Perícia de Tecnologia da Informação e Comunicação e de Crimes Cibernéticos no MPF

Por

Marcelo Beltrão Caiado

Trabalho de Conclusão de Curso apresentado ao
Curso Intensivo de Pós-Graduação em Administração Pública
Pós-Graduação *latu sensu,* Nível de Especialização
Programa FGV in company

Julho/2016

Página de Aprovação

FUNDAÇÃO GETÚLIO VARGAS
PROGRAMA FGV IN COMPANY
Curso Intensivo de Pós-Graduação em Administração Pública

O Trabalho de Conclusão de Curso
Perícia de Tecnologia da Informação e Comunicação e de Crimes Cibernéticos no MPF

elaborado por Marcelo Beltrão Caiado

e aprovado pela Coordenação Acadêmica do **Curso Intensivo de Pós-Graduação em Administração Pública**, foi aceito como requisito parcial para a obtenção do certificado de curso de pós-graduação, nível especialização, do Programa FGV IN COMPANY

Data:

_____
Armando Santos Moreira da Cunha

_____
Roberto Bevilacqua Otero

Termo de Compromisso

O aluno Marcelo Beltrão Caiado, abaixo-assinado, do Curso Intensivo de Pós-Graduação em Administração Pública, do Programa FGV *In Company*, realizado nas dependências da FGV de Brasília, no período de setembro de 2014 a junho de 2016, declara que o conteúdo do trabalho de conclusão de curso intitulado: Perícia de Tecnologia da Informação e Comunicação e de Crimes Cibernéticos no MPF, é autêntico, original, e de sua autoria exclusiva.

Brasília, 01 de julho de 2016.

MARCELO BELTRÃO CAIADO

Perícia de Tecnologia da Informação e Comunicação e de Crimes Cibernéticos no MPF

Projeto de Pesquisa apresentado à Fundação Getúlio Vargas, como requisito parcial para a aprovação na disciplina Introdução ao Trabalho Científico do Curso Intensivo de Pós-Graduação em Administração Pública.

Brasília
2016

Sumário

1 Introdução....6
1.1 Contextualização....6
1.2 Objetivo....8
1.2.1 Objetivo final....8
1.2.2 Objetivos Intermediários....8
1.3 Relevância do Estudo....8
2 Revisão de Literatura....8
2.1 Crimes de informática....11
3 Metodologia....16
3.1 Tipo de Pesquisa....16
3.2 Universo e Amostra....16
3.3 Coleta de Dados....17
3.4 Análise dos Dados....17
4 Perícias no MPF....17
4.1 Perícias de TIC....18
4.2 Perícias de Crimes Cibernéticos....19
5 Conclusões....21
6 Referências Bibliográficas....22

1 Introdução

1.1 Contextualização

A perícia de Tecnologia da Informação e Comunicação (TIC) e de Crimes Cibernéticos tem sido bastante demandada de órgãos da lei nos últimos anos, em função da migração de diversas atividades criminosas do mundo real para o mundo virtual, somado ao fato do surgimento de novas modalidades de crimes proporcionadas pela Internet e tecnologias computacionais.

Segundo dados fornecidos pelo Perito Criminal Federal McDonald Parris, no Curso de Técnicas Investigativas nos Crimes Cibernéticos promovido pela Procuradoria da República em São Paulo (PR/SP) realizado em outubro de 2015, a quantidade de peritos na área de informática da Polícia Federal era de aproximadamente 230 (duzentos e trinta), número esse considerado insuficiente para as demandas atuais.

No âmbito do Ministério Público Federal (MPF), o quantitativo de peritos de TIC é praticamente irrisório, não obstante a importância da área pericial. Tal área foi bem destacada inclusive durante o trabalho de modernização desenvolvido pela FGV e pela PwC no órgão, e devidamente ilustrada na estrutura de processos internos, no Mapa Estratégico do Ministério Público Federal[1]:

Figura 1: Mapa estratégico do Ministério Público Federal

1 Disponível para download em http://www.modernizacao.mpf.mp.br/pei-2011-2020/pei_2011_2020

Inclusive, o relatório de diagnóstico da Fundação Getúlio Vargas, do projeto de Modernização da Gestão Administrativa do MPF, menciona a necessidade de expansão específica no quadro de peritos na área de informática, como se observa à página 119:

> "Em relação ao número de servidores (quantidade), muito se observou a questão do déficit de modo geral. Como principais desafios surgiram a necessidade de se alcançar uma distribuição adequada de recursos humanos, a ampliação o quadro tanto em relação à atividade meio quanto à atividade fim, inclusive nas PRM, a ampliação do quadro de peritos ou convênios (contabilidade, meio ambiente e informática) e busca pela redução do turnover (servidores)."

Além disso, a importância também é constatada nas diversas perícias realizadas, em que se destacam aquelas com suposto superfaturamento na aquisição de equipamentos e sistemas de informática, e as perícias de pornografia infantojuvenil e de processos administrativos disciplinares.

Contudo, poucos investimentos em recursos humanos, capacitação e equipamentos específicos vinham sendo realizados, inclusive, se observa que durante o período de 2002 a 2014 um único servidor concursado ocupava o cargo de Analista de Informática / Perito[2] em todo o MPF. Somente no ano de 2014 é que mais um servidor para o mesmo cargo entrou em exercício.

Nesse sentido, recentemente houve uma definição prática de tratar tal área com a necessária atenção com a criação da Secretaria de Apoio Pericial (SEAP), em 2015, em que foi definida a criação de uma Assessoria Temática Modular cujas atribuições seriam de uma área temática específica de TIC e de crimes cibernéticos. Até a data da finalização deste trabalho essa área ainda não havia sido criada, em função de contingenciamento e de restrições orçamentárias aplicadas ao MPU pelo Governo Federal.

