do Governo Federal, e no segundo caso, dentro da relação de servidores do ente em que está vinculado.

Ao consultar determinada informação na internet, o investigador deve levar em conta alguns aspectos, dentre os quais a *qualidade* e a *relevância* da informação. A Internet é "território livre", onde as pessoas postam ou escrevem assuntos que podem não ser verdadeiros e não devem ser levados em conta nessa coleta. Deve, para tanto, saber distinguir informação de boato.

A fim de que a informação coletada seja útil à investigação o policial deve:

- ✓ Filtrar conteúdo: precisão no termo a ser pesquisado, busca clara e precisa. Essa coleta feita corretamente auxilia na análise posterior apenas do conteúdo que realmente possa ser relevante para uma investigação;

- ✓ Utilizar de forma correta o motor de busca e da aplicação de internet: o uso de buscadores conhecidos a fim de que se obtenham resultados mais precisos. Deve levar em conta a aplicação de internet a ser utilizada, com informações sobre quem hospeda o conteúdo, referências sobre a página além do respectivo domínio (.gov, .com., .edu, .net etc.);
- ✓ Criar de alertas: os serviços mais conhecidos são o *Google Alerts* e o *TalkWalker Alertas.* Eles possibilitam que a busca por determinado termo e seu envio diretamente para o email de quem solicitou a busca. Não há necessidade, portanto, de que se faça a busca todos os dias. O princípio a ser seguido é deixar a internet trabalhar para você. Há casos conhecidos em que policiais colocam nomes de foragidos nos serviços de alertas e tem conseguido cumprir mandados de prisão em outros estados da federação face às notícias veiculadas em portais.
- ✓ Relatório de Missão Policial: a coleta de dados em fontes abertas deve ser formalizada através de relatório de missão policial. Para tanto, o investigador deverá fazer o relato do conteúdo pesquisado, metodologia utilizada, data e hora da coleta e referências utilizadas com os *links* nos quais os conteúdos se encontram disponíveis.

2.10 OBJETIVOS DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA (OISP):

Orientar estrategicamente a produção do conhecimento no SEISP (Sistema Estadual de Inteligência de Segurança Pública) é o Objetivo de Inteligência de Segurança Pública.

São alguns exemplos de possíveis OISP (utilizaremos o Estado do Rio de Janeiro):

a) avaliar a potencialidade das organizações criminosas (ORCRIM) no Estado do Rio de Janeiro;

b) acompanhar as condições do Sistema Penitenciário do Estado do Rio de Janeiro;

c) analisar as condições gerais de Segurança Orgânica no âmbito do Poder Executivo Estadual;

O Repertório de Conhecimentos Necessários (RCN) é o desdobramento dos OISP. Pode ter uma abrangência geral, tratando de todo o Sistema Estadual de Inteligência de Segurança Pública, mas fundamentalmente deve explicitar as necessidades de conhecimentos para cada órgão do Sistema. Como os Objetivos, o RCN deve pautar a Inteligência e a Contra-inteligência, nos campos interno e externo.

Para uma melhor compreensão, observe-se o OISP contido no tópico anterior: “avaliar a potencialidade das organizações criminosas (ORCRIM) no Estado do Rio de Janeiro”. Tem-se como um possível exemplo de RCN derivado desse objetivo:

a) identificar as ORCRIM que atuam no estado;

b) analisar o *modus operandi* das ORCRIM;

c) conhecer a estrutura organizacional de cada uma delas;

d) avaliar a influência sobre a população carcerária;

e) acompanhar a dinâmica entre facções aliadas e contrárias;

O Plano de Inteligência deve propiciar as condições necessárias para que se estabeleça um Fluxo de Conhecimentos adequado a propiciar efetividade ao Sistema de Inteligência. Os membros integrantes ao sistema devem produzir os conhecimentos determinados no RCN, transmitindo-os de maneira a gerar um Fluxo de Conhecimentos que proporcione o atendimento dos Objetivos de Inteligência, subsidiando os decisórios apropriadamente.

É interessante que exista uma plataforma criptográfica universal para o tratamento dos documentos que são transmitidos dentro do SEISP. A manutenção do sigilo é algo basilar à Atividade de Inteligência. Importante também é estudar no planejamento estratégico quais são os tipos de conhecimento produzidos por cada órgão, para que se determine os conteúdos que sejam de interesse, ou possam ser necessários, ao SEISP.

> A manutenção do sigilo implica, minimamente, que exista uma norma de classificação da informação e existência de mecanismos de Contra-inteligência que garantam a manutenção do sigilo dos dados e informações compartilhadas. Um instrumento fundamental na montagem desse arcabouço é a existência de estrutura de Credenciamento de Segurança e de normas de Segurança Orgânica que tenham efetividade na proteção de dados e informações sigilosas. (FARAH, 2015).

A Constituição Federal, em seu artigo 144, definiu para o âmbito estadual, a existência de duas polícias, cada uma com diferentes características:

a) Polícias Civis: são polícias judiciárias responsáveis pela apuração dos crimes estaduais, exceto os militares.

b) Polícias Militares: são polícias predominantemente administrativas, porém exercem a função de polícia judiciária na apuração dos crimes militares de sua incumbência; responsáveis pelo policiamento ostensivo e pela preservação da ordem pública.

