Instituto de Pesquisas Tecnológicas do Estado de São Paulo
Centro de Aperfeiçoamento Tecnológico - CENATEC

Monica Keiko Kosaka

Uma Comparação de Padronizações Gerais do Processo Investigativo em Perícia Computacional

São Paulo

2007

Monica Keiko Kosaka

Uma Comparação de Padronizações Gerais do Processo Investigativo em Perícia Computacional

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT, Engenharia de Computação, para a obtenção do título de Mestre em Engenharia de Computação

Área de concentração: Redes de Computadores

Orientador: Prof. Dr. Pedro Luis Próspero Sanchez

São Paulo

Julho 2007

Ficha Catalográfica
Elaborada pelo Departamento de Acervo e Informação Tecnológica – DAIT
do Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

K86c Kosaka, Monica Keiko
Uma comparação de padronizações gerais do processo investigativo em perícia computacional. / Mônica Keiko Kosaka. São Paulo, 2007.
215p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Pedro Luis Próspero Sanchez

1. Perícia digital 2. Forense digital 3. Vestígio digital 4. Prova digital 5. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Coordenadoria de Ensino Tecnológico II.Título

07-165 CDU 004.085.7:34(043)

Dedicatória

À minha família.

"Qualquer coisa que você possa fazer ou sonhar – Comece! A audácia contém em si mesma, o poder, o gênio e a magia". (Goethe)

Agradecimentos

Primeiramente agradeço ao Prof. Dr. Pedro Luis Próspero Sanchez, que me orientou nesse trabalho, pela paciência, disposição e pelo compartilhamento da sua vasta experiência.

Agradeço aos meus pais Maria e João e aos meus irmãos Márcia e Marcos por todo apoio até o término do trabalho, principalmente nos momentos mais difíceis e desafiadores.

Fico grata aos Prof. Dr. Volnys Bernal e Prof. Dr. José Henrique Andrade, pela oportunidade e enriquecedora presença na banca.

Gostaria de agradecer também ao Daniel Ramos, pelo apoio e incentivo.

Finalmente agradeço a todos os meus amigos que de alguma forma outra contribuíram nessa empreitada.

Resumo

À mesma medida em que a tecnologia da informação torna-se cada vez mais complexa e acessível, viabilizando novos usos nos mais diversos segmentos e tornando-se intrínseca às nossas vidas, os problemas associados a ela também estão evoluindo e se adaptando aos novos usos.

E nesse sentido, as tecnologias computacionais têm sido exploradas, identificando-se oportunidades para cometer ações ilícitas. Freqüentemente supõe-se que essas ações sejam mais difíceis de detectar, investigar e examinar em se tratando de ambientes digitais.

A investigação ou mesmo o processo investigativo como um todo pode ser comprometido em decorrência do negligenciamento de regras e procedimentos para a coleta, preservação e processamento de vestígios digitais, o que pode impossibilitar a admissibilidade da prova.

Esse trabalho faz o levantamento de algumas padronizações e métodos propostos aos processos investigativos e periciais computacionais e realiza um estudo comparativo, identificando elementos mínimos comuns e discutindo sobre os elementos que podem tornar-se diretrizes para uma abordagem sinergética em casos onde seja necessária a colaboração internacional.

Nesse estudo foram considerados fatores relevantes para a admissibilidade da prova no Brasil, nos Estados Unidos e países da União Européia.

Palavras-chave: Perícia, Forense Computacional, Perícia Digital, Tratamento de Incidentes, Vestígio Digital, Prova Digital, Admissibilidade da Prova

Abstract

In the same way Information Technology becomes more complex and accessible, making new uses possible in several segments of society and becoming instrinsic to our lives, the problems associated to it are evolving and adapting to those new uses.

In this sense, the Information Technology has been explored and consequently, illicit activity perpetration opportunities are identified. It is frequently assumed that these activities are more difficult to detect, to investigate and to examine when dealing with digital environment.

The reliability of investigation or even of the whole investigative process can be compromised by neglecting rules and procedures for digital evidence handling, making the evidence inadmissible.

This essay identifies some stardizations and methods proposed to the investigative and computer forensic processes and a comparative study is developed and it is composed of the minimum common elements among them and it is discussed what elements can conduct to a sinergetic approach in cases where the collaboration among nations is necessary. In this essay, it was considered relevant factos for digital evidence admissibility in Brazil, United States of America and European Union nations.

Keywords: Forensics, Computer Forensics, Digital Forensics, Incident Handling, Digital Evidence, Evidence Admissibility

Lista de Ilustrações

Lista de Tabelas

Sumário

1 INTRODUÇÃO

Desde a sua invenção, o computador, assim como o seu uso têm evoluído rapidamente e atingido a nossa sociedade de tal forma que começamos a depender dele em muitos aspectos.

O uso da rede de computadores e de seus serviços, proporcionam facilidades no cotidiano, otimização do trabalho nas corporações, que incluem serviços como telefonia, comércio eletrônico e Internet Banking.

No entanto, da mesma forma que o uso dessas tecnologias facilitam ou criam novos serviços, elas também dão oportunidade a novas modalidades criminosas e ao uso incorreto em geral. Criminosos estão se utilizando dessas novas tecnologias e novos meios para perpetrar crimes que incluem pornografia infantil, abuso de menores, fraude, espionagem, sabotagem, assédio, corrupção de menores (Casey, 2004).

Na mesma medida em que se aumenta a quantidade de dispositivos e sistemas computacionais, aumenta-se a quantidade dos incidentes de segurança. Cada vez mais, surgem novas técnicas, artefatos e categorias de ataques com nível de complexidade cada vez maior e mais “popularizado”.

De acordo com a Agência FAPESP (2006), o número de tentativas de fraudes bancárias e financeiras pela Internet cresceu 579% em 2005, em relação ao ano anterior, segundo levantamento feito pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br), mantido pelo Comitê Gestor da Internet no Brasil.

Em 2004, as tentativas de fraudes não passavam de 5% do total de incidentes reportados. Em 2005, chegaram a 40%. Os números são de estatísticas sobre incidentes na internet notificados espontaneamente ao Cert.br por administradores de rede e usuários.

Na ocorrência de incidentes, a investigação certamente requisitará a inclusão de dados eletrônicos nas análises. O desafio na situação é identificar o que pode ser um vestígio importante dentre a imensidão de dados e dispositivos que podem se tornar um indício importante, como coletá-la, armazená-la sem que seja adulterada e

analisar esses materiais através de procedimentos que sejam aceitos pela comunidade científica.

1.1 Motivações

Em virtude dessa crescente informatização nos mais diversos ambientes e setores da sociedade, há um aumento da complexidade das aplicações e especialização e ao mesmo tempo, facilidade de acesso.

Cada vez mais e numa velocidade crescente será necessária a utilização de informações digitais nas investigações. Como a perícia computacional é incipiente e os vestígios digitais possuam peculiaridades se comparados com os físicos, pode-se concluir prematuramente que existe pouca documentação e padronização nessa área de especialização.

Além disso, no processo investigativo e pericial agentes das diversas esferas, com conhecimento específico ou não, podem lidar com vestígios digitais nos mais diferentes processos que incluem a investigação, a perícia e o tratamento de incidentes.

Ao desempenhar essas atividades sem se cumprir um mínimo de requisitos procedurais e legais, os vestígios e indícios podem ser comprometidos, impossibilitando a constituição de prova, independentemente se serão tratados em âmbito de processo legal.

Em incidentes que envolvam ambientes computacionais localizados em território internacional, a situação é agravada pois cada nação pode ter requisitos legais e investigativos específicos, o que pode dificultar ou inviabilizar o aproveitamento do trabalho pericial já efetuado.

Existem trabalhos acadêmicos no sentido de proposição de métodos para a forense computacional, mas são escassos os estudos comparativos de padronizações e procedimentos existentes e principalmente contextualizado no Brasil.

1.2 Objetivos

O objetivo principal desse trabalho é identificar padrões e recomendações já estabelecidos para a investigação e perícia digital. Um dos requisitos fundamentais para a admissibilidade legal é o uso de técnicas e procedimentos idôneos.

Dentre os objetivos específicos, procurou-se apresentar as relações teóricas entre as padronizações e métodos na investigação e perícia em crimes cibernéticos.

Além disso, procurou-se também identificar requisitos técnicos e legais atualmente estabelecidos no Brasil e em países da União Européia.

1.3 Metodologia

Inicialmente, foi efetuado um levantamento bibliográfico detalhado referente ao assunto.

Neste levantamento foram identificados os principais autores e seus respectivos artigos e teses, além das instituições que definiram normas, documentações e referências nesse sentido, dentre as quais podemos citar o DoJ (Departament of Justice), Federal Judicial Center, Nist (National Institute of Standards and Technology), instituições americanas, o European Commission Directorate-General Information Society e organizações policiais européias.

Primeiramente, através de documentos sobre o procedimento de perícia e legislação foram elencados os conceitos fundamentais utilizados na perícia computacional e nos procedimentos investigativos.

Na segunda parte são apresentados os fundamentos de perícia computacional, o histórico e desafios.

Na terceira parte, foram levantados padrões e métodos utilizados para a investigação e perícia em informática, considerando-se padrões e procedimentos adotados em empresas, organizações policiais e periciais e no judiciário.

Os documentos que descrevem métodos científicos, como o Reference Manual on Scientific Evidence e o levantamento comparado dos métodos da forense digital do trabalho desenvolvido por Brian Carrier, Carrier (2006), avaliando-se as categorias das camadas de análises a serem consideradas na forense

computacional. Nessa parte foram identificadas critérios como os Fryes e Daubert que podem determinar a admissibilidade da prova.

Na quarta parte, foi feito um levantamento do panorama internacional em termos de alguns incidentes de segurança da informação, a legislação e procedimentos existentes.

Na quinta parte os padrões, modelos de processos investigativo-pericial e o cenário internacional são comparados.

1.4 Justificativa

O trabalho de comparação é importante para a determinação da relevância dos procedimentos e técnicas utilizados e a aplicabilidade nos casos investigados.

Os estudos teóricos permitem um comparativo entre as normas e procedimentos existentes no Brasil e União Européia consistentes e que podem determinar a admissibilidade da prova.