O objetivo da SEAP é, conforme descrito na apresentação realizada pela Secretária da SEAP, Procuradora Regional da República Dra. Elizabeth Mitiko Kobayshi, no I Seminário de Modernização dos Gabinetes:

> "A estruturação organizacional da área pericial do MPF, otimizando a alocação dos peritos de forma nacional, aumentando a celeridade no atendimento das demandas e resguardando a qualidade do conhecimento produzido."

Pelo exposto, fica evidente a necessidade urgente de um quadro maior de peritos, amparados por uma estrutura específica, com capacitações e ferramental adequados, para tratar de temas correlatos às perícias de crimes cibernéticos de tecnologia da informação e comunicação.

---

2 Com a publicação da Portaria PGR/MPU nº 302/2013, a denominação do cargo passou a ser Analista do MPU / Perícia / Tecnologia da Informação e Comunicação

1.2 Objetivo

1.2.1 Objetivo final

Identificar as áreas de atuação de perícias de TIC e de crimes cibernéticos mais importantes para a atuação institucional do MPF, propondo alterações que propiciem melhorias e os investimentos necessários em capacitação, contratação de recursos humanos e aquisição de soluções, incluindo, se for o caso, a assinatura de convênios de cooperação.

1.2.2 Objetivos Intermediários

- Identificar problemas atuais enfrentados pelas forças da lei no combate aos crimes cibernéticos;
- Possibilitar uma melhor preparação do MPF para responder mais adequadamente a demandas futuras, as quais tendem a aumentar em função do crescimento intrínseco da adoção de novas tecnologias;
- Expor melhores práticas na gestão de perícias de TIC e de crimes cibernéticos adequadas à realidade do MPF;
- Identificar as formas mais comuns de crimes cibernéticos; e
- Identificar os tipos de serviços prestados por peritos de TIC e de crimes cibernéticos do MPF.

1.3 Relevância do Estudo

Com a disseminação e popularização das tecnologias da informação e da consumerização, observa-se um incremento nas demandas de perícias de TIC em investigações e inquéritos de crimes contra a Administração Pública, onde, em muitos casos, o perito do MPF atua na condição de assistente técnico.

Além disso, nota-se nos últimos anos um aumento significativo nos crimes cibernéticos correlatos à área de atuação do MPF, especificamente aqueles relacionados a crimes de ódio, racismo, fraudes bancárias e pornografia infantojuvenil.

Não obstante, também tem sido bastante demandada a atuação do perito na elaboração de Notas Técnicas que auxiliam os membros do MPF em assuntos específicos de informática, os quais podem estar relacionados a questões criminais, do consumidor, de legislação, entre outras.

2 Revisão de Literatura

No mundo moderno, a Tecnologia da Informação e Comunicação (TIC) está cada vez mais presente na rotina das empresas e da maioria da população urbana. Acerca do vertiginoso aumento da importância das TIC, Porter e Millar (1985) definem a sua relevância na cadeia de valor e apontam que elas geram novos negócios inteiros, muitas vezes de dentro das operações existentes da própria empresa, além de criar

vantagens competitivas e mudar a estrutura da indústria alterando as regras de competição. Tais características foram em grande parte as responsáveis pela propagação das novas tecnologias.

Com tal disseminação de uso das TIC, os recursos eletrônicos não estão sendo apenas empregados pelas empresas, mas também estão sendo mais utilizados na prática de diversos crimes como estelionato, furto mediante fraude e pornografia infantojuvenil, entre outros. Não é nenhuma novidade que os computadores, smartphones, tablets, GPS, câmeras digitais, e outros dispositivos eletrônicos são utilizados e estão envolvidos em crimes e ações ilegais. Surge então um novo paradigma, que é a necessidade de lidar adequadamente com a análise e as investigações que envolvam o uso desses novos recursos tecnológicos.

Cumpre observar a definição de crime, conforme apresentada pelo Michaelis Moderno Dicionário da Língua Portuguesa (2009), de que é uma “violação dolosa ou culposa da lei penal”, podendo também ser socialmente definido como “violação das regras que a sociedade considera indispensáveis à sua existência” ou uma “infração moral grave; delito”.

Para Welch (2007, p.2781-2782) é notório que as mesmas novas tecnologias que “permitiram o avanço e a automação de processos de negócio, também abriram as portas para muitas novas formas de uso indevido de computadores”, sendo que aqui devemos incluir as diversas modalidades de crimes cibernéticos. Ele ainda ressalta a importância da conscientização e devida preparação para enfrentar uma “miríade de questões tecnológicas e jurídicas que afetam os sistemas e os usuários”.

Assim, faz-se importante que um órgão como o MPF esteja devidamente preparado para auxiliar na apuração dos crimes cometidos por meio da Internet e/ou dispositivos inteligentes conectados em rede, bem como no uso dos vestígios tecnológicos para a elucidação de crimes e os procedimentos para preservação da evidência digital. Inclusive, deve-se lembrar que a Internet é intrinsecamente vulnerável, pois foi concebida utilizando-se de protocolos inseguros.

Cabe destacar, conforme nos ilustram Farmer e Venema (2007), que a perícia computacional é, basicamente, a preservação, aquisição, análise, descoberta, documentação e apresentação de evidência presente em meio digital (equipamentos computacionais e mídias de armazenamento). O intuito é de comprovar a existência (ou ausência) de determinados eventos que possam ter levado à consecução de crimes ou atividades não autorizadas, ou ainda que possam provar que o evento não foi realizado conforme pode estar sendo imputado. Ademais, a forense computacional requer a combinação de técnicas de investigação com as exigências das leis e normas de cada País, organização e empresa.

Não obstante, cumpre destacar é devida uma distinção entre a utilização de soluções de TIC e investigação e perícia de TIC. Para tal, e considerando o Planejamento Institucional do MPF (2011), temos pela primeira abordagem o objetivo estratégico (OE)

número 4 de “Prover soluções de tecnologia da Informação e comunicações alinhadas com a estratégia”, enquanto pelo segundo enfoque temos o OE 13 de “Assegurar um corpo pericial flexível às demandas”.