Com atribuições bem diferentes, os próprios nomes manifestam a qual instituição se reporta: de caráter civil e militar. Embora exista essa diferença de nomenclatura, as atribuições das polícias estaduais são necessariamente complementares, e necessitam da cooperação efetiva entre as forças, para que a rivalidade não impeça a troca de informações e a coordenação das ações de enfrentamento à criminalidade. No tocante à Inteligência de

Segurança Pública, a tendência natural é de que os subsistemas de cada instituição reproduzam essa cultura.

3 CONCLUSÃO

Conclui-se que a fiscalização, tanto das redes sociais, quanto das regras e leis vigentes no país, dificultaram a burocracia anterior vivida por nós, deixando mais fácil o acesso de dados como ferramenta de investigação policial.

Nesse contexto, as OISP podem utilizar de perfis, fotos, acesso a comunidades e obter dados verídicos de possível criminoso. O acesso a redes sociais já facilitou a prisão e condenação de criminosos ditos como foragidos, que foram localizados em outro estado, graças as redes sociais, e a um delegado que fez uso dessa ferramenta e divulgou a imagem do cidadão, que por fim, teve seu objetivo atingido.

Em se tratando do marketing pessoal que fazem toda nossa sociedade, as redes favorecem de fato essa propaganda em diversos campos de atividades, tanto como para um emprego como para relacionamento amoroso. O que foi pesquisado e concluído é de que se devem orientar melhor os usuários das redes, pois nem todas as postagens podem lhe fazer bem, ao mesmo tempo em que poderá trazer aborrecimentos, também pode ter atividades de cunho vexatório, e alguns casos relatados de homicídios entre internautas. Tudo que é feito sem responsabilidade pode acarretar problemas inenarráveis. Concluiu-se também que ferramentas gratuitas como *Google, Google Maps, Street view, Instagram* e *Facebook* são fundamentais na busca de dados, a fim de perceber realidades fundamentais em determinados planejamentos operacionais.

As conhecidas nuvens podem ser um alívio para muitos, pois você pode acessar documentos e fotos de onde estiver mesmo sem estarem portando um pen drive ou outra forma de armazenamento de dado físico. É tudo virtual, e nunca mais ocorrerá à perda de dados por um defeito do aparelho de armazenamento, pois está na nuvem, porém ela pode ser *hackeada* também e acabar sendo fonte de horror para alguns desavisados. Como no casão da atriz que tirou fotos nuas para o namorado pelo celular, os arquivos foram parar na nuvem, ela apagou de seu aparelho, mas um *hacker* conseguir driblar a rede e obter as imagens. Claro que vendeu as fotos à imprensa que postou sem nenhum problema. Conclui-se que a nuvem é como todo o contexto do trabalho é importante, porém obtém um número de riscos que devem ser observados pelos usuários.

Conforme a lei e normas, os dados que podem ter livre acesso deveriam ser aqueles que não são tão pessoais, como fotos, festas, relatos simples. Os dados que contém numeração de documentos, senhas importantes, dentre outros só são compartilhados na rede de duas formas: ou a justiça solicitou, ou o usuário postou. Esse último é o mais preocupante, pois

depois que os dados caem na rede, jamais somem e sempre ficam "*cookies*" desse arquivo em alguma nuvem.

A segurança já á tempos vêem usando algumas dessas redes como base para investigações. Agora com o beneficiamento da lei, fica mais livre esse acesso para pesquisa investigativa.

No caso das operações das Forças Armadas nas ações do Plano de Segurança Pública para o Estado do Rio de Janeiro, é de grande relevância esse estudo mais aprofundado pela segurança nacional. Não é surpresa assistirmos em jornais televisivos sobre como os criminosos não possuem parâmetros em suas divulgações. São fotos de crianças portando armas, de traficantes com fuzis, vídeos de presidiária dando festinha em presídio regado a bandejas de maconha e cocaína para as colegas do presídio, dentre outras notícias que já circularam pela TV e que demonstra a fragilidade das estruturas de fiscalização tanto nos presídios, como das redes sociais. O uso desses dados teria teor punitivo hoje pela regulamentação do acesso as inteligências de fontes de dados.

Da mesma forma que as fontes de dados abertas serem de tudo positivas para todos os setores que fizerem um bom uso delas, é evidente que a despeito das vantagens citadas, o ambiente virtual mostra-se um cenário propício à prática de diversos atos ilícitos, no que se refere aos danos extra-patrimoniais e patrimoniais. Nesse sentido, haja vista os riscos evidentes, parte da doutrina e jurisprudência têm entendido que as redes sociais respondem objetivamente pelos danos causados por seus usuários.

Investigaram-se as aplicações dos dados pessoais, e se conclui que seus usos são variados, quais sejam: utilidade comercial, em campanhas políticas, são manuseados para fins de vigilância de governos e também para a governança eletrônica, e como tal, dentro dos limites legais, pode ser utilizada para o planejamento de operações militares no estado do Rio de Janeiro ou outros estados.