1.5 Trabalhos correlatos

Existem várias propostas de modelos apresentadas para a condução de perícias digitais, algumas com similaridades.

Como base para esse estudo, foram analisados os trabalhos de NIJ (U.S. National Institute of Justice), Carrier e Spafford (2003), Beebe e Clark (2004) e Casey (2004) e Carrier (2006), faz um comparativo entre modelos atuais, identifica classes e técnicas de análises e propõe um novo modelo com abordagem em hipóteses, usando Máquinas de Estados Finitos.

1.6 Sumário Estruturado

Este trabalho abordará os tópicos: 1- Introdução, 2- Conceitos básicos de perícia, 3 - A Contextualização da perícia de informática, 4 – A padronização existente e os processos Investigativos e Periciais, levantando-se métodos utilizados pela Ciência Forense, métodos utilizados pela Forense Computacional, 5 – A admissibilidade e regras de valoração de provas, 6 – Legislação e Perícia

Computacional no Panorama Internacional, 7 - Comparação entre padrões, modelos e questões transnacionais, 8 - e finalmente o último tópico com as conclusões do trabalho.

2 PERÍCIA – CONCEITOS

Nesse capítulo, são apresentados alguns dos conceitos fundamentais relacionados às provas, utilizados nos meios policial, judicial e pericial, de forma a permitir uma melhor compreensão da aplicação desses conceitos nas variadas atividades investigativas e periciais nos ambientes computacionais e digitais.

Embora esse trabalho não tenha o objetivo de se aprofundar em temas jurídicos e da segurança pública, procurou-se levantar conceitos, identificando requisitos e procedimentos que estejam relacionados ou que possam de alguma forma afetar a perícia computacional ou mesmo as atividades extrajudiciais investigativas e de resposta a incidentes de computador.

2.1 Prova

Para que o juiz possa decidir sobre um determinado fato, ou ainda no campo penal, para que ele possa ter a convicção de que um delito foi cometido, de que o acusado é o autor e para aplicar as sanções, ele deverá estar convencido da veracidade dos fatos apresentados.

Conforme Fernandes, Gomes Filho e Grinover (2006), a prova é o instrumento através do qual o juiz poderá chegar a esse convencimento.

"Prova é um conjunto de atividades de verificação e demonstração, mediante as quais se procura chegar à verdade quanto aos fatos relevantes para o julgamento" (DINAMARCO, 2005, p. 43).

Essas atividades de demonstração que compõem a prova são promovidas pelas partes, por terceiros, como os peritos e testemunhas, e também pelo próprio juiz, de acordo com Mirabete (2007).

Malatesta (2001) já concluía que a eficácia da prova será tanto maior, quanto mais clara, plena e seguramente ela induzir a certeza da verdade e, portanto, não deve dar espaço às dúvidas de veracidade, denominadas de questões de fato por Fernandes, Gomes Filho e Grinover (2006), durante a apreciação das provas.

Posteriormente, alguns tipos de provas serão abordados com mais detalhes, entretanto, vale salientar a importância da prova pericial, que é um dos principais

objetos de estudo desse trabalho, apontada por Fernandes, Gomes Filho e Grinover (2006), como um dos meios mais eficazes de prova.

2.1.1 Fontes de Prova

Dinamarco (2005) define fonte de prova como “pessoas ou coisas das quais se possam extrair informações capazes de comprovar a veracidade de uma alegação” (DINAMARCO, 2005, p. 86).

Dinamarco (2005) as classifica como fonte de prova real quando constitui-se de coisa ou ainda de pessoas examinadas (ex. perícia médica) e também como fonte de prova pessoal quando a pessoa for chamada para participar da instrução probatória (ex. testemunha). Além dessa classificação, considera as fontes pessoais como ativas e as reais como inativas.

2.1.2 Meio de Prova

“Meios de prova são as técnicas destinadas a atuar sobre as fontes e delas extrair o conhecimento dos fatos relevantes para a causa” (DINAMARCO, 2005, p. 48).

Assim, a prova pericial é uma das técnicas probatórias consideradas meio de prova.

Segundo Mirabete (2007), no processo penal brasileiro, diferentemente do civil, é utilizado o princípio da verdade real, que determina a redução dos requisitos da prova, permitindo que as partes se utilizem dos meios de prova com ampla liberdade.

O objetivo dessa liberdade probatória é não limitar a prova, porque a limitação pode dificultar a obtenção da verdade e consequentemente da aplicação da lei.

Essa liberdade, porém, não é absoluta devido a algumas restrições previstas no Código Civil. A exemplo disso, como regra, o estado civil casado deve ser provado através da certidão de casamento.

No Código de Processo Civil brasileiro, os depoimentos pessoais das partes, provas testemunhal, documental e pericial, a inspeção judicial e a confissão são

considerados meios de provas. Dinamarco (2005) faz a ressalva de que a confissão não é conceitualmente um meio de prova por não se tratar de uma técnica para extrair fatos de uma fonte de provas.

No procedimento probatório do processo civil, as partes fazem o requerimento das provas e devem determinar para cada prova a ser apresentada, qual o meio de prova a ser utilizado e o que se quer demonstrar.

2.1.3 Objeto de Prova

Objeto de prova é o fato que deve ser provado para a decisão da causa. E segundo Mirabete (2007), no campo penal, tais fatos incluem o próprio delito, o autor e todas as circunstâncias que podem determinar a sanção a ser aplicada.

Esse autor frisa ainda que na esfera penal, os fatos que não se tornaram controversos também podem se tornar objeto de prova. O juiz deve questionar sobre tudo o que considerar dúbio ou suspeito e não chegar necessariamente à convicção como as partes o fizeram, ao contrário do que ocorre nos processos civis, onde a preocupação está somente nos fatos controversos.

2.1.4 Classificação das Provas

Tanto Mirabete (2007) quanto Dinamarco (2005) classificam as provas nas categorias a seguir, divergindo nas peculiaridades dos âmbitos cível e penal, principalmente no que se refere aos objetos de prova (ou coisas demonstradas).

Quanto ao conteúdo ou objeto:

a) *Direta* – a prova é a demonstração do fato ou circunstância sem a necessidade de um processo lógico construtivo. Ex. Carta caluniosa em um processo de calúnia;

b) *Indireta* – refere-se aos elementos probatórios que não estão conectados diretamente aos fatos relevantes para o julgamento ou ao delito e é necessário raciocínio para interpretá-los. Ex. Casaco ensangüentado na casa do acusado em um processo de homicídio;

Quanto à fonte:

a) *Prova Pessoal* (ou verificação da pessoa) – emprega fontes ativas (pessoas) como elementos probatórios. Ex. testemunhas.

b) *Prova Real* (ou verificação da coisa) – emprega fontes passivas como elementos probatórios. Ex. Perícias (prova técnica).

Quanto à forma:

a) *Testemunhal* – afirmação de pessoal fundamentalmente baseado na oralidade. São exemplos, as queixas ou as denúncias, os relatórios, os autos e as certidões e os interrogatórios;

b) *Documental* – "todo ser composto de uma ou mais superfícies portadoras de símbolos capazes de transmitir idéias e demonstrar ocorrência de fatos". "Esses seres são ordinariamente coisas e, mais corriqueiramente, papéis", (DINAMARCO, 2005, p. 564). São exemplos documentos escritos, imagens ou sons gravados, registros magnéticos em geral;

c) *Material* – permite a percepção direta da coisa probante, devido à materialidade de suas formas, conforme Malatesta (2001). São exemplos, os exames, o corpo de delito, as vistorias, o instrumento do crime e as provas técnicas.

De acordo com Dinamarco (2005), a classificação quanto à forma está baseada nos meios de prova, que são as técnicas utilizadas na investigação do fato a provar.

Cada espécie de fonte de prova possui peculiaridades que demandam técnicas específicas (meios de prova) para a extração das informações contidas nas fontes. Esse trabalho abordará especialmente um dos meios de prova, o pericial.

2.2 Evidência

Como os termos evidência e *evidence* em inglês foram encontrados em várias das obras coletadas para esse estudo em diferentes acepções, optou-se por tratá-los em seção específica.

É possível que a palavra evidência encontrada em algumas obras em português, trate-se da tradução direta da palavra “evidence” encontrada em trabalhos publicados no idioma inglês.

Dinamarco (2005) considera o uso um equívoco quando o termo evidence é traduzido como evidência, mas significando prova:

> É uma profanação ao vernáculo e às tradições vocabulares ligadas ao linguajar jurídico romano o emprego do vocábulo *evidência* em lugar de prova. Esse péssimo uso é obra de maus tradutores que, iludidos por um falso cognato (*pitfall*), não se apercebem de que *evidence* significa *prova* e não *evidência* (DINAMARCO, 2005, p.43).

Espíndula (2005), refere-se à evidência como o vestígio que passou por perícia e que está relacionado ao crime, numa definição, segundo o autor, utilizada na criminalística.

E frisa ainda que a evidência pode constituir “uma prova por si só ou em conjunto, para ser utilizada no esclarecimento dos fatos” (ESPÍNDULA, 2005, p. 86), numa acepção assemelhada ao de indício definido no artigo 239 do Código de Processo Penal.

Para entender o significado geral, foi realizada uma pesquisa pelo verbete e numa das definições do dicionário Houaiss, evidência é “a qualidade ou caráter de evidente, atributo do que não dá margem à dúvida”. Percebe-se o uso dessa acepção na definição de evidência de Espíndula (2005).

Mas evidência pode ser também “aquilo que indica, com probabilidade, a existência de (algo); indicação, indício, sinal, traço” em outra significação do dicionário Houaiss que pode remeter também às definições de vestígio e indício que serão descritos nesse trabalho.

Todavia, não foi identificada a utilização de evidência nos atuais códigos penal ou civil, bem como nos códigos processuais.

O termo *evidence* é definido pelas Cortes dos Estados Unidos (2006), em acepção próxima ao de prova apresentada nesse trabalho:

"Evidence – Information presented in testimony or in documents that is used to persuade the fact finder (judge or jury) to decide the case in favor of one side or the other". Tribunais dos Estados Unidos (2006).