Ademais, conforme mencionado por Joia (2012, p.36), que faz referência ao modelo de decomposição de gestão estratégica de TI proposto por Michael J. Earl, a estratégia de tecnologia da informação busca uma arquitetura tecnológica corporativa, sendo que “preocupa-se com o conjunto de tecnologias e infraestruturas necessárias, isto é, com a pergunta 'como?' (*how*)”, o que certamente não inclui a atividade de perícia. Os processos envolvidos nessa estratégia são relacionados com: escopo, arquitetura, capacidade e forças.

Tal divisão fica ainda mais clara, quando se observa a atuação específica de um profissional de TIC e de um perito de TIC. Apenas para um breve exemplo, na realização de uma atividade de obtenção ou coleta de dados, sob a ótica exclusiva de um profissional de TIC, uma cópia (também chamada de imagem) possuirá os dados armazenados (não necessariamente os excluídos e ainda não sobrescritos) em um disco rígido de origem, e pode ser obtida com uso de ferramentas como Clonezilla.

Por outro lado, uma cópia forense exige ferramentas bem específicas, com funcionalidades não disponíveis no Clonezilla. Conforme bem definido por Mandia (2003, p.153), uma cópia forense admissível como evidência é “um arquivo que contém cada bit de informação da origem, em formato *raw bitstream*”, como por exemplo o comando dd do Unix e o dcfldd[3]. Aqui ainda deve ser observada a necessidade de captura de dados voláteis, quase sempre ignorados pelos profissionais de suporte de TIC.

Observe-se ainda que uma cópia forense qualificada também pode ser armazenada em um formato diferente do *raw bitstream*, mas que contenha cada bit de informação da origem. São diversas as ferramentas que executam a cópia de tal forma, e ainda incluem outras características como o cálculo do *hash* e a compressão do arquivo de imagem, entre as quais vale mencionar o EnCase e o FTK.

Assim sendo, o viés do profissional de TIC que resolve todos os problemas relacionados a qualquer coisa que envolva informática deve ser fortemente combatido, especialmente na área pericial. Porém, devemos destacar que é certo que tal processo não é fácil, pois como Kahneman (2012, p. 5714) afirma, temos muitas vezes uma “cegueira induzida pela teoria: uma vez você tendo aceito uma teoria e a utilizado como ferramenta em seu pensamento, é extraordinariamente difícil notar suas falhas”.

Castanhar (2007, p.46-47), fazendo referência ao trabalho de Lumpkin e Dess, estipula que existe uma diferente definição entre empreendedorismo e orientação empreendedora (OE), destacando que a OE “é o conjunto de processos chaves que resultam num modo empreendedor de gestão estratégica” a qual “descreve como novos negócios serão desenvolvidos”. Ainda mencionando os citados autores, ele destaca a importância de observar cinco dimensões nas organizações empreendedoras: autonomia,

3 dcfldd – é um *fork* do dd, desenvolvido pelo U.S. Department of Defense (DoD) Computer Forensics Lab

capacidade de inovação, capacidade de assumir riscos, capacidade de agir proativamente e competitividade agressiva.

Tal abordagem empreendedora pode inclusive habilitar mais facilmente as necessárias mudanças nas perícias de TIC e de crimes cibernéticos no MPF, como bem define Mintzberg (2010, p.212), ao mencionar novas direções para a escola de aprendizado, de que uma organização capaz de aprendizado cumulativo e autorenovação constante é aquela que combina "flexibilidade com eficácia; é capaz de aprender com a experiência sem ser apanhada por esta e pode alavancar seu aprendizado no mercado".

2.1 Crimes de informática

O atual ordenamento jurídico brasileiro passou por algumas significativas mudanças nos últimos em função da jurisprudência relacionada ao julgamento de crimes cibernéticos, e aqui especialmente destaca-se a aprovação do novo Marco Civil da Internet (MCI) brasileira, sancionado em 23 de abril de 2014 por meio da Lei nº 12.965/14.

Anunciado por alguns como tendo criado um grande avanço na área de neutralidade da rede, que exige tratamento igualitário a todo conteúdo que trafega na Internet, admitidas algumas exceções, o MCI de fato apresentou alguns avanços, diversos dos quais ainda pendem de devida regulamentação. Contudo, foi duramente criticado por peritos em informática e advogados especialistas em direito digital, em diversos aspectos tais como a guarda de registros (logs) de acesso de usuários e privacidade de usuários e liberdade de expressão.

Nesse sentido, na subseção I da mencionada Lei é estabelecido um prazo muito exíguo em relação ao prazo mínimo que os provedores de conexão à Internet (por exemplo: Net, GVT, Oi, etc) e os provedores de aplicação de Internet (por exemplo: Google, Facebook, Uol, etc) deverão manter os seus registros de acessos:

> "Da Guarda de Registros de Conexão
> Art. 13. **Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano**, nos termos do regulamento. (…)
> Art. 15. **O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses,** nos termos do regulamento." (grifos nossos)

Os logs oferecem informações essenciais para iniciar adequadamente uma investigação, a qual fica bastante comprometida sem o fornecimento devido de dados que possibilitem a identificação de qual usuário estava vinculado a um IP identificado como origem de um suposto crime.

Para piorar ainda mais esse exíguo prazo de armazenamento definido, o Decreto nº 8.771, de 11 de maio de 2016, que regulamentou a Lei nº 12.965, definiu em

seu artigo 11 que “o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, **ficando desobrigado de fornecer tais dados**”. Isto é praticamente um convite aos criminosos para utilizarem redes WiFi abertas para o cometimento de delitos.

