

KAIQUE RODRIGUES DA SILVA¹, RUBENS ALVES DA SILVA²

¹Acadêmico de Graduação em Direito pelo o Instituto Nacional de Ensino Superior e Pós-Graduação do Centro Universitário Luterano de Manaus - CEULM/ULBRA, Manaus-AM. E-mail: krds.kaique@gmail.com. ²Mestre em Direito pelo o Instituto Nacional de Ensino Superior e Pós-Graduação da Faculdade de Direito do Sul de Minas – FDSM/MG, Pós-Graduação em Processo Judiciário pela FIC/SERGIPE, Pós-Graduação em Docência e Gestão em Ensino Superior pela Universidade Estácio do Amazonas, Professor do Curso de Direito do Centro Universitário Luterano de Manaus - CEULM/ULBRA.

RESUMO

Este Artigo versa sobre um dos maiores desafios da Polícia no momento que são as investigações de crimes em ambiente virtual. A ideia básica é buscar analisar novas ferramentas de investigação como encargos do ônus da prova no levantamento de informações substanciais para que o crime cibernético possa ser combatido de forma efetiva.

Palavras-chave: Investigações; Crimes Cibernéticos; Ônus da Prova.

CRIMES CIBERNÉTICOS: NECESSIDADE DE NOVAS FERRAMENTAS DE INVESTIGAÇÃO COM ENCARGOS NO ÔNUS DA PROVA

INTRODUÇÃO

O advento da informação indica claramente novos rumos para os processos organizativos da sociedade, principalmente no contato diário e cotidiano entre as organizações e seus públicos, além das relações sociais. Neste contexto, este ambiente se tornou propício para a execução de crimes, denominados de crimes virtuais e/ou cibernéticos.

Assim, nesta fase atual da sociedade humana, novas metodologias de investigações despontam para ocupar o espaço já superado de antigos métodos

investigativos, justamente com o intuito de acompanhar a evolução natural das formas do agir criminal. A polícia nasceu juntamente com o conceito de Estado e de justiça. O Estado se constituiu a partir da efetivação de normas de conduta impostas às sociedades. As normas nasceram com os agrupamentos humanos e sua institucionalização criou o Estado com a extrema necessidade de se fazer justiça para quem não cumprisse as normas.

Com o passar do tempo importantes mudanças ocorreram na forma de investigação policial, em decorrência do próprio avanço nos sistemas de informação. No contexto dessa evolução, surgiram sistemas de informação que agilizam e colocam a Polícia muito perto de desvendar com maior celeridade esses crimes.

A ideia básica foi buscar analisar a necessidade de novas ferramentas de investigação com encargos no ônus da prova no levantamento de informações para a formatação de um inventário de interesses que sirva como base para a elucidação de crimes virtuais e/ou cibernéticos.

1. Origem histórica

No início a polícia era diretamente ligada ao exército, pois esse incorporava o conceito de segurança interna e externa. Mas diante a especificidade da atividade policial, esse desprendimento era absolutamente natural e necessário.

De acordo com Colares (2009, p. 33):

“Logo os exércitos passaram a ter enorme dificuldade de se concentrar em duas atividades: a policial e a de segurança externa, até em função das guerras que eram muito intensas e obrigavam os exércitos a terem que usar todo o seu contingente na atividade de segurança externa, o que dificultava as atividades de segurança interna”.

Assim nasceu a polícia como se conhece hoje. Na Grécia, berço da democracia, o poder judiciário utiliza escravos na função de polícia, mas o trabalho de investigação de crimes era realizado pelos próprios cidadãos. (GONÇALVES, 2013).

Desta forma, ficou claro para o Estado que a função policial era necessária e fundamental, além da individualização da mesma. Com isso, a função de segurança

interna, passou ganhar contornos de muita importância por ser um primeiro passo para incrementar ações para todos aqueles que não cumpriam as normas jurídicas (COLARES, 2009).