A palavra "*evidence*" foi verificada em diversas acepções, dentre elas a de evidência de Espíndula (2005), bem como significando indício ou prova, principalmente nos materiais sobre forense computacional pesquisados, no idioma inglês.

A distinção entre os significados só ocorre através da compreensão do termo no contexto da obra. Na opinião de Casey (2004) há uma falta de consenso e consequentemente de padronização no que se refere aos termos utilizados na perícia computacional, até para os termos mais básicos.

Para Carrier (2006), algumas definições de "*digital evidence*" consideram somente os dados que possam ser utilizados em âmbito legal, enquanto que outros consideram todos os dados úteis durante uma investigação, mesmo que não sejam admissíveis juridicamente.

Casey (2004) redefiniu "*digital evidence*" na segunda edição de seu livro, justamente para ampliar o conceito, englobando outros dados colhidos e analisados que possam ser importantes nas investigações, mas que eventualmente não venham a constituir prova:

"Digital Evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi" (CASEY, 2004, p.12).

Apesar dessas divergências na definição de *evidence*, ora utilizado significando vestígio, ora indício, foi verificado que no livro de Mandia e Prosise (2001), em sua versão traduzida para o português por Tomas Bueno, o termo *evidence* é utilizado em tradução próxima ao de prova:

Prova é "qualquer informação com valor comprobatório, seja para confirmar ou para rejeitar uma hipótese" (MANDIA e PROSISE, 2001, p. 93).

Para evitar equívocos conceituais decorrentes de tradução, procurou-se não usar o termo evidência nesse trabalho.

2.3 Indício

Na definição do Código Processo Penal brasileiro:

> Considera-se indício a circunstância conhecida e provada que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias. (CPP, Art. 239).

Indício é um fato-base que revela a presença de outro fato. O juiz se apóia nos indícios, através da técnica das presunções, para tirar conclusões sobre o fato a ser provado, conforme Dinamarco (2005).

O indício por si só ou em conjunto de outros fatos probatórios pode constituir prova indireta.

Mirabete (2007) salienta que devido ao sistema de livre convencimento do juiz, não há uma relação de maior ou menor prestígio entre os tipos de provas e portanto, a prova indiciária tem o mesmo valor que as provas diretas.

No que se refere ao âmbito penal, Mirabete (2007) lembra que há situações onde indícios múltiplos e concatenados podem excluir qualquer hipótese favorável ao acusado, dando base para uma decisão condenatória. Mas também em outras situações, na apresentação de indícios isolados, se existir a possibilidade de que o acusado não tenha cometido o ilícito, a prova indiciária pode não ser suficiente para a condenação.

De acordo com Espíndula (2005), os termos vestígio, indício e evidência possuem significados semelhantes, mas somente vestígio e evidência são utilizados no âmbito da perícia, ao passo que indício é utilizado na fase processual, ou seja, no meio jurídico.

2.4 Vestígios

Espíndula (2003) define vestígios como todos os elementos, sejam objetos, marcas ou sinais sensíveis que possam ter relação com o fato investigado.

Segundo Rocha (2003), os vestígios podem ser classificados quanto à volatilidade em:

a) Transitórios – Vestígios que desaparecem rapidamente.

b) Permanentes – Vestígios que permanecem por longo tempo.

Espíndula classifica os vestígios quanto à sua produção:

a) Verdadeiro – é o vestígio produzido diretamente pelo autor do delito ou de suas ações;

b) Ilusório – é o elemento encontrado no local do crime, mas que não tenha relação com o autor do delito;

c) Forjado – vestígio produzido com o intuito de alterar o local do crime.

Os vestígios devem ser buscados, coletados e encaminhados para exame pericial quando ocorrer delito, conforme a legislação brasileira:

> Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado. (CPP, Art. 158).

De acordo com Espíndula (2005), todos os vestígios são importantes num primeiro momento para a elucidação dos fatos. Entretanto, pela impossibilidade dos peritos de realizarem a análise individual de cada vestígio no local do crime, é somente nos laboratórios do Instituto de Criminalística que os peritos poderão realizar todas as análises e exames complementares dos vestígios para a determinação da relevância ou de suas conexões com o crime.

Ainda conforme Espíndula (2005), é ao final dos exames periciais que se determinam quais dos vestígios estão relacionados ao crime e que serão utilizados pelos peritos para subsídio de suas conclusões.

2.5 Corpo de delito

Corpo de delito é um termo utilizado no âmbito penal e, de acordo com Costa (1999), são todos os elementos que tenham ligação com crime, o que inclui os sinais da ação do perpetrador do crime, do resultado da infração e dos meios empregados pelo autor.

Assim, conforme Rocha (2003), o corpo de delito é formado pelo exame pericial dos vestígios encontrados em local de crime durante a investigação, cuja

finalidade é permitir que se prove a materialidade, ou seja, que houve crime e responsável.

O juiz criminal não pode formalizar a pronúncia do crime (art. 408 do CPP) e nem decretar prisão preventiva (CPP, art. 312) caso não haja a certificação da existência do crime e é o exame de corpo de delito que poderá prová-lo, conforme Costa (1999).

O corpo de delito pode ser classificado como direto (quando há traços materiais) ou indireto (quando o fato não deixou vestígios ou já desapareceram ou foram destruídos). É obrigatório o exame de corpo de delito nos crimes que deixam vestígios (CPP, art. 158), podendo ocasionar nulidade do processo, segundo o art. 564, III, letra “b” do CPP, caso não seja obedecido o procedimento.

Embora o foco do trabalho esteja no corpo de delito direto, que demanda e permite a execução pericial, verificaremos que no aspecto investigativo, o corpo de delito indireto, que se baseia no testemunho da existência dos vestígios fugidios, pode ser fator direcionador do foco da coleta e análise dos vestígios no local do crime.

“Não se deve confundir o *corpo de delito* com o *corpo da vítima*”. (Rocha, 2003, p.83).

2.6 Perícia

A Perícia é o exame feito em coisas ou pessoas por especialista técnico para obter informações que esclareçam um fato. É necessária para se demonstrar o fato quando sejam necessários conhecimentos técnicos especializados que estejam fora do alcance do juiz, dos advogados e das partes, de acordo com Dinamarco (2005).

No âmbito penal brasileiro, conforme Mirabete (2007), a perícia pode ser solicitada assim que a autoridade obtiver conhecimento do delito ou até o final do inquérito policial, ou ainda solicitada pelo juiz. O autor salienta também que a perícia é uma atividade executada por órgão auxiliar da justiça, através do perito oficial que é funcionário público sujeito à disciplina judiciária.

Já no âmbito civil, a solicitação de perícia é iniciada na petição inicial ou na contestação, prosseguindo com o requerimento específico e justificado da fase

ordinatória. E é de responsabilidade das partes a fazer requisição, especificar o tipo de perícia e o objeto de prova, conforme Dinamarco (2005).

Na esfera civil é possível também a utilização do depoimento de testemunhas técnicas, considerada prova atípica.

Dinamarco (2005) indica que a perícia pode consistir de:

a) Exames – exames efetuados sobre pessoas, móveis, semoventes, papéis ou livros mercantis;

b) Vistorias – diligências para inspeção ou exame ocular, incidem sobre imóveis;

c) Avaliações – medições ou orçamentos sobre coisas em geral;

d) Arbitramentos – têm por objeto os serviços ou os valores indenizatórios.

A perícia não é realizada somente como exigência de processos judiciais penais ou cíveis, ela pode ser também contratada independentemente, através da perícia extrajudicial, cujo objetivo é a obtenção do parecer técnico para esclarecimento e orientação sobre determinado fato, na definição de Cabral (2003).

Nas corporações, no que se refere à informática, esse tipo de perícia pode ser iniciada a partir da detecção ou suspeita de incidentes computacionais. No decorrer das atividades investigativas e periciais, pode-se identificar a necessidade do acionamento de autoridades policiais ou judiciárias, levando-se à abertura de ações judiciais.

Nos Estados Unidos, durante a reunião inicial entre o procurador e o juiz é determinada a necessidade, o tipo e escopo da perícia, conforme requisitos da lei federal 16, segundo Cecil e Schwarzer (2000).

Na opinião de Casey (2004), os órgãos policial e judiciário estão tendo acesso a vestígios e indícios digitais em suas atividades, numa proporção gradativamente maior. E além disso, muitas organizações estão dando uma maior importância aos procedimentos de processamento dos vestígios digitais, de forma que possam constituir prova, e serem admissíveis se apresentados em juízo.

De acordo com Vacca (2005), os indícios digitais podem ser utilizados nas seguintes situações:

a) Em processos criminais, como por exemplo, em pedofilia;

b) Em processos cíveis, como por exemplo, em casos de quebra de sigilo comercial;

c) Em perícias de companhias seguradoras, como por exemplo, para avaliação de risco;

d) Por corporações, para investigações internas, como por exemplo, para casos de contrafação de banco de dados;

e) Por organizações policiais em procedimentos de busca e apreensão;

f) Por particulares, para confirmar ou refutar alegações.

Existem conceitos específicos nos processos investigativos e periciais que podem ser usados de forma específica nos procedimentos da polícia, do judiciário e da perícia.

Entretanto, não há um consenso entre os profissionais das diversas áreas que de alguma forma lidam com as atividades investigativas e periciais em informática, sobre o padrão a ser adotado no que se refere principalmente aos termos prova, evidência, vestígio e indício.

Isso ocorre tanto nos Estados Unidos, conforme Casey (2004) e Carrier (2006), quanto no Brasil, onde segundo Dinamarco (2005), existem traduções equivocadas de documentos do idioma inglês.

3 A CONTEXTUALIZAÇÃO DA PERÍCIA DE INFORMÁTICA

Nesse capítulo, as diferenças conceituais entre os vestígios físicos e digitais são abordadas procurando-se clarificar as questões que aparentam ser exclusivas dos materiais digitais ou da perícia computacional.

Além disso, essa distinção pode auxiliar no definição da estratégia a ser adotada principalmente no processo de coleta do processo investigativo.

Um breve histórico do processo investigativo e pericial em informática é apresentado de forma a se compreender a evolução dos delitos de informática, assim como da investigação e perícia.