Ainda em relação ao Decreto nº 8.771, um grande equívoco foi gerado ao definir que os provedores possuem a obrigação de apagarem os dados de logs após o período previsto em lei, conforme estipula o parágrafo 2º do artigo 13:

> “§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, **os quais deverão ser excluídos**:
> I – tão logo atingida a finalidade de seu uso; ou
> II – **se encerrado o prazo determinado por obrigação legal**”. (grifos nossos)

Não obstante, a Lei nº 12.737/12 (conhecida na mídia como Lei Carolina Dickman, que havia sido vítima recente de uma divulgação indevida de fotos íntimas, pouco tempo antes da votação da Lei) já havia finalmente trazido para o ordenamento jurídico criminal o crime de “Invasão de dispositivo informático”, alterando o Decreto-Lei nº 2.848 de 7 dezembro de 1940, onde foram incluídos os artigos 154-A e 154-B.

Aqui cabe a ressalva de que ainda não está pacificado nos tribunais o que é necessário que ocorra para caracterizar a violação indevida de mecanismo de segurança, visto que nem sempre o usuário possui qualquer nível de segurança implementado ou talvez seja inviável comprovar tal violação.

Um outro fato bastante significativo foi o relatório da CPI de Crimes Cibernéticos (2016), que ratificou a necessidade urgente de investimentos na área de perícia com a apresentação de vários projetos de lei, os quais buscam melhor tipificação para alguns crimes, além de auxiliar tanto na investigação de tais crimes, como em uma melhor capacidade dos entes públicos para lidar com esse problema. Os investimentos nessa capacidade serão auxiliados com recursos oriundos do FISTEL, conforme proposto no projeto de lei que visa à alteração da Lei nº 5.070, de 7 de julho 1966.

Entre as justificativas apresentadas nos projetos de lei mencionados no relatório da CPI de Crimes Cibernéticos (2016), algumas constatam claramente o fato de que é essencial uma melhor tipificação de alguns crimes, como em “conforme apurado por esta Comissão Parlamentar de Inquérito, a legislação brasileira ainda é muito incipiente no que diz respeito aos crimes cibernéticos”. Isso também observado em outras duas distintas justificativas, que comentam a aprovação da Lei nº 12.737/12, e as quais afirmam que “em que pese essa disposição legal, os trabalhos da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos evidenciaram a falta de estrutura dos Estados no combate a esses tipos de crimes” e também “que não há dúvida que a legislação precisa ser aprimorada”.

Além disso, legislações anteriores ao advento da Internet, também são

utilizadas na tipificação de crimes, pois a conduta já era prevista como criminosa, como é o caso de, por exemplo, criar uma comunidade para se expressar contra grupos étnicos (este sendo inclusive um crime investigado pelo MPF), segundo dispõe o artigo 20, da Lei nº 7.716/89:

> "Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15/05/97)
> Pena: reclusão de um a três anos e multa. (Redação dada pela Lei nº 9.459, de 15/05/97) (...)"

Observando a questão jurídica pela ótica de quem trabalha na investigação, analisando alguma evidência, é importante mencionar o Código de Processo Civil (Lei nº 13.105/2015), em especial os artigos 156 a 158:

> "Art. 156. **O juiz será assistido por perito quando a prova do fato depender de conhecimento técnico ou científico.**
> § 1o Os peritos serão nomeados entre os profissionais legalmente habilitados e os órgãos técnicos ou científicos devidamente inscritos em cadastro mantido pelo tribunal ao qual o juiz está vinculado. (…)
> Art. 157. O perito tem o dever de cumprir o ofício no prazo que lhe designar o juiz, empregando toda sua diligência, podendo escusar-se do encargo alegando motivo legítimo. (…)
> Art. 158. **O perito que, por dolo ou culpa, prestar informações inverídicas responderá pelos prejuízos que causar à parte** e ficará inabilitado para atuar em outras perícias no prazo de 2 (dois) a 5 (cinco) anos, independentemente das demais sanções previstas em lei, devendo o juiz comunicar o fato ao respectivo órgão de classe para adoção das medidas que entender cabíveis."
> Grifos nossos.

Conforme constata-se, o trabalho pericial é bastante especializado e além de demandar profundos conhecimentos técnicos e necessária constante atualização, traz consigo uma enorme responsabilidade ao profissional que o executa, o qual responde juridicamente pelo resultado da perícia realizada.

Nesse contexto, fica clara a necessidade de uma remuneração distinta, com uma gratificação que seja automaticamente aplicada a todos que desempenham a função pericial no MPF, e não apenas nos moldes atuais da GAP (Gratificação de Atividade Pericial) que somente é prevista nas ocorrências de perícias externas.

Ainda, não se deve esquecer também da Seção X do mencionado CPC, e em especial do artigo 465 que estipula de prazos e define a possibilidade de somente inquirição pelo juiz competente:

> "Art. 465. O juiz nomeará perito especializado no objeto da perícia e fixará de imediato o prazo para a entrega do laudo.
> § 1o Incumbe às partes, dentro de 15 (quinze) dias contados da intimação do despacho de nomeação do perito:
> I – arguir o impedimento ou a suspeição do perito, se for o caso;
> II - indicar assistente técnico;
> III - apresentar quesitos.
> § 2o Ciente da nomeação, o perito apresentará em 5 (cinco) dias:
> I - proposta de honorários;
> II - currículo, com comprovação de especialização;

> III - contatos profissionais, em especial o endereço eletrônico, para onde serão dirigidas as intimações pessoais.
> § 3o As partes serão intimadas da proposta de honorários para, querendo, manifestar-se no prazo comum de 5 (cinco) dias, após o que o juiz arbitrará o valor, intimando-se as partes para os fins do art. 95. (…)
> § 5o Quando a perícia for inconclusiva ou deficiente, o juiz poderá reduzir a remuneração inicialmente arbitrada para o trabalho (...)".

Eleutério e Machado (2011) ratificam o entendimento de que, apesar da utilização de computadores não ser nada de novo, de fato a legislação brasileira não está preparada e precisa ser revista, de forma a possibilitar a adequada tipificação das diversas modalidades de crimes cibernéticos.