Considerando as publicações de Política Nacional de Inteligência, em 2016, e a de Estratégia Nacional de Inteligência, em 2017, vive-se um momento chave para a Atividade de Inteligência no Brasil. Os Estados da Federação precisam estar alinhados a este movimento. Portanto, a elaboração de Planos Estaduais de Inteligência de Segurança Pública é uma forma determinante para o fortalecimento dos Sistemas Estaduais de Inteligência de Segurança Pública, e a efetiva integração destes no Subsistema de Inteligência de Segurança Pública, de forma a contribuir, também, para o desenvolvimento de todo o Sistema Brasileiro de Inteligência.

4 REFERÊNCIAS BIBLIOGRÁFICAS

BARRETO, Alesandro Gonçalves; WENDT, Emerson. CASELLI, Guilherme. **Investigação Digital em Fontes Abertas**. BRASPORT Editora. Rio de Janeiro. 2017.

BETIM. Felipe. Jornalista | Periodista - El País, online. **Intervenção Federal no Rio de Janeiro: A história das operações e planos de segurança no Rio: três décadas de fracassos.** Acessado em 23 de agosto de 2018. Disponível em:https://brasil.elpais.com/brasil/2018/02/19/politica/1519058632_353673.html.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em 24 de agosto de 2018.

_____. Lei 12.735, de 30 de novembro de 2012. **Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providência**s. Acesso em 24 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>.

_____. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 25 de agosto de 2018.

_____. Ministério da Defesa. Exército Brasileiro. **Operações. 4ª Ed - EB20-MF-10.103**. Brasília: Estado Maior do Exército, 2014.

_____. Ministério da Defesa. Exército Brasileiro. **Instruções Provisórias - IP 31 21 - Operações de Forças Especiais**. Brasília: Estado Maior do Exército, 1991.

_____. Comando da 2ª Brigada de Cavalaria Mecanizada. **Reunião de Coordenação da OperaçãoHermandad 2015**. Disponível em http://www.2bdacmec.eb.mil.br/index.php/noticias/141-2-reuniao-de-coordenacao-daoperacao-hermandad. Acesso em 24 de agosto de 2018.

_____. Centro de Doutrina do Exército (C Dout Ex). **Operações de Paz**. Brasília: C Dout Ex, 2015b. Disponível em http://www.eb.mil.br/missoes-de-paz/-/asset_publisher/xbkIlDCFFYVl/content/apresentação Acesso em 24 de agosto de 2018.

_____. Ministério da Defesa. Exército Brasileiro. Centro de Doutrina do Estado Maior do Exército. **Nota de Coordenação Doutrinária Nr 02/2012 – C Dout** Ex. Brasília: Estado Maior do Exército, 2012a.

CERT.br. **Cartilha de Segurança para Inte**rnet. Comitê Gestor da Internet no Brasil, São Paulo, 2006.

EUROPÉIA. Parlamento Europeu e o Conselho da União,.**Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679. Acesso em 25 de agosto de 2018.

FARAH Camel André de Godoy. **Auditoria na atividade de Inteligência**. Palhoça: UnisulVirtual, 2015.

HAUSER. Kathryn;. WBZ-TV.BOSTON (CBS).**Real-Life 'Scorpion' ajudou ID suspeitos de bombardeio de maratona de Boston.** De 6 de outubro de 2014, 23h20Disponível em: https://boston.cbslocal.com/2014/10/06/real-life-scorpion-helped-id-boston-marathon-bombing-suspects/. Acesso em 25 de agosto de 2018.

KAHN, David. (1995). "**Toward a Theory of Intelligence**". In: Military History Quarterly, vol. 07 # 02, (winter 1995).

KENT, Sherman. **Strategic Intelligence for American World Policy**. Princeton, New Jersey: Princeton University Press, 1966.

MEDEIROS, Luciana Maria. **Evolução histórica do Direito Comercial. Da comercialidade à empresarialidade**. **Jus Navigandi,** Teresina, ano 16, jan. 2011. Disponível em: http://jus.com.br/artigos/18219. Acessado em 24 de agosto de 2018.

NACIONAL. Congresso,. (LGPD, 2018). **Dispõe sobre a proteção de dados pessoais e alteraa Leinº 12.965**, de 23 de abril de 2014. Acesso em 23 de agosto de 2018. Disponível em: http://www.migalhas.com.br/arquivos/2018/7/art20180710-04.pdf.

NOVAES, Antonio Galvão. **Logística e gerenciamento da cadeia de distribuição: estratégia, operação e avaliação**. 3. ed. Rio de Janeiro: Elsevier, 2007.

O'TOOLE, George J. A. (1990). "**Kahn's Law: A Universal Principle of Intelligence?**". In: International Journal of Intelligence and Counterintelligence, vol. 04 # 01 (spring 1990).

SOPHOS. (2010). "**Security Threat Report: 2010**". Acessado em 25 de agosto de 2018. Disponível em: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf.

SHULSKY. Abram N., SCHMITT, Gary James. (1992). **Warfare Silent.** Potomac Books Inc. Washington DC.

UGARTE, David (2007): **O poder das redes** (em português). Ed. El Cobre.