E finalmente são apresentados os desafios postos à investigação e perícia computacional que podem determinar a diferenças relevantes com relação aos princípios gerais da investigação e ciência forense, principalmente no que se refere a tempo e recursos dispendidos no processo.

3.1 A Diferença Entre os Vestígios Físico e Digital

A perícia computacional é eventual e equivocadamente encarada de forma diferente das demais modalidades de perícia. Para Kruse e Heiser (2001), isso se deve à falta de familiaridade com a perícia computacional e com a informática em si.

Apesar de parecer que a fragilidade e a volatilidade sejam características exclusivas do vestígio digital, assim como o desafio nos procedimentos periciais e a exigência de rigor científico no procedimento, isso ocorre também em outros ramos da perícia.

Nas perícias de reconhecimento de identidade por voz, por exemplo, vários fatores influenciam negativamente na qualidade final do vestígio coletado. O desafio desse tipo de perícia está no procedimento adotado para o registro do vestígio, o que poderá determinar a qualidade do indício e consequentemente da prova, segundo Meuwly (2001).

Nesse sentido também, Smith e Bace (2003) lembram que as cortes americanas têm questionado a fundamentação científica do processo de análise de

vestígios, como é o caso das impressões digitais para o reconhecimento da identidade de suspeitos, principalmente após a adoção dos critérios Daubert.

Conforme Casey (2004), o computador pode ser utilizado de várias formas num crime, como local ou instrumento do crime e por isso, os vestígios gerados podem ter forma e apresentação diversas.

Os procedimentos para o processamento de vestígios físicos e digitais são muito distintos, e essa distinção pode determinar a estratégia de busca e apreensão e da própria investigação.

Por essa razão, o Departamento de Justiça dos Estados Unidos (USDOJ) adotou em 1994, uma categorização que faz a distinção entre os vestígios físico e digital.

Casey (2004) detalha a categorização definida pelo U.S. DOJ (2002), subdividindo-as entre hardware e informação, de acordo com o papel que o item desempenha no crime e com o processo de busca e apreensão adotado nos Estados Unidos:

a) *Hardware como ilícito*: equipamento de posse proibida. Exemplo: telefones celulares clonados e os computadores utilizados para clonálos;

b) *Hardware como fruto de crime*: resultante de atividades criminosas. Exemplo: computadores roubados ou adquiridos com cartão de crédito roubado;

c) *Hardware como instrumento*: equipamentos utilizados para perpetração ou promoção de ações criminosas. Exemplo: computador utilizado para observação, aquisição e transmissão de imagens de pornografia infantil;

d) *Hardware como indício*: equipamentos que por fatores específicos ou características peculiares podem ser ligados a algum elemento do crime. Exemplo: scanner de imagens utilizado para digitalizar imagens que possui características únicas que podem ligar o equipamento às imagens;

e) *Informação como ilícito*: informação de posse proibida. Exemplo: arquivos de imagens de pornografia infantil;

f) *Informação como fruto de crime*: resultante de atividades criminosas. Exemplo: cópia ilegal de programas;

g) *Informação como instrumento*: informação utilizada para perpetração ou promoção de ações criminosas. Exemplo: programas usados para invadir sistemas;

h) *Informação como indício*: indícios digitais em geral. Exemplo: atividades relacionadas ao crime registradas no registro de eventos de sistemas.

Nessa classificação, Casey (2004) adiciona a categoria hardware como indício à definição do documento do U.S. DOJ (2002).

Nesse trabalho, foi adotado o substantivo *ilícito* em substituição ao termo original em inglês "*contraband"* utilizado no manual Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations do U.S. DOJ (2002), de forma a ser evitada a associação à acepção de contrabando como o "ato de importar ou exportar mercadorias proibidas", Houaiss (2006).

3.2 Perícia Computacional

Como as outras áreas da ciência forense, a perícia computacional envolve a utilização de técnicas que permitam a coleta e preservação dos vestígios e a precisão nos resultados de seu processamento, possibilitando a admissibilidade dos indícios resultantes desses procedimentos, de acordo com Marcella e Greenfield (2002).

A perícia computacional é incipiente se comparada a outros ramos da ciência forense e ainda não é reconhecida como uma disciplina científica formal, segundo Nolan et al (2005).

3.2.1 Histórico

Os primeiros crimes relacionados a computadores datam dos anos 1969 e 1970, em crimes “físicos”, quando estudantes universitários queimaram computadores em protesto.

Nessa mesma época, foi registrada uma evolução no que se refere ao tipo de ataque, ao se descobrir como ganhar acesso a computadores. O uso não-autorizado de tempo de máquina não constituía crime nos Estados Unidos na época, de acordo com Casey (2004).

A expansão da Internet no início dos anos 1990 abriu novos meios e oportunidades para a ações criminosas envolvendo informática.

Em resposta a essa evolução, nessa mesma época, as agências policiais nos Estados Unidos e outros países iniciaram um processo de capacitação e especialização.

Inicialmente, foi criada uma equipe de contato inicial com o crime, que recebeu fundamentos básicos para coleta e exame de vestígios digitais, e contava com a assistência de laboratórios regionais e nacionais para os casos de maior complexidade.

Essa é uma abordagem encontrada em alguns países, como será verificado posteriormente nesse trabalho, cujo desafio está no rápido desenvolvimento da tecnologia, criando-se uma necessidade de especialização constante.

Casey (2004) reforça que essa divisão dos papéis separando-os em atividades iniciais de coleta, de exames laboratoriais e de investigação, facilitam a definição de padrões e consequentemente de programas de treinamento, como é o caso da iniciativa internacional do guia da ENFSI, que será abordada posteriormente nesse trabalho.

A forense computacional tem evoluído significativamente. Até pouco tempo atrás, era comum se trabalhar diretamente nos sistemas afetados, não se tomando precauções adequadas para a preservação dos vestígios.

Isso devido ao desconhecimento da importância da manutenção da confiabilidade dos materiais e procedimentos e dos requisitos de admissibilidade, ainda que existissem ferramentas que possibilitassem tais precauções.

A partir da década de 1990 se iniciou o desenvolvimento de ferramentas comerciais especializadas, como o Safeback, Maresware e NTI.

Num segundo momento, os procedimentos passaram a se voltar praticamente aos dados persistentes, ou seja, dados armazenados em discos rígidos locais ou outras mídias que poderiam ser recuperados caso o computador fosse desligado, negligenciando-se vestígios importantes provenientes de dados voláteis.

Segundo Casey (2004), em decorrência da complexidade dos sistemas de computadores atualmente, é difícil eliminar ou mensurar erros e incertezas, o que é importante em termos da admissibilidade da prova, em especial nos Estados Unidos.

3.2.2 Desafios da Perícia Computacional

De acordo com Casey (2004), vários são os desafios postos à Perícia Computacional.

Dentre eles está a forma na qual se apresenta o vestígio digital. As informações são dispostas no disco rígido de forma descontínua e apenas pequena parte delas pode ter relevância no caso.

Para interpretá-las, seria necessário identificar as partes úteis, juntá-las e traduzi-las de forma que possam ser interpretadas.

Não obstante, as tecnologias de armazenamento e mídias atualmente possibilitam uma grande capacidade de armazenamento. Em se tratando de grandes volumes de dados, tirar uma cópia pericial pode ser uma tarefa impraticável.

Outro fator desafiador é a dificuldade de contextualizar o vestígio ou o indício no crime, de forma a entender a relevância no todo, visto que geralmente são uma abstração de algum evento ou objeto.

Além disso, um terceiro fator é a facilidade de acesso e manipulação dos vestígios, permitindo alterações intencionais ou não, sem deixar sinais aparentes dessa alteração. Nesse sentido, as precauções e procedimentos adequados são imprescindíveis para a credibilidade do processo investigativo e pericial e para reforçar a idoneidade da prova.

A distribuição e dispersão geográfica que as redes de computadores constituem um outro fator crítico: os componentes da rede podem estar espalhados em vários pontos, ou seja, dispersos em diversos prédios que podem estar localizados em várias partes da cidade, do país ou ainda em vários países.

Tanto a dispersão das redes de computadores quanto os grandes volumes de dados, são fatores que podem ocasionar dificuldades no processo investigativo e pericial, podendo levar a um aumento do tempo gasto e de recursos alocados para esse trabalho.

A volatilidade das informações contidas num sistema é um fator importante no processo pericial digital, que deve ser considerado desde o primeiro contato com o local do crime e que pode determinar a estratégia pericial.

Ignorar as informações voláteis ou tratá-las de forma incorreta pode ocasionar a perda de informações relevantes ao caso investigado.

As informações voláteis são informações armazenadas em memória ou em trânsito que podem ser perdidas ao se desligar o computador. Estão incluídas, nessa categoria, informações presentes em registradores, cache e memória RAM.

A perícia tradicional preconiza o uso de cópia exata do sistema e seus dados, de forma a preservar os vestígios, permitindo revisões posteriores.

Por isso, até pouco tempo atrás, a perícia computacional lidava somente com dados persistentes, ou seja, dados armazenados em discos rígidos e por isso, muitos dos testes científicos publicados até o momento lidam praticamente só com esse tipo de dado. Informações voláteis importantes ao processo investigativo eram negligenciadas.

O desafio está em se definir procedimentos de coleta e preservação de vestígios sem violar o local do crime ou perder dados voláteis.

Farmer e Venema (2007) defendem que é melhor se obter uma melhor compreensão do cenário do incidente, em detrimento da certeza dos dados coletados e armazenados, através do uso de procedimentos consistentes, sugerindo também ferramentas de automatização. Pedro L. P. Sanchez, em sua revisão técnica da obra, lembra que o processo automatizado pode agilizar o trabalho, mas

em decorrência da configuração padronizada, detalhes importantes podem ser perdidos.

4 PADRONIZAÇÕES E PROCESSOS INVESTIGATIVOS

Um fator que pode afetar a admissibilidade é a falta de métodos e padronizações. Uma das questões fundamentais da admissibilidade da prova é a idoneidade dos procedimentos, desde a coleta de dados até a constituição da prova.

Na opinião de Casey (2004), a falta de padronização pode ocasionar erros de procedimentos e interpretação, podendo levar ao comprometimento da investigação ou do caso em si.

Procurou-se então, identificar iniciativas de padronização e recomendações existentes para a manipulação de vestígios.