Cumpre observar que são duas as categorias essencialmente utilizadas para categorização dos chamados crimes cibernéticos: a dos crimes digitais próprios (ou puros), e a dos crimes digitais impróprios (ou mistos), conforme bem colocado pelo Prof. Marcelo Crespo (2015):

> "**Crimes digitais próprios ou puros** (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e
> **Crimes digitais impróprios ou mistos** (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio."

A seguir são ilustradas algumas formas de crimes cibernéticos mais comuns, com as suas respectivas tipificações:

Tabela 1: Algumas tipificações de formas de crimes Cibernéticos comuns

Crime	**Tipificação**
Estelionato e furto eletrônicos (fraudes bancárias)	arts. 155, §§ 3º e 4º, II, e 171 do CP
Invasão de dispositivo informático e furto de dados	art. 154- A do CP
Falsificação e supressão de dados	arts. 155, 297, 298, 299, 313-A, 313-B do CP
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infantojuvenil.	arts. 241 e 241-A, do ECA (Lei nº 8.069/90)
Assédio e aliciamento de crianças	art. 241-D, do ECA (Lei nº 8.069/90)
Ameaça	art. 147 do CP
Cyberbullying (criação e publicação de perfis falsos, veiculação de ofensas em blogs e comunidades virtuais)	arts. 138, 139, 140 do CP

Crime	Tipificação
Interrupção de serviço	art. 266, parágrafo 1º, do CP
Incitação e apologia de crime	arts. 286 e 287 do CP
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	art. 20 da Lei 7.716/89
Crimes contra a propriedade intelectual artística e de programa de computador	art. 184 do CP e Lei 9609/98
Venda ilegal de medicamentos	art. 273 CP

Assim, também observa-se que a velocidade vivenciada na mudança dos hábitos da população, em função dos usos de novas tecnologias, tem trazido consigo um enorme desafio na adaptação e definição de regras de boas condutas, as quais muitas vezes são indevidamente utilizadas e exploradas por mentes criminosas. No mesmo sentido, a Internet possibilitou novas formas de interação social, as quais também facilitaram a aplicação de golpes e o cometimento de crimes.

Deste modo, são várias as modalidade possíveis de fraudes cibernéticas, e a figura do mapa mental a seguir, adaptado de Krebs (2012), ilustra alguma dessas diversas possibilidades de forma bastante didática.

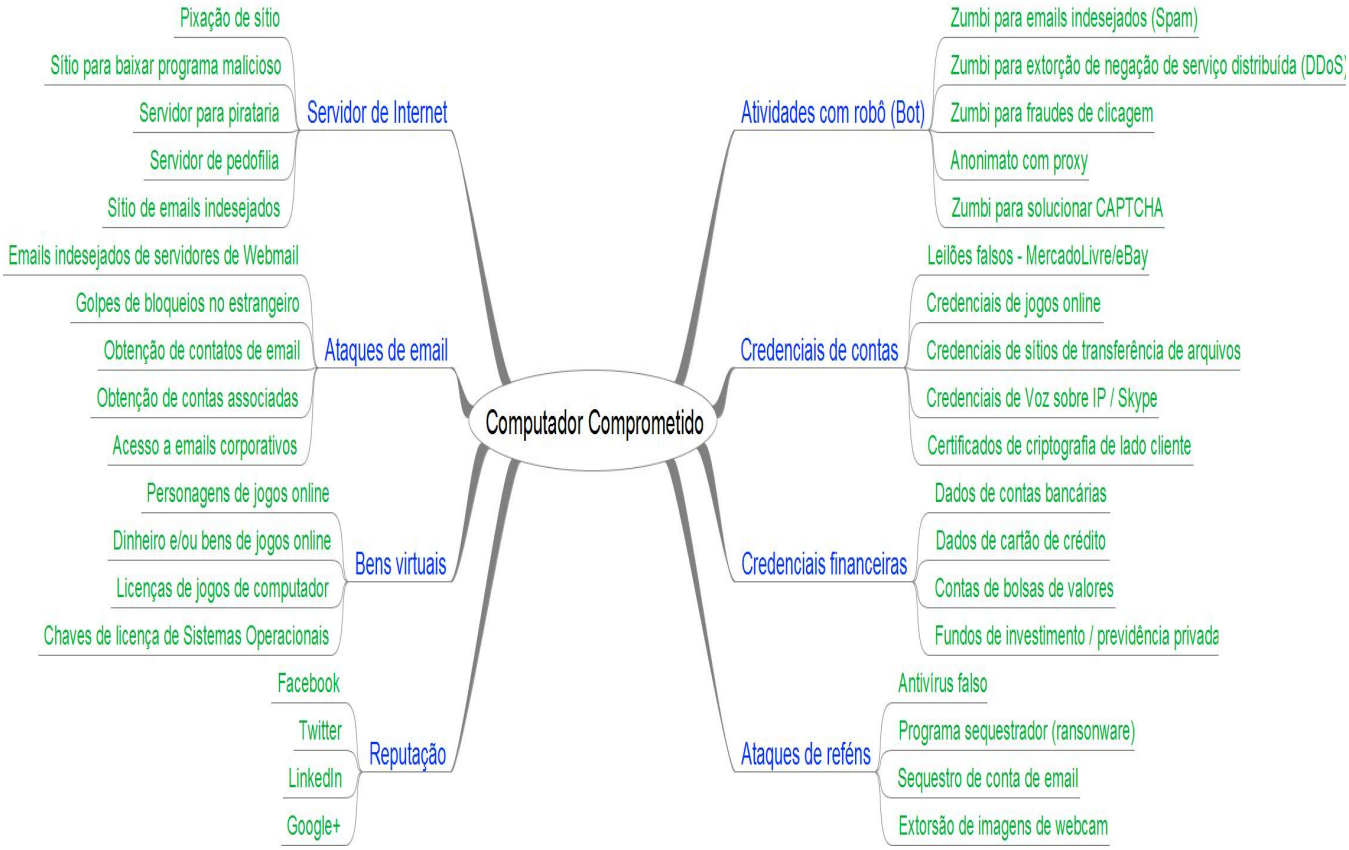

Figura 2: Mapa Mental de Fraudes Cibernéticas

Enfim, é fundamental que exista um tratamento adequado, nos incidentes de segurança e crimes cibernéticos, pelas forças da lei e também nas próprias organizações, conforme ilustrado no texto do Software Engineering Institute da Carnegie Mellon University (CERT, 2016): “A rapidez com que a organização pode reconhecer, analisar e responder a um incidente limitará os danos e diminuirá o custo de recuperação”.