2. Evolução da atividade policial

Com o passar dos tempos, a atividade policial foi se ampliando, passando a incorporar cada vez mais as atividades de inteligência. Atualmente todas as corporações policiais possui em sua estrutura hierárquica um setor de Inteligência Policial que desenvolve ações de combate ao crime, sendo necessário que o trabalho informativo seja um adendo a mais no levantamento sistemático de informações que servirão de base para a formatação de um protocolo de intenções e um inventário de interesses que possa servir de modelo para investigações na área virtual ou cibernética (DIAS, 2010).

O argumento exposto possuiu o caráter claro de reiterar as análises críticas e prospectivas sobre a questão do combate ao crime virtual e/ou cibernético e sua intrínseca relação com a dinâmica da segurança pública, meio do monitoramento dos sistemas de informação de forma geral, redes sociais etc. As tendências desta contínua mudança nesse tipo de tecnologia permitiram identificar novas ferramentas de inteligência para subsidiar as decisões policiais e jurídicas (COURI, 2009).

Os recursos de informática continuam sendo explorados de todas as formas, pois o computador tornou-se uma ferramenta cotidiana na vida das pessoas, porém muita das vezes está sendo utilizada de forma equivocada. Agora com os aparelhos celulares que se transformaram rapidamente em instrumentos de sistemas de informação, são muito utilizados também para que se cometam crimes (ANGELUCI, 2017).

3. Modelos de inteligências bem-sucedidos e a incorporação no âmbito estatal

Nos Estados Unidos, o Federal Bureau of Investigation – FBI utiliza a inteligência policial para formatar provas irrefutáveis contra criminosos de todas as espécies. Um exemplo famoso é o caso do Agente Federal Joseph D. Pistone que se infiltrou, nos anos de 1970, na Máfia Americana como o nome fictício de Donnie Brasco e, lá permaneceu por cerca de cinco (5) anos, levantando informações que no futuro foram

decisivas para o aniquilamento da máfia nos Estados Unidos. Na França a polícia de inteligência que hoje adquiriu contexto internacional – é a Organização Internacional de Polícia Criminal – INTERPOL que exercita a atividade de inteligência policial em várias frentes de crimes e cujo caso mais famoso foi à descoberta de um possível atentado contra o então presidente francês Charles de Gaulle em 1962, que culminou com a intervenção da referida instituição com a morte do terrorista. (COLARES, 2009).

Mas atividade de inteligência no âmbito estatal não só se refere à atividade da polícia em si, pois também se ampliou para o âmbito da segurança nacional e se tornou inteligência governamental. Segundo CEPIK (2003, p. 1):

“A atividade de inteligência é essencial ao desenvolvimento e à preservação do Estado Democrático de Direito.”

Todos os países economicamente desenvolvidos, com democracia consolidadas, possuem serviços de inteligência responsáveis, legais e fortes. Mas no caso deste trabalho, embora possam surgir alguns pontos em um caso ou outro, só interessa a inteligência policial, ou seja, o processo de sintetizar informações provindas de fontes de informações (abertas e fechadas) que fundamentam o processo decisório (CEPIK, 2003).

4. Coleta de informações

O trabalho policial está relacionado à prevenção, repressão e controle da violência. Evidentemente, a população necessita e espera que a polícia previna e desvende o crime e preserve a ordem pública. Isto exige uma mudança gradativa, nos procedimentos adotado, saindo de um sistema fechado e indo para um sistema aberto na área policial, com prioridade na organização e em certo ponto até mesmo na extinção da abundância de níveis funcionais na sua estrutura (GONÇALVES, 2013).