4.1 Padronizações

Da pesquisa, foram identificados alguns documentos que foram divididos entre os padrões voltados para as atividades de contato inicial (incluem atividades de coleta e preservação com contato inicial com as fontes de prova) e atividades periciais (exames dos vestígios coletados, em geral composto de procedimentos laboratoriais).

Atividades de Contato Inicial (Organizações Policiais e empresas):

a) RFC 3227 – Coleta e Preservação de Vestígios;
b) Guia de Melhores Práticas para Vestígios Eletrônicos baseados em Computador da ACPO (Association of Chief Police Officers) ;
c) Princípios do G8;

Atividades Periciais:

a) Guia de Melhores Práticas de Exame Pericial em Tecnologia Digital da ENFSI;
b) CTOSE Cyber Tools On-Line Search for Evidence;

4.1.1 RFC 3227 - Coleta e Preservação de Vestígios

A RFC 3227 é uma recomendação voltada ao público técnico que tenham contato inicial com o incidente, como os administradores de sistemas que participam do processo de coleta e armazenamento dos vestígios no processo de tratamento de incidentes de segurança.

De acordo com os autores, a RFC 3227 deve ser utilizada como base nos procedimentos de coleta e armazenamento de vestígios e devem ser incorporados ao processo de tratamento de incidentes.

O documento é composto de 12 princípios:

a) Estar de acordo com as políticas de segurança da organização e engajar as equipes de tratamento de incidentes e jurídico no processo;

b) Capturar imagem do sistema, o quanto mais precisa possível;

c) Manter anotações detalhadas, incluindo data e hora;

d) Documentar as diferenças de fuso horário identificadas;

e) Preparar-se para testemunhar sobre os procedimentos utilizados;

f) Minimizar o risco dos dados serem modificados;

g) Remover vias externas que possam ocasionar modificações;

h) Ao se deparar em situação de escolha entre coletar e analisar, deve-se optar por coletar primeiro e analisar depois;

i) Os procedimentos devem ser viáveis e devem ser testados. Se possível, os procedimentos devem ser automatizados para torná-los mais rápidos e precisos;

j) Deve ser adotado um procedimento metódico;

d) Coletar os dados em ordem de volatilidade, do mais ao menos volátil;

e) Efetuar cópias de disco em nível de bit para a preservação do original.

A RFC 3227 se refere à ordem de volatilidade, nos princípios e atividades principais, e lista um exemplo de itens do mais ao menos volátil, similar à tabela OOV de Farmer e Venema (2007):

a) registradores, cache;

b) tabela de roteamento, cache da tabela arp, lista de processos, estatísticas do kernel;

c) memória;

d) arquivos temporários;

e) discos;

f) registro de eventos;

g) configuração física e topologia da rede;

h) mídias de backup.

O documento recomenda evitar procedimentos que podem destruir os vestígios inadvertidamente:

a) Não reinicializar ou desligar os equipamentos antes da coleta de vestígios;

b) Não confiar nos programas do sistema afetado e utilizar ferramental apropriado a partir de mídias protegidas;

c) Não utilizar programas invasivos que podem modificar a data e hora de acesso dos arquivos;

d) A desconexão de conectores que ligam o equipamento à rede a qual está conectado pode ativar algum mecanismo que possa destruir o vestígio.

No que se refere à privacidade, recomenda que deve ser dada atenção às normas de privacidade da empresa e à legislação local, de forma que não sejam conduzidas atividades intrusivas à privacidade das pessoas sem forte justificativa e que a empresa dê respaldo ao procedimento de coleta de vestígios do incidente.

A única referência que o documento faz quanto ao aspecto legal, está relacionado às características que os vestígios devem possuir:

a) Admissibilidade: as leis e normas aplicáveis devem ser obedecidas;

b) Autenticidade: o vestígio deve estar relacionado ao incidente;

c) Completa: deve apresentar a visão completa e não somente perspectiva do fato;

d) Confiabilidade: não deve ser suscitadas dúvidas quanto à autenticidade do vestígio em decorrência dos procedimentos adotados;

e) Credibilidade: deve ser crível e compreendida no tribunal.

A RFC 3227 recomenda que os procedimentos sejam detalhados evitando-se ambigüidades. Os métodos utilizados devem ser claros e reprodutíveis, de forma que seja possível a condução de testes por especialistas sobre os métodos adotados.

De acordo com esse documento, a coleta deve ser efetuada conforme os passos:

a) Levantamento dos sistemas envolvidos no incidente, de onde os vestígios serão coletados;

b) Estabelecer o que pode ser relevante ou admissível;

c) Estabelecer a ordem de volatilidade;

d) Remover conexões externas que permitam alterações;

e) Efetuar a coleta dos itens mais aos menos voláteis;

f) Registrar as diferenças de horário;

g) Checar o que pode adicionalmente ser vestígio durante o processo de coleta;

h) Documentar todos os passos;

i) Documentar as atividades dos usuários no incidente.

Gerar checksums e assinar criptograficamente os vestígios de forma a assegurar sua autenticidade. Após esses passos, os vestígios devem ser protegidos e todos os procedimentos documentados através da cadeia de custódia (chain of custody).

Na cadeia de custódia são registradas as informações sobre o local, data e responsáveis pelos procedimentos de identificação, coleta e análise dos vestígios, assim como da custódia de tais materiais.

Os vestígios devem ser armazenados em tipos de mídias conhecidas e o acesso a elas, deve ser extremamente restrita e documentada, recomendando ainda a utilização de mecanismos de detecção de acesso não autorizado.

Recomenda procedimento operacional, como a criação de mídia como cd, com acesso somente de leitura com ferramentas que podem ser utilizadas no processo de coleta e análise de vestígios com ferramentas que permitam analisar processos, estado do sistema, copia bit a bit, geração de checksum e de imagens e scripts para automatizar o processo.

Essas ferramentas não devem solicitar ou se conectar a qualquer outro código que não esteja na mídia.

4.1.2 ACPO (Association of Chief Police Officers)

O Guia de Melhores Práticas para Tratamento de Vestígios Eletrônicos baseados em Computador é um documento desenvolvido pela ACPO (Association of Chief Police Officers), utilizada por organizações britânicas de abrangência nacional, direcionado a agentes policiais.

Com o intuito de cooperação internacional, esse documento é consistente com os princípios definidos pelo grupo de trabalho do G8.

De acordo com ACPO (2007), são aplicadas as mesmas regras e legislações tanto às provas documentais quanto às digitais no Reino Unido. O ônus da autenticidade da prova é da promotoria.

O documento define 4 princípios:

a) Nenhuma ação tomada deve alterar os dados do computador ou das mídias que podem constituir prova.

b) Em circunstâncias excepcionais que exijam a manipulação do vestígio original, essa tarefa deverá ser efetuada por pessoal competente e que

esteja habilitado a explicar a relevância e implicações das ações tomadas.

c) Devem ser estabelecidas e preservadas trilhas de auditoria em todos os processos aplicados aos vestígios digitais.

d) O encarregado pela investigação será responsável pela aplicação e cumprimento de desses princípios e das legislações aplicáveis.

O documento recomenda procedimentos operacionais de coleta e busca, listando atividades a serem adotada para máquinas ligadas e desligadas.

Para máquinas desligadas, o documento recomenda:

a) Resguardar o local onde encontra-se o equipamento que pode ser suporte de prováveis vestígios;

b) Deixar que impressoras terminem a impressão;

c) Afastar as pessoas dos equipamentos e dos suprimentos de energia;

d) Não ligar os equipamentos em hipótese alguma;

e) Certificar-se de que o computador esteja realmente desligado;

f) Abrir computadores móveis para certificar-se de que estão desligados;

g) Remover a bateria dos computadores móveis;

h) Desconectar os cabos de força e outros periféricos;

i) Etiquetar, fotografar ou filmar todos os componentes no local onde se encontravam;

j) Etiquetar portas e cabos conectados;

k) Remover cuidadosamente os equipamentos e identificar cada componente;

l) Assegurar que todos os itens foram identificados e etiquetados;

m) Procurar por diários, cadernos e papéis que possam fornecer senhas;

n) Perguntar aos usuários por senhas e caso de obtê-las, registrá-las adequadamente;

o) Documentar detalhadamente todos os procedimentos adotados.

Quando as máquinas estiverem ligadas o documento recomenda:

a) Resguardar o local onde encontra-se o equipamento, suporte que contém prováveis vestígios;
b) Afastar as pessoas dos equipamentos e dos suprimentos de energia;
c) Desconectar modem;
d) Caso o equipamento esteja conectado, deve ser solicitado o apoio de especialistas;
e) Não confiar nas instruções de usuários ou proprietários dos equipamentos;
f) Etiquetar, fotografar ou filmar todos os componentes no local onde se encontravam;
g) Remover todos os cabos de conexões que possam conduzir a conectores e equipamentos;
h) Remover cuidadosamente os equipamentos e identificar cada componente;
i) Assegurar que todos os itens foram identificados e etiquetados;
j) Deixar que o equipamento resfrie antes de removê-lo;
k) Procurar por diários, cadernos e papéis que podem fornecer senhas;
l) Perguntar aos usuários por senhas e caso de obtê-las, registrá-las adequadamente;
m) Documentar detalhadamente todos os procedimentos adotados;
n) Registrar o conteúdo da tela, através de fotografia e anotações;
o) Não tocar no teclado ou no mouse caso proteção de tela esteja ativada, exceto se o perito ou investigador encarregado decida verificar o conteúdo da tela;
p) Se não houver disponibilidade de peritos, desligue o equipamento desconectando o cabo de força direto da CPU, sem fechar os

programas. Esse procedimento poderá acarretar a perda de alguns vestígios, mas assegurará a integridade das informações.

Materiais que devem ser apreendidos para a extração de vestígios:

a) CPU;
b) Teclado e mouse;
c) Conectores;
d) Fontes;
e) Discos rígidos não instalados no computador
f) Hardlocks;
g) Modem;
h) Drives e periféricos externos;
i) Cartões de rede sem fio;
j) Câmeras digitais;
k) Disquetes;
l) Fitas de backup;
m) Cartuchos jaz/zip;
n) CD;
o) DVD;
p) Discos Rígidos não conectados ao computador;
q) Cartões PMCIA;
r) Cartões de memória e pen drives;

Com o objetivo de auxiliar nas análises recomenda também apreensão de:

a) Manuais;
b) Qualquer material que possa conter senha;
c) Chaves;

Para o exame e comparações de materiais impressos, recomenda também a apreensão de impressoras, impressos e papéis.