3 Metodologia

3.1 Tipo de Pesquisa

A pesquisa realizada foi bibliográfica e documental.

Os aspectos ilustrados na pesquisa bibliográfica abordaram as áreas de perícias em TIC e de crimes cibernéticos, sempre buscando uma correlação com a atividade institucional do MPF.

Destaca-se que o MPF no Brasil possui uma atuação singular, sendo um órgão com atribuição para tutela coletiva e dos interesses difusos da sociedade, conforme disposto no artigo 6º da Lei Complementar nº 75, de 20 de maio de 1993.

No mesmo diapasão, e conforme dispõe o inc. III do art. 129 da Constituição da República Federativa do Brasil, o MPF pode instaurar o inquérito civil público e ajuizar ação civil pública para a proteção de interesses difusos e coletivos:

> “Art. 129. São funções institucionais do Ministério Público:
> I - promover, privativamente, a ação penal pública, na forma da lei;
> II - zelar pelo efetivo respeito dos Poderes Públicos e dos serviços de relevância pública aos direitos assegurados nesta Constituição, promovendo as medidas necessárias a sua garantia;
> III - promover o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos;”

A pesquisa documental teve por objetivo coletar informações sobre as perícias de TIC e cibernéticas atualmente realizadas no MPF, levantando os seguintes fatores: tipos de perícia, especializações temáticas, distribuição dos peritos, impactos no trabalho, limitações, necessidades e recursos desejados.

3.2 Universo e Amostra

O Universo considerado foi o de atividades de perícias de TIC e cibernéticas realizadas no Ministério Público Federal, bem como a atuação como assistente técnico nessas áreas.

A amostra considerada foi não-probabilística, composta pelos dados registrados pelos únicos dois peritos de informática atualmente do corpo de servidores do MPF, e também pelos dados do sistema pericial, que foi nacionalmente implementado no ano de 2015.

3.3 Coleta de Dados

Os dados foram coletados por meio de análise de informações do sistema e de registros mantidos sobre perícias de TIC.

3.4 Análise dos Dados

Os dados coletados foram submetidos a tratamento quantitativo e qualitativo.

4 Perícias no MPF

As perícias de TIC e de crimes cibernéticos no MPF, em que pese possuírem várias semelhanças com perícias digitais em um sentido amplo, carregam características distintas das atividades desenvolvidas por peritos criminais e também por peritos digitais que trabalham em organizações privadas.

Tais características distintas decorrem em razão das funções institucionais do MPU em geral, e do MPF em específico, conforme definidas pela Constituição da República Federativa do Brasil e pela Lei Complementar nº 75/1993.

Assim, deve-se ter bem definidas quais as áreas de atuação, as quais apresentam, entre outros, os seguintes requisitos profissionais necessários para um bom desempenho da atividade pericial, sabendo que a experiência profissional é certamente a mais importante condição para a adequada formação de um bom profissional de perícia:

- Sólida formação acadêmica em TIC, com domínio especialmente de: hardware, redes de computadores, sistemas de arquivos, sistemas operacionais, linguagens de programação, sistemas de banco de dados, auditoria de segurança, aplicativos, *hashes* e criptografia;
- Conhecimentos específicos de técnicas de análise de dispositivos computacionais e de dispositivos móveis;
- Profundos conhecimentos de procedimentos de aquisição, investigação, pesquisas, recuperação de dados, análise de mídias, linha do tempo e cadeia de custódia;
- Bons conhecimentos na área jurídica, em modo particular de legislação correlata a contratos e licitações, administração pública, direito civil e direito do consumidor;
- Possuir certificações na área;
- Forte ética profissional; e
- Redação de documentos e relatórios, e técnicas de apresentação.

Essencialmente, são apresentadas duas grandes áreas de atuação do profissional perito de TIC no MPF: perícias de TIC e perícias de crimes cibernéticos.

4.1 Perícias de TIC

As perícias de TIC realizadas no MPF veem observando uma forte associação com crimes relacionados ao Patrimônio Público, notadamente com denúncias de suporto superfaturamento na aquisição ou contratação de serviços de informática, bem como de inobservância da Lei nº 8.666:

> "Lei nº 8.666, de 21 de junho de 1993
> Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências."

O próprio Tribunal de Contas da União (2012, p.7), que vem monitorando um grande número de falhas nos procedimentos de compras de bens e serviços de TIC pelos entes públicos, publicou o documento Guia de boas práticas em contratação de soluções de tecnologia da informação para tentar diminuir esse problema:

> "Nos dias atuais, é difícil vislumbrar alguma ação desenvolvida pelos órgãos e entidades da Administração Pública Federal que não dependa direta ou indiretamente da Tecnologia da Informação (TI), cuja utilidade reveste-se cada vez mais de grande relevância. (...)
> Esta publicação propõe-se ajudar os gestores públicos a planejar as contratações de TI e evitar problemas já conhecidos, de maneira consistente e sustentável."

Cumpre mencionar que além das perícias, em uma concepção mais ampla de seu significado, existem várias outras atividades demandadas dos peritos de informática do MPF, entre as quais se destacam:

- Assessoramento de interlocução no relacionamento com agências e órgãos públicos;
- Acompanhamento de Políticas Públicas;
- Assessoramento in loco para atuação em projeto e atividades coordenados pelos Grupos de Trabalho (GTs) das Câmaras de Coordenação e Revisão (CCRs); e
- Esclarecimentos técnicos.