É preciso criar uma proximidade e entendimento mútuo entre a população e a organização, partindo da premissa fundamental de que a responsabilidade pela segurança pública não é só da polícia, mas compartilhada entre o Estado e seus cidadãos. Assim, a crescente insatisfação experimentada pela sociedade ocasiona a mudança das organizações policiais. Aos poucos, por toda parte, observa-se a adoção em caráter experimental de estruturas descentralizadas e menos burocratizadas de aplicação da lei com novos conceitos de polícia como este. Neste sentido, os

departamentos de inteligência policial nasceram com a necessidade de se obter e guardar informações pertinentes aos crimes e usá-las como forma de prova contra seus autores. Sobre esse contexto, CEPIK (2003, p. 29) afirma que:

“Inteligência lida com o estudo do "outro" e procura elucidar situações nas quais as informações mais relevantes são potencialmente manipuladas ou escondidas, em que há um esforço organizado por parte de um adversário para desinformar, tornar turvo o entendimento e negar conhecimento”.

Como se pode observar, o trabalho da inteligência policial é levantar o maior número de informações pertinentes para usar como prova contra a quem comete o delito, que por sua vez procura, em sentido contrário evitar que essas informações sejam trabalhadas e usadas como prova contra si (CEPIK, 2013).

É um trabalho de levantamento de informações contundentes justamente por ser percebida que a informação é a matéria-prima mais valiosa. A informação é fator-chave do trabalho policial, principalmente nos tempos atuais, denominados de “Era da Informação”. Neste sentido, o importante é dispor de informações seguras que embasem o processo de levantamento de provas. Então o trabalho policial se torna um elemento balizador do levantamento de provas, fornecendo uma visão cristalina da prática delituosa, em função das informações possibilitarem a formação de um retrato fiel da situação (CEPIK, 2013).

5. Empecilhos no mundo virtual para obtenção do ônus da prova

O levantamento de informações parte de uma situação geral para uma situação particular, ou seja, deve-se partir de uma situação geral (todos são cumpridores da lei) para se identificar se alguém não a cumpriu em determinado espaço de tempo usando as ferramentas de controle, como a verificação de atividades suspeitas por parte dos provedores de internet, ou ainda em casos de crimes financeiros no âmbito virtual o uso de informações de movimentações bancárias atípicas. Para isso os órgãos de investigação precisam manter uma relação bem amistosa com essas instituições. E para isso se faz necessário a resguarda de determinadas especificidades que não podem ser burladas (ROESCH, 2014).

Assim caso alguma coisa aconteça no âmbito virtual que vá de encontro às políticas de gestão das empresas provedores de internet ou ainda de outras empresas se faz necessário que esta identificação seja imediatamente comunicada aos órgãos de investigação criminal. Assim deve estar bem inscrito nas relações entre empresas de informática e telecomunicações alguns requisitos como: não possuir nenhum tipo de conduta inadequada; (i) ter comportamento civil correto de acordo com as normas sociais deflagradas. Como comprovar isso? Somente com o controle diário dos acessos devidos e indevidos (caso de sites pornográficos). O processo de investigação de crime virtual e/ou cibernético é mais amplo do que simplesmente cadastrar alguém. Alguns dados são sigilosos como garantia constitucional, como, por exemplo, os dados bancários, que para serem comprovados, devem seguir um regime jurídico, ou seja, necessita-se de uma autorização judicial.

O crime virtual e/ou cibernético é um crime de muito difícil prevenção, que produz enormes dificuldades de ser investigado, de perseguição bem complicada, cuja comprovação é bastante difícil e a punição quase impossível, até por conta da ausência de legislação mais específica (DIAS, 2010).

Dentre os problemas para investigar essa tipologia de crime está certamente à ausência de uma legislação adequada e a completa ausência de um método mais específico no tratamento das condicionalidades deste crime, dentre elas a completa ausência de compartilhamento informações entre as instituições, principalmente as empresas que trabalham especificamente com os sistemas de informação (empresas de informática - provedoras). Tudo isso dificulta a ação célere dos órgãos de investigação (DIAS, 2010).