Os Pdas e agendas eletrônicas podem ser suportes importantes de vestígios. Porém, os procedimentos para a coleta e exame desses equipamentos e a aplicação dos princípios diferem quando comparado aos PCs.

É maior a dificuldade em se preservar sua integridade, visto que muito provavelmente o equipamento deverá ser ligado para o exame, tomando-se o cuidado para não alterar as informações em memória.

Se o pda for encontrado ligado, ele deverá ser desligado para que a bateria seja poupada e a data/horário deve ser registrada.

Outros equipamentos eletrônicos que podem conter vestígios:

a) Celulares;

b) Pagers;

c) Telefones;

d) URAs;

e) Facsimile;

f) Gravadores de voz;

g) Câmeras digitais;

h) Celulares com acesso Internet;

i) TV digital com acesso Internet.

Faz considerações quanto à coleta de impressões de digitais e de materiais para testes de DNA que possam ser encontrados nos equipamentos e que porventura sejam necessários à investigação, lembrando que algumas das técnicas, como o uso de pó de alumínio, podem afetar o equipamento.

4.1.2.1 Procedimentos de Busca

A ACPO (2007) Recomenda que seja verificado se são necessárias providências especiais antes de iniciar a busca e apreensão.

4.1.2.2 Procedimentos Pré-busca

A ACPO (2007) recomenda que seja obtida a maior quantidade de informações possível relacionados ao tipo, localização e conexão dos computadores de forma a se definir uma estratégia de busca, considerando-se a complexidade do ambiente.

Os investigadores devem considerar no processo de busca e apreensão, a disponibilidade de especialistas que possam dar suporte no processo.

A equipe de busca deve ser informada previamente sobre a inteligência, informações, logística e também sobre procedimentos com relacionados à informática.

A equipe deverá ser instruída a tratar as salvaguardar os vestígios digitais como os demais tipos de vestígio, e evitar o comprometimento do material por desconhecimento de procedimentos.

Esse guia também faz referência às ferramentas que podem ser utilizadas nesse processo como:

a) Chaves de fenda, philips, alicates pequenos, alicates de corte para a remoção de fixadores de fios;
b) Registro de propriedade;
c) Etiquetas e fitas para marcar e identificar os componentes;
d) Etiquetas de exibição;
e) Fitas para proteção dos cabos;
f) Flat pack assembly boxes;
g) Canetas – marcadores;
h) Câmeras de fotografia e vídeo;
i) Celulares.

O que deve ser registrado:

a) Croqui do local do crime;
b) Detalhes das pessoas presentes onde os computadores foram localizados;

c) Detalhes dos computadores – marca, modelo, número serial;

d) Detalhes do monitor e periféricos conectados;

e) Comentários fornecidos pelo(s) usuário(s) do computador(es);

f) Ações tomadas no local da cena indicando o horário exato.

De acordo com o documento, a recuperação de vestígios é um procedimento que deve ser executado por pessoal especializado. O processo é composto de 4 fases: coleta, exame, análise e relatório. O documento foca no processo de coleta.

4.1.2.3 Fase de coleta

A fase de coleta envolve a procura, reconhecimento, coleta e documentação de vestígios eletrônicos. Na fase de coleta informações relevantes podem ser perdidas se não forem seguidos procedimentos adequados.

A fase de exame auxilia a tornar o vestígio visível e a explicar sua origem e significância.

Uma vez que a informação tornou-se visível, inicia-se o processo de redução, onde são separadas as informações relevantes na investigação. Esse processo é importante em decorrência da grande quantidade de informações que pode ser armazenadas em mídia.

4.1.2.4 Fase de análise

Nessa fase são analisados os produtos da fase de exame quanto ao valor probatório e significância no caso.

4.1.2.5 Fase de relatório

Completa o processo de exame, revisando o processo e os dados pertinentes recuperados. As anotações devem ser preservadas e mantidas em sigilo. O examinador pode ser chamado a testemunhar quanto ao procedimento executado, à

validade do procedimento e competência do examinador. Na Escócia, as anotações são preservadas como prova a serem apresentadas em tribunal.

O papel do examinador é obter uma cópia fiel do material apreendido que deve ser obtido sem o comprometimento do original. Por isso deve-se tomar cuidado na seleção das ferramentas.

Os princípios da perícia devem ser aplicados, como a documentação de todas as ações tomadas. A disponibilização das documentações pode ser necessária para o exame e validação das ações executadas. Os autores frisam também que em decorrência das atualizações no âmbito legal, é importante ficar atento aos requisitos legais, incluindo-se as práticas e resultados de casos recentes e de precedentes abertos, principalmente no que se refere à Internet.

4.1.2.6 Controle sobre o material coletado

O documento reforça a importância de que os vestígios sejam preservados, recuperados e armazenadas de uma forma sistemática e correta de forma a manter a segurança, a integridade e a continuidade dos vestígios, o que possibilitará que o vestígio mantenha-se intacto e posteriores críticas e refutações ocorram nos tribunais.

4.1.2.7 Controle sobre material de pedofilia

A ACPO (2007) recomenda precauções ao lidar com material de pedofilia. O simples fato de se portar imagens pode ser considerado crime. Além disso, a confidencialidade sobre o material é de extrema importância, uma vez que pode conter informações pessoas e inclusive a identidade da vítima.

Recomenda a utilização de senha e criptografia nas mídias de vestígios duplicadas e controle rígido sobre o material impresso.

4.1.2.8 Acesso da Defesa

Após a acusação, a defesa possui permissão de visualização das imagens. O acusado, no entanto, só poderá ter acesso às imagens na companhia do

representante legal. Em nenhuma circunstância o acesso ao material ocorrerá em local que não sejam instalações judiciárias ou policiais. Na Escócia esse procedimento é conduzida através do Fiscal Procurador.

Não é permitido à defesa fazer cópias ou imagens do material e só é possível a exceção através de determinação do juiz ou magistrado alocado ao julgamento. Essa exceção não é válida na Escócia.

A defesa pode solicitar acesso tanto ao disco rígido quanto à imagem recolhidos pela polícia para verificação da integridade dos vestígios e dos padrões contra as alegações. Na Escócia é necessária a presença do perito nos estabelecimentos da polícia, em condições controladas e não é permitida nenhum tipo de cópia.

4.1.2.9 Audiências

Durante a audiência preliminar, normalmente não há a apresentação do material do disco. Nas audiências posteriores, devem ser seguidos os procedimentos e o oficial responsável deverá manter o controle sobre o material e retorná-lo ao local de armazenamento após o exame.

4.1.2.10 Encaminhamento para Julgamento

Raramente ocorre a apresentação do material, exceto se a defesa quiser alegar que a acusação é improcedente.

4.1.2.11 Audiência de Acordo

Nesse procedimento, o responsável ou o perito ficarão à disposição para a elucidação de questões técnicas.

4.1.2.12 Julgamento

Nesse procedimento, o responsável ou o perito apresentará as imagens como prova no tribunal.

O Criminal Procedure and Investigations Act 1996 (CPIA), vigente a partir de 1997, estabelece regras de divulgação do material coletado.

4.1.2.13 Manuseio de celulares

Esse documento faz recomendações para o manuseio de celulares. Antes do análise do celular em si, o documento recomenda que seja avaliado se há a necessidade de coleta de outros tipos de vestígios que não sejam digitais, como impressões digitais, DNA, drogas, etc.

Caso não haja a necessidade de acompanhamento de alguma atividade investigativa, o celular deverá ser desligado e embalado em caixa rígida e etiquetada.

4.1.3 Princípios do G8

Em uma iniciativa de possibilitar a cooperação internacional, o G8 (Grupo dos 8, formado pela Alemanha, Canadá, Estados Unidos, França, Itália, Japão, Reino Unido e Rússia) designou a IOCE (International Organization on Computer Evidence) para desenvolver princípios comuns a serem adotados nos procedimentos relacionados aos vestígios digitais.

Os seguintes princípios foram definidos:

a) Ao lidar com vestígios digitais, todos os princípios da perícia geral devem ser aplicados;

b) As ações tomadas durante a coleta dos vestígios digitais não devem alterá-los;

c) Quando for necessário acessar os vestígios digitais originais, o procedimento deverá ser realizado por pessoal treinado para essa finalidade;

d) Todas as atividades relacionadas à coleta, acesso, armazenamento ou transferência dos vestígios digitais devem ser totalmente documentados e preservados e devem ficar à disposição para revisões;

e) Todas as ações tomadas sobre o vestígio digital será de responsabilidade do oficial que estiver com sua posse;

f) Quaisquer agências responsáveis por coleta, acesso, armazenamento ou transferência de vestígios digitais são responsáveis pelo cumprimento desses princípios.

4.1.4 CTOSE

O programa de Tecnologias da Sociedade da Informação da Comissão Européia patrocinou o projeto CTOSE (Cyber Tools On-line Search for Evidence), cujo objetivo era o de desenvolver metodologia, arquitetura, modelo de processo e um conjunto de ferramentas e procedimentos comuns para a investigação eletrônica, voltada aos investigadores oficiais (policial e judiciário) e particulares, bem como para profissionais do campo jurídico.

Ao final do projeto em 2003, foram gerados os seguintes produtos que podem ser utilizados pelos profissionais envolvidos no processo de investigação e perícia:

a) Modelo de Metodologia CTOSE;

b) Consultor Jurídico;

c) Modelo de Processo;

d) C*CAT – Cyber Crime Advisory Tool;

e) Guias de Prontidão Forense;

f) Ferramenta de Autopsia forense;

g) Demonstrador CTOSE;

h) Story Board do projeto.