Mesmo com um número extremamente reduzido de peritos de informática, diversas têm sido as perícias e atuações como assistente técnico na área de TIC, conforme pode-se constatar em alguns exemplos, ilustrados na tabela a seguir:

Tabela 2: Exemplos de perícias de TIC realizadas no MPF

Referência	**Descrição**
Inquérito Civil 1.24.000.000445/2012-44 / ICP 445/2012	Suposto uso indevido de verba pública pela Prefeitura Municipal de João Pessoa no Jampa Digital
Inquérito Civil 1.30.012000737/2008-64 / ICP 1161/2010	INCA – licitação de equipamentos

Referência	Descrição
Inquérito Civil 1.30.012000801/2008-5 ICP 456/2010	ANP – Haliburton – Contratação de software
Processo 2006.34.00.033947-2	MAPA – Consórcio CNTC – Locação e atualização de computadores
Processo 2005.34.00.007998-2	Prodasen – Aceco – Sala cofre
Inquérito Civil MPF/RJ 1.30.001.0005713/2011-26	Transferência de Tecnologia da Informação entre os Hospitais de Excelência e as empresas TOTVS S.A. E GENS S.A.
Inquérito Civil Público 1.34.001.004757/2012-71	Contrato para Prestação de Serviços de Comunicação Digital celebrado entre a União e a Empresa Brasileira de Comunicação Produção Ltda
Processo 1.29.000.001929/2012-24	Apurar a atuação da ANATEL para fiel observância dos artigos 16 e 17 do regulamento de gestão da qualidade do serviço de comunicação multimídia por ela editado (resolução n. 574/2011), que dispõem sobre o mínimo de velocidade oferecida aos consumidores.
Inquérito Civil Público 1.21.002.000147/2012-46	Apurar possíveis problemas de abrangência de sinal de telefonia celular das empresas de telecomunicações Vivo, TIM, Claro e Oi.
Inquérito 1.22.000.002061/2015-83	Representação contra candidato, que no período eleitoral de 2012 ofertou a eleitores viagem de ônibus

Desse modo, o incremento da utilização de procedimentos de aquisição de bens e serviços de TIC como ferramenta para fraudar o erário, deve possuir a sua devida contrapartida na posse, preparação e adequação dos peritos de informática do MPF.

Nesse sentido, o presente trabalho possui um significado especial pelo fato de ser elaborado no exato momento em que na SEAP está sendo criada área funcional na qual as perícias de TIC e de crimes cibernéticos começarão a se estruturar devidamente, por meio da Assessoria Temática Modular.

4.2 Perícias de Crimes Cibernéticos

As perícias de crimes cibernéticos no âmbito do MPF são aquelas cujo objeto trata de crimes cuja atuação e competência é da Justiça Federal.

A página do MPF (2015) da sala de atendimento ao cidadão esclarece sucintamente quais são os crimes investigados pelo órgão:

> “Na área criminal, cabe ao MPF promover a ação penal pública quando a competência para o julgamento é da Justiça Federal. A instituição atua de forma preventiva e repressiva nos casos de crimes contra a Administração Pública

> Federal (delitos que causem prejuízo aos bens, serviços ou interesses da União, de suas entidades autárquicas ou das empresas públicas), inclusive nos crimes praticados por servidor público federal, como estelionato, roubo, peculato, corrupção ativa ou passiva, concussão, tráfico de influência e emprego irregular de verba ou renda pública. **Também são objeto da atuação do MPF crimes cometidos por meio da internet, como divulgação de pornografia infantil, racismo e fraudes bancárias**". (grifo nosso)

A seguir são listadas algumas das perícias cujos escopos de atuação, análise e investigação se enquadram na categoria de crimes cibernéticos, podendo não representarem necessariamente um crime cibernético.

Tabela 3: Exemplos de perícias de crimes cibernéticos realizadas no MPF

Referência	**Descrição**
Ação Civil Pública 0009596-94.2015.4.03.6100	Indenização de danos materiais e morais ocasionados a bebês e crianças que foram enviados ilicitamente ao exterior
Processo 1.26.000.000285/2016-92	Apurar notícias de publicação de conteúdo Nazista na Internet
Processo 1.26.000.003637/2015-81	Possível veiculação de opiniões preconceituosas em página da rede social Facebook
Processo 1.26.000.001340/2016-61	Compartilhamento de vídeo no youtube, de informações e imagens com suposta apologia aos crimes de tortura e de ódio
Processo 1.26.000.001495/2015-1	Apurar, em sede de controle externo da atividade policial, noticia de possível existência de cavalo de troia em máquina da Polícia Federal
Inquérito 0002746-97.2014.4.05.830	Pedido de quebra para instruir investigação em relação a divulgação de mensagens discriminatórias contra nordestinos
Inquérito 0000097-10.2015.4.05.8306	Divulgação de imagens de meninas menores de idade, vestindo roupas íntimas de tamanho mínimo, por meio do Facebook
Processo 1.15.000.001481/2014-04	Denúncia sobre divulgação de dados pessoais de residentes no Brasil pelo site: www.fonedados.com

Ademais, a Comissão Permanente Disciplinar também tem demandado perícias internamente, com uma abordagem similar às investigações e análises de crimes cibernéticos, onde se destacam atividades ilegais ou que violam a Política de Segurança da Informação do MPF.

Tais perícias não vinham sendo registradas no Sistema Pericial em função de restrições do próprio sistema, e portanto não há como apresentar dados precisos. Contudo, uma atualização do sistema realizada em junho de 2016 (versão 5.0) passou a

permitir o seu registro, por meio de cadastramento de perícia com a opção de membro responsável.

Até o momento foram solicitadas algumas poucas perícias de dispositivos móveis, especificamente de aparelhos de *smartphone*, mas não existe capacidade no MPF que possibilite a execução de tais trabalhos, em função de não possuir nem software e nem hardware específicos para este objetivo.