Também não se esquecer de que criminosos virtuais nem sempre atuam nos seus locais de origem, o que dificulta muito as ações de órgãos de investigação. São criminosos transacionais e nem sempre onde ocorre o crime é o local de origem do criminoso. Assim, se faz necessário que o investigador desse tipo de crime tenha profundo conhecimento de Tecnologia da Informação (TI) e possa a partir desse conhecimento identificar a origem da comunicação, que no ambiente de TI se refere a identificar o Internet Protocol (IP) e a quem este está vinculado e isso só é possível que exista uma parceria entre o órgão de investigação e as empresas responsáveis pelo controle do IP. Os crimes virtuais são muito próprios e os criminosos sempre

tentam esconder suas ações com uso de programas que geram dúvidas como o programa troyano, sendo necessário um procedimento de identificação bem aprazível que não gere dúvidas (DIAS, 2010).

Assim a investigação tem que produzir provas que possam ser aceitas em julgamento, por ser esta o fator-chave para o trabalho do magistrado. Assim uma decisão judicial leva em consideração o elemento probatório. Nos tempos atuais, denominados de era da informação, estas são imprescindíveis para que o trabalho do juiz seja eficiente no processo de tomada de decisão. Decidir com exatidão virou sinônimo de decidir com todas as informações disponíveis e o elemento probatório é o principal deles (ANGELUCI, 2017).

O trabalho de levantamento de informações que se constituirão em prova é o subsídio que mantém a quem de direito bem informado, por que busca informações de forma sistemática para produzir conhecimento. Os conhecimentos mais importantes sobre o trabalho do juiz estão relacionados ao fato de se aprofundar no estudo como forma de contribuir para a melhoria e estabelecer um processo decisório coerente (DEL-CAMPO, 2018).

Assim, alguns sistemas de segurança estão criando metodologias próprias para investigar os crimes virtuais e/ou cibernéticos. No caso da União Europeia eles estabeleceram uma metodologia centrada em 5 pilares básicos: Preparação e prevenção, Detecção e resposta; Mitigação e recuperação; Cooperação internacional; e, por fim, estabelecer critérios para a Tecnologias da Informação e Comunicação (TIC) (COURI, 2009).

No caso da preparação e prevenção esta está centrada na informação, ou seja, estabelecer sistemas de informação concentrada na maior difusão possível das possibilidades e os métodos utilizados pelos criminosos. Faz parte disso uma campanha intensa de conscientização da população no sentido de prover o máximo de informações possíveis. No caso da Detecção e resposta, esta, busca apoio na multidisciplinaridade, ou seja, a investigação tem que ser um trabalho em equipe e das renovadas estratégias da pesquisa científica com base nos pressupostos filosóficos admitidos; o objeto a investigar; a metodologia da investigação; e, a linguagem técnica a ser utilizada, destacando em cada um deles, os principais atributos a serem considerados (DIAS, 2010).

Na questão da mitigação e recuperação envolve a formação de recursos adequados aos profissionais, ou seja, o profissional tem que ser preparado dentro da especificidade necessária para investigar o crime além de contar com os recursos tecnológicos necessários para tal intento (DIAS, 2010).

No caso da cooperação internacional se faz necessário a formatação de um inventário de interesses entre as nações. Ainda de acordo com Saylor e Alexander (2014, p. 33):

“A primeira característica diz que um plano deve estar baseado no conhecimento e interesses daqueles que serão atingidos positivamente ou negativamente por ele; o segundo diz que o plano deve ser caracterizado por uma alta flexibilidade. Faz-se previsões para modificações no plano para igualarem-se às necessidades e interesses dos envolvidos com muitas opções válidas para eles”.

Segundo Silva (2010, p. 14), “a legislação penal contra crimes virtuais e/ou cibernéticos representa hoje um espaço de marco regulatório essencial”, que surgiu da necessidade de se desencadear um processo de reflexão do ser humano para com o próprio ser humano e deste com o sistema de informação por intermédio de uma normatização, suas interações frente às questões socioeconômicas e culturais, situando-o na natureza por se tratar de um ser biossocial. Entretanto, não refere a uma forma específica de normas, e sim, de um processo contínuo de uma filosofia normativa, onde todos: Estados e sociedade civil devem estar engajados.