4.1.4.1 Modelo de Metodologia CTOSE

O Modelo de Metodologia CTOSE dá embasamento aos outros componentes gerados nesse projeto é a fundação para a produção dos outros itens descritos. Foi definido um ciclo evidenciário, composto das seguintes fases:

a) Processamento – Estado de pronto onde as transações e interações estão acontecendo, sem sinais ou atividades suspeitas aparentes;

b) Conscientização – Ocorrência de evento que inicia processo de análise de risco desse evento. Termina por voltar à fase de Processamento ou então de iniciar a próxima (Investigação);

c) Investigação – A fase é iniciada a partir da decisão gerencial e os procedimentos investigativos conduzidos por profissional especializado interno ou não à companhia;

d) Aprendizado – Considerada uma fase vital do modelo, após análise da ocorrência, as lições aprendidas devem ser incorporadas às medidas técnicas, aos procedimentos, documentos e planos.

Figura 1. Modelo de Metodologia CTOSE

4.1.4.2 O Consultor Jurídico

O Consultor Jurídico é uma ferramenta online composta de aconselhamento e melhores práticas de organizações jurídicas destinada aos investigadores para a tomada de decisões ou para obter suporte legal nos processos investigativos.

Os requisitos legais e o ônus da prova podem variar conforme o país e devido à natureza global da Internet, é possível que o investigador se depare com situações às quais não esteja familiarizado.

Organizações policiais e jurídicas, experientes na produção de provas, contribuíram para o desenvolvimento dessa ferramenta.

4.1.4.3 Modelo de Processo Investigativo

O Modelo de Processo Investigativo está focado no processo de aquisição de provas e é composto de cinco fases:

a) Preparação;

b) Processamento;

c) Levantamento;

d) Investigação;

e) Aprendizado.

Este modelo disponibiliza um guia de ações e decisões a serem considerados em caso de incidente. Em cada passo descrito, são disponibilizadas informações adicionais que incluem funções, conhecimento necessário e aconselhamento legal.

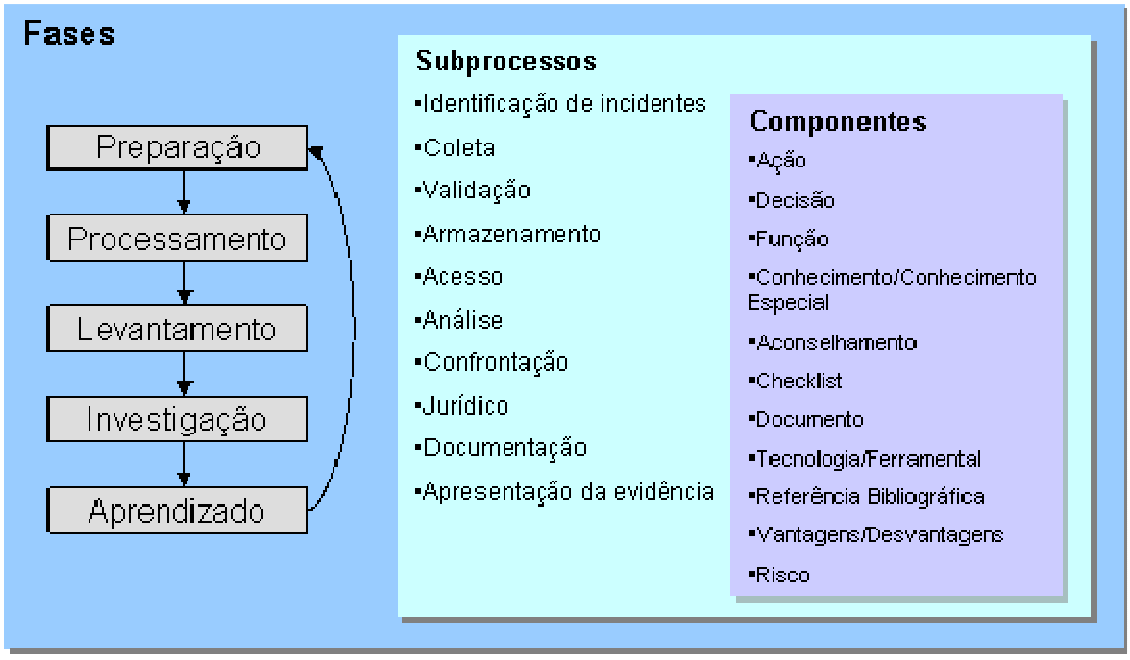

Figura 2. Modelo de Processo Investigativo CTOSE

4.1.4.4 C*CAT – Cyber Crime Advisory Tool

O C*CAT – Cyber Crime Advisory Tool é a ferramenta desenvolvida para dar suporte ao modelo de processo.

Essa ferramenta permite ao usuário inicialmente definir a situação e então apresenta as ações e decisões necessárias. A cada caso, a ferramenta permite ao usuário obter aconselhamentos e dicas. As tarefas executadas são documentadas e em decorrência, os procedimentos devem ser seguidos a risca para que a integridade da cadeia de custódia seja mantida.

4.1.4.5 Guias de Prontidão Forense CTOSE

Os Guias de Prontidão Forense CTOSE reforçam um aspecto da fase de preparação que são os procedimentos preventivos que permitem que as organizações assegurem uma melhor chance de obter provas admissíveis.

4.1.4.6 Ferramenta de Autopsia Forense

Ferramenta de Autopsia Forense - (Forensic Autopsy Tool – FAT) foi criado para tratar de aspectos legais relacionados às provas e autenticá-las como autêntica, completa e confiável.

4.1.4.7 Demonstrador CTOSE

O Demonstrador CTOSE mostra a metodologia aplicada numa formatação comercial em cenários de ataque, demonstrando como o ataque pode ser investigado e atribuído ao atacante.

4.1.5 ENFSI

A ENFSI (Working Group Forensic IT) é uma organização européia que desenvolveu Guia de Melhores Práticas de Exame Pericial em Tecnologia Digital, como membro da IOCE, seguindo tanto os princípios da IOCE como os da G8. Este documento, no entanto, foca a fase de exame e dá direcionamento aos laboratórios membro da ENFSI.

Um dos principais objetivos desse material em termos de padronização é definir uma estrutura e procedimentos padrão que cumpram com os requisitos da ISO 17025 (aplicada a laboratórios), implantando esses requisitos em laboratórios forenses e facilitando a troca de informações entre tais laboratórios.

Esse documento cobre os requisitos de garantia de qualidade, recomendações para definição de requisitos dos clientes de forma a ajustar cronograma, tarefas relacionadas ao levantamento do caso, priorização das atividades de exame e recomendação de procedimentos específicos, desde a análise do local do crime até a apresentação das provas nos tribunais.

4.1.5.1 Garantia de Qualidade

O Guia de Melhores Práticas de Exame Pericial em Tecnologia Digital faz recomendações sobre a organização de pessoal em um laboratório forense, programa de aperfeiçoamento de pessoal, qualidade de documentação, equipamentos, software, e das instalações do laboratório, procedimentos de validação e auditoria.

O guia indica as funções-chave que são usualmente encontradas nos laboratórios de perícias e define as respectivas qualificações e competências mínimas esperadas:

a) Gerente de Operações – Responsável pelo gerenciamento da qualidade do trabalho no laboratório. A recomendação do guia é que o gerente tenha formação superior na área ou seja especialista em tecnologia e vestígio digital, comprovado através de experiência e publicações e alto nível de conhecimento em procedimentos e tecnologias relevantes para o exame de hardware e software, além da habilidade de gerenciar recursos;

b) Relator – Responsável pelo exame, interpretação dos fatos, elaboração de relatórios e apresentação dos resultados em tribunal. A recomendação é a de que esse profissional tenha formação superior na área ou seja um especialista na área através da comprovação por revisão de pares ou publicações e que possua conhecimento em tecnologias e procedimentos relevantes, habilidade para demonstrar

teorias, competência para a avaliação dos vestígios no caso e experiência com procedimentos do sistema judiciário;

c) Especialista Técnico – perito com competência em serviços ou equipamentos específicos, responsável pelos relatórios sobre os fatos específicos de sua área de atuação. Conforme o guia, deve ter formação superior na área ou seja um perito comprovado através da comprovação por revisão de pares ou publicações e possua alto nível de conhecimento de procedimentos e tecnologias aplicáveis;

d) Assistente/Analista/Técnico – responsável por exames e trabalhos técnicos sob supervisão. A recomendação é a de que possuam conhecimento de teoria, procedimentos e tecnologias aplicáveis e conhecimentos práticos para a operação de ferramentas especializadas e conduzir exames de forma segura e confiável, de acordo com os protocolos do laboratório e dos requisitos legais.

O guia também recomenda que seja desenvolvido um plano de desenvolvimento e manutenção da capacitação da equipe e testes periódicos de comprovação de competência.

Nos mesmos moldes dos padrões de qualidade ISO, recomenda a utilização de sistema de gerenciamento de qualidade que faça o controle de todos os sistemas, processos e métodos utilizados no exame e elaboração de relatórios no laboratório. E também devem ser definidos os requisitos mínimos para a elaboração de relatórios.

A ENFSI recomenda que todos os equipamentos utilizados no laboratório sejam inventariados e mantidos em ótimas condições operacionais.

O laboratório deve se utilizar somente de procedimentos e técnicas validadas, sendo que a ENFSI define os requisitos mínimos para validação, como:

a) Definição da técnica ou procedimento necessários;

b) Aspectos críticos do procedimento de exame com a identificação e definição das limitações;

c) Demonstração de que os métodos, materiais e equipamentos a serem utilizados são adequados para cumprir os requisitos definidos;

d) Procedimentos adequados para assegurar o controle de qualidade;

e) Documentação completa do procedimento ou técnica;

f) Os resultados obtidos devem ser confiáveis e reprodutíveis;

g) A técnica ou procedimento foram submetidos a avaliação independente ou caso a técnica ou procedimento sejam novos, passem por revisão de pares;

h) Os examinadores devem demonstrar que são competentes no uso das técnicas ou procedimentos requeridos.

A ENFSI define requisitos para as ferramentas de geração de imagem de discos, como:

a) software não deve alterar o vestígio;

b) A ferramenta deve possuir um processo de checagem da imagem gerada e deve ser confiável;

c) As funções de registro de eventos deve ser detalhadas e precisas;

d) Se possível os resultados devem ser comparados com outro produto para geração de imagem.