5 Conclusões

O quadro de servidores que compõem a especialidade de Analista do MPU / Perícia / Tecnologia da Informação e Comunicação está muito aquém das atuais necessidades do MPF, com apenas 2 ocupantes nesse cargo. Tal incremento no quantitativo de profissionais dever ser acompanhado de uma estrutura de equipamentos e de treinamentos específicos às áreas de atuação e demandadas no MPF.

Urge que seja quebrado o paradigma de dependência da realização de perícias de TIC e de crimes cibernéticos por profissionais de TIC de outras áreas distintas da perícia. É certo que tais profissionais são muito importantes neste momento crítico de um quadro completamente deficitário, e também que alguns sempre possuirão espaço como atuar peritos eventuais.

Não obstante, conforme demonstrado neste trabalho, é essencial que seja iniciado um processo de melhoria no suporte às perícias de TIC e de crimes cibernéticos solicitadas pelos Membros do MPF. Esses, inclusive, já veem buscando alternativas para resolver tais questões, como a criação de núcleos de combate a crimes cibernéticos em unidades isoladas. Isso pode até mesmo consolidar um modelo inadequado, em que a SEAP não possua espaço, não exista gestão de conhecimento, não seja viável qualquer controle de qualidade ou padronização, e inexistam métricas de quantidade e tempo para a realização de perícias nessas áreas.

Assim, o viés de resolução de problemas por profissionais que não sejam preferencialmente peritos e especializados na área, o que difere inclusive do disposto no CPC, deve ser descongelado, criando uma melhoria duradoura com monitoração persistente, onde os gerentes não sejam recompensados pelos resultados, mas por boas decisões, conforme modelo de processo decisório proposto por Bazerman (2014).

Por fim, um modelo que também não pode deixar de ser mencionado é o da Polícia Federal, que conta com o Instituto Nacional de Criminalística em Brasília e os Setores Técnicos Científicos nos estados para a realização de perícias.

Conforme anteriormente mencionado, os trabalhos periciais do MPF podem ser em alguns momentos distintos daqueles desenvolvidos pela PF, mas é possível que no futuro seja interessante a utilização no MPF de um modelo semelhante ao da PF. Independente da adoção do modelo, é bastante relevante que ocorra um intercâmbio de

informações e de troca de conhecimentos entre os peritos da área de TIC e de crimes cibernéticos. Ademais, tais intercâmbios devem ser não apenas com a PF, como também com outros órgãos de forças da lei e de investigação nacionais e internacionais, de forma a alavancar o necessário alto padrão de qualidade nas perícias em TIC e de crimes cibernéticos no MPF.

6 Referências Bibliográficas

BAZERMAN, Max H., MOORE, Don. **Processo Decisório** – 8ª edição. Rio de Janeiro: Elsevier Editora Ltda, 2014.

Câmara dos Deputados. **Relatório Final da CPI - Crimes Cibernéticos**. Disponível em http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125&filename=Tramitacao-RCP+10/2015, Acesso: 15 de maio de 2016.

CASTANHAR, José Cezar. **Empreendedorismo e Desenvolvimento Regional no Brasil: Uma Análise da Relação entre a Criação de Empresas e o Desenvolvimento Regional ao Longo do Tempo e de Estratégias de Empreendedores Selecionados**, 2007. Tese (Doutorado em Gestão) – Escola de Gestão, Instituto Superior de Ciências do Trabalho e da Empresa, Lisboa.

CERT - Computer Emergency Response Team. **CSIRT FAQ** - Tradução do CSIRT FAQ do CERT®/CC, chttp://www.cert.br/certcc/csirts/csirt_faq-br.htmlom permissão especial do Software Engineering Institute (SEI). Disponível em , Acesso: 6 de junho de 2016.

CRESPO, Marcelo. **Crimes Digitais: Do que Estamos Falando?**. Disponível em http://canalcienciascriminais.com.br/artigo/crimes-digitais-do-que-estamos-falando/, Acesso: 20 de julho de 2015.

ELEUTÉRIO, Pedro Monteiro da Silva e MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** São Paulo: Novatec, 2011.

FARMER, Dan e VENEMA, Wietse. **Perícia Forense Computacional – Teoria e Prática Aplicada.** São Paulo: Pearson, 2007

JOIA, Luiz Antonio et all. **Gestão Estratégica da Tecnologia da Informação**. Rio de Janeiro: Editora FGV, 2012.

KAHNEMAN, Daniel. **Rápido e Devagar – Duas Formas de Pensar**. Rio de Janeiro: Objetiva, 2012. Formato: ePub.

KREBS, Brian. **The Scrap Value of a Hacked PC, Revisited**. Disponível em: https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/, Acesso: 5 de junho de 2016.

MINTZBERG, Henry, AHLSTRAND, Bruce, LAMPEL, Joseph. **Safári de**

estratégia: um roteiro pela selva do planejamento estratégico – 2ª Edição. Porto Alegre: Bookman, 2010.

MPF – Ministério Público Federal. **Atendimento ao cidadão – Perguntas Frequentes**: Quais são os crimes investigados pelo MPF. Disponível em: http://cidadao.mpf.mp.br/perguntas-frequentes, Acesso: 19 de julho de 2015.

PORTER, Michael e MILLAR, Victor. **How Information Gives You Competitive Advantage.** Disponível em https://hbr.org/1985/07/how-information-gives-you-competitive-advantage/ar/1, Acesso: 14 de maio de 2016.

TCU - Tribunal de Contas da União. **Guia de boas práticas em contratação de soluções de tecnologia da informação**. Disponível em http://portal2.tcu.gov.br/portal/pls/portal/docs/2511467.PDF. Acesso em 18 de agosto de 2015.

WELCH, Thomas. Computer Crime Investigation and Computer Forensics. In: TIPTON, Harold; KRAUSE, Micki (Org.). **Information Security Management Handbook** – 6th Edition. Florida: Auerbach Publications, 2007.