Portanto, a legislação contra crimes em ambiente virtual leva à mudança de mentalidade e faz com que as pessoas se comportem de maneira responsável, com sensibilidade para não atacar outras pessoas e/ou instituições e, saibam exigir e respeitar os seus próprios direitos e de toda a comunidade, modificando-se interiormente e interagindo de maneira correta com o ambiente virtual. (Nascimento e Silva, 2012, p. 113).

CONSIDERAÇÕES FINAIS

O comportamento sociocultural ilibado é a causa, condição e o fundamento para o exercício do comportamento das pessoas em ambiente virtual. Desta forma, o

trabalho operacional da investigação desta tipologia de crimes é primordial ao desenvolvimento da atividade policial nesta área como um todo.

A investigação como metodologia indispensável no trabalho do magistrado, justamente por ser o método que vai buscar as especificações de comportamento como uma forma que garanta o caráter ilibado do processo decisório, condição “si nem qua non” para a atividade do juiz.

Em níveis mais elevados estão sendo cada vez mais incluídas descrições comportamentalistas, que buscam descrever os atos ostensivos das pessoas ao invés dos traços que causam ou se acham subjacentes a seus atos. Desse modo se torna mais acessível à tentativa para resoluções de crimes Cibernéticos.

REFERÊNCIAS

1. ANGELUCI, R. A.; SILVA, E. A. da.; SANTOS, C. A. de A. C. Sociedade da Informação: O mundo virtual Second Life e os Crimes Cibernéticos. Artigo, 2017. Disponível em http://www.oabsp.org.br/comissoes2010/gestoes-anteriores/direito-eletronico-crimes-alta-tecnologia/artigos/2010-2012/SL_lccbyer_final0311.pdf Acesso em 12 de agosto de 2019.
2. BORGES, S. da C. Polícia e constituição. São Paulo: RT, 2005.
3. CEPIK, M. A. C. Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV, 2003.
4. COLARES, M. De S. Polícia: história da instituição de segurança pública. São Paulo: RT, 2009.
5. COURI, G. F. Crimes pela Internet. Artigo, 2009. Disponível em http://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2009/trabalhos_22009/GustavoFuscaldoCouri.pdf Acesso em 12 de ago de 2009.

6. DEL-CAMPO, E. R. A. Exame e levantamento técnico pericial de locais de interesse a justiça criminal: abordagem descritiva e crítica. Dissertação de mestrado. São Paulo: USP, 2008.
7. DIAS, V. E. A problemática da investigação do cibercrime. UNIVERSIDADE DE LISBOA FACULDADE DE DIREITO/IDPCC I CURSO PÓS-GRADUAÇÃO DE APERFEIÇOAMENTO EM DIREITO DA INVESTIGAÇÃO CRIMINAL E DA PROVA. LISBOA, NOVEMBRO DE 2010. Disponível em http://www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf Acesso em 12 de ago de 2019.
8. GONÇALVES, J. B. Atividade de inteligência e legislação correlata. Niterói-RJ: Impetus, 2013.
9. NASCIMENTO E SILVA, Geraldo Eulálio do. O direito ambiental internacional. RF 317/135. Rio de Janeiro, Forense, 2012.
10. ROCHA, G. de M. O método de investigação criminal. São Paulo: Cutrix, 2007.
11. ROESCH, S. Projetos de estágio e de pesquisa em administração. 4ª ed. São Paulo: Atlas, 2014.
12. SAYLOR, J. G & ALEXANDER, W. Planificação social com base em interesses. 3ª ed. São Paulo: Cortez, 2014.
13. SILVA, Gilmaro Geraldino da, à inconstitucionalidade da prova ex officio no processo penal brasileiro: a imparcialidade do juiz. Monografia apresentada ao curso de Direito da Universidade Estadual da Paraíba - UEPB como um dos requisitos básicos para a obtenção do grau de bacharel em Direito pela Universidade Estadual da Paraíba. Campina Grande: Universidade Estadual da Paraíba, 2010. Disponível em: <http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/5750/1/PDF%20-0Gilmaro%20Geraldino%20da%20Silva.pdf>. Acesso em 10 de agosto de 2019.