E define também que para os demais tipos de ferramentas que possam ser utilizados no processo investigativo, deve ser estabelecido um plano para cada objetivo de uso da ferramenta no exame, de forma a garantir que a ferramenta é adequada e confiável.

Para as ferramentas que possibilitam customização, cada configuração utilizada na ferramenta e todos os passos seguidos no exame devem ser documentados.

As instalações do laboratório devem ser adequadas e periodicamente todos os aspectos do trabalho pericial deve ser auditado.

4.1.5.2 Requisitos do Cliente

A ENFSI recomenda que seja estabelecido um acordo com o requisitante da perícia e confirmada a finalidade do exame. Também aconselha que seja feito um planejamento de forma a levantar as prioridades do solicitante, os prazos que devem ser cumpridos e identificar quaisquer ressalvas que devem ser consideradas durante o trabalho.

4.1.5.3 Levantamento do Caso

Segundo a ENFSI, o relator deve fazer o levantamento das informações e materiais entregues à perícia, confrontando com o acordo estabelecido com o solicitante. O relator deve também levantar os riscos de contaminação antes de serem submetidos ao exame.

Quando necessário, o relator deve avaliar se o que o solicitante propôs procurar no exame pode ser testado e se os dados poderão ser preservados e disponibilizados para testes posteriores que venham a ser necessários.

Durante o levantamento do caso, o relator deverá, fazer uma pré-análise do que ele espera encontrar nos vestígios se cada proposição do solicitante estiver correta e para o levantamento da probabilidade de que posse acidental ou não intencional, para isso, sugere que sejam levantados:

a) Como era o uso do sistema computacional em questão antes, durante e depois do incidente e da apreensão;

b) Pessoas envolvidas;

c) Seqüência e horários de eventos;

d) Seqüência e horários de eventos da recuperação dos itens submetidos a exame.

O relator também deverá avaliar também qual a possibilidade de conseguir extrair e recuperar os vestígios digitais e analisar a sua relevância na proposição do solicitante.

4.1.5.4 Priorização

A ENFSI recomenda que antes do início do trabalho seja:

a) Estabelecida a urgência e prioridade junto com o solicitante da perícia;

b) Verificado se outros exames poderão ser necessários sobre os mesmos vestígios;

c) Avaliado que vestígios possuem o potencial de proporcionar a maior quantidade de informações em resposta às proposições do solicitante da perícia.

Além disso, sugere iniciar o exame nos vestígios que possam ter a maior relevância probatória e efetuar todos os exames necessários em um item antes de manipular outros vestígios para evitar a possibilidade de contaminação.

4.1.5.5 Princípios Gerais para o Tratamento de Vestígios Digitais

A ENFSI adota todos os princípios recomendados pelo G8, conforme a seção 4.1.3.

4.1.5.6 Práticas de Perícia Digital

Toda prática adotada deve obedecer aos princípios gerais, de acordo com a seção 4.1.5.5 e o laboratório deve estabelecer um manual de Procedimentos Operacionais Padrão e a ENFSI recomenda que nesse documento sejam incluídos como tópicos, os detalhes do procedimento de coleta, preservação e exame dos vestígios.

4.1.5.7 Localização e Coleta de Vestígios no Local do Crime

Conforme a ENFSI, o pessoal de perícia deve agir ou dar assistência no local do crime para a coleta de vestígios e deve estar ciente de que outros procedimentos e regras devam ser seguidos, como:

a) Precaução contra contaminações de vestígios;

b) Procedimentos de Busca;

c) Coleta de vestígios;

d) Embalagem, etiquetação e documentação dos vestígios coletados;

4.1.5.8 Exames Laboratoriais

A ENFSI recomenda que antes que as atividades laboratoriais se iniciem, sejam tomadas as precauções necessárias contra a contaminação.

Os vestígios encaminhados em embalagens violadas ou que possam ter a integridade comprometida devem ser recusados.

O planejamento das atividades periciais deve estar de acordo com o estabelecido pelo solicitante da perícia e deve ser adotada uma abordagem sistemática.

Os requisitos para o registro das informações da perícia pode variar conforme o sistema legal local, mas deve-se seguir um mínimo, de forma que qualquer outro técnico na mesma especialidade seja capaz de compreender o que foi feito e conseguir conduzir análises independentes sobre os mesmos vestígios examinados.

4.1.5.9 Avaliação e Interpretação

O processo de avaliação e interpretação das informações geradas no exame deve levar em consideração as proposições definidas no início dos trabalhos pelo requisitante da perícia. A ENFSI sugere utilizar a abordagem bayesiana para se calcular a probabilidade da ocorrência das hipóteses levantadas.

4.1.5.10 Apresentação do Indício

Os resultados obtidos na perícia, numa primeira instância, para o uso da polícia ou da promotoria, são disponibilizados geralmente na forma escrita.

O relatório deve prover as informações de forma clara, concisa, estruturada, não deve dar margem a interpretações ambíguas e deve atender aos requisitos legais locais.

Nas apresentações orais, a ENFSI recomenda que o testemunho fique restrito somente às informações obtidas no exame.

4.1.5.11 Revisão do Caso

Todos os trabalhos periciais estão sujeitos às revisões técnicas e administrativas. As revisões técnicas devem englobar a validade das informações obtidas na perícia e todo o procedimento deve ser documentado. As revisões administrativas incluem a validação do exame efetuado contra a proposição feita pelo requerente da perícia e do cumprimento das regras e procedimentos adotados pelo laboratório.

Todos os casos de prestações de queixa contra os procedimentos laboratoriais devem ser investigados, tomadas as providências necessárias de correção e conduzidas auditorias independentes, se considerado necessário.

4.1.5.12 Segurança

A ENFSI faz recomendações sobre a segurança no ambiente do laboratório que incluem a conscientização e divulgação de manuais de segurança no ambiente laboratorial e sobre os riscos os materiais a serem periciados podem ocasionar.

4.2 Processos Investigativos e Periciais

Nessa seção são levantados os processos executados nos primeiros níveis, ou seja, de contato inicial com o incidente e os periciais, de análise e exame por peritos nas diversas esferas de atuação.

Também são levantados os principios científicos e outros princípios e que devem ser aplicados nesses processos.

4.2.1 Princípios Científicos

De acordo com Casey (2004), a ciência forense proporciona uma gama de métodos e técnicas investigativas que possibilitam, entre outros fatores, reconstruir o crime, identificar suspeitos e entender as motivações para o cometimento do delito.

O uso dos princípios científicos para analisar vestígios, reconstruir crimes e testar hipóteses, possibilita ao investigador montar cenários mais sólidos e prováveis do ocorrido. Além disso, as ferramentas científicas podem dar assistência ao judiciário para a tomada de decisões em questões que envolvem tecnologia.

Nesse sentido, os Estados Unidos estabeleceram em 1923 o teste de Frye, o qual definia que para que a prova seja admissível, a técnica utilizada na perícia deve ser suficientemente sólida de forma que possua aceitação geral na comunidade científica no seu campo de conhecimento. O objetivo desse teste era evitar que teorias científicas controversas ou inadequadas fossem utilizadas nas perícias.

Frye foi criticado por ser muito rígido, impedindo que muitas provas fossem consideradas em julgamento e foi praticamente suplantado pelos critérios Daubert em 1993 e pela promulgação das Regras Federais de Provas (FRE – Federal Rules of Evidence) que adota os critérios Daubert.

Os critérios Daubert define alguns critérios que os juízes devem considerar ao apreciar as provas:

a) A técnica ou teoria científica foi revisada por pares ou publicada?

b) A técnica publicada é aceita pela comunidade profissional relevante?

c) A técnica ou teoria científica pode ser testada?

d) Qual é a taxa de erro?

Em decorrência desses princípios, o NIST (National Institute of Standards and Technology) definiu um grupo responsável por testes de ferramentas de forense computacional, mas as atividades são ainda incipientes e o foco principal desse grupo está em técnicas e ferramentas para análise de discos rígidos.

A aplicação de técnicas, ferramentas e a determinação das taxas de erro em testes, requeridos às provas cientificas nos procedimentos periciais são desafiadores para todas as disciplinas da ciência forense.

Existem também questões do ponto de vista dos juizes e Berger (2000) indica entre outros desafios, a dificuldade da análise da confiabilidade das disciplinas periciais. Cita por exemplo que é possível que a identificação por DNA talvez seja uma das poucas especialidades que se utiliza de padrões científicos convencionais

já consolidados, sendo que em outras os peritos se baseiam em sua experiência para se chegar ao resultado da perícia.

Na análise de Carrier (2006), muitos dos modelos de processo investigativo digital se baseiam na experiência de seus autores, reforçando a idéia de Berger.

4.2.2 Resposta e Tratamento de Incidentes

Segundo Mandia e Prosise (2001), num contexto de avanço tecnológico, de limites aparentemente tênues entre as informações da companhia e dos empregados, e da crescente capacidade técnica dos usuários de computadores, os principais desafios das corporações em termos de proteção à informação são:

a) Impedir o furto de informações proprietárias e confidenciais;

b) Proteger a privacidade e o bem-estar dos empregados e dos clientes;

c) Proteger a integridade dos dados confidenciais;

d) Impedir a interrupção dos serviços aos clientes e aos empregados;

e) Treinar adequadamente o pessoal para enfrentar esses desafios.

Ainda segundo esses autores, para se alcançar esses objetivos, é fundamental a implementação de um mecanismo de resposta e tratamentos a incidentes que permita a avaliação da situação com precisão, a recuperação rápida dos incidentes, a coibição do ataque e a aplicação de medidas legais contra os invasores.

Kruse e Heiser (2001) também reforçam a importância da recuperação dos serviços de forma segura e rápida na resposta e tratamento de incidentes.

Grance, Kent e Kim (2004) afirmam que o objetivo primário da coleta de vestígios no ponto de vista do processo de respostas a incidentes é resolver o incidente.

A European Commission Directorate-General Information Society (2003) entretanto, frisa que devido a esse foco na recuperação rápida dos sistemas visando o mínimo de impacto à companhia, os vestígios podem ser ignorados, destruídos ou destituídos de valor legal.

Os vestígios, no entanto, devem ser coletados de forma que todas as leis e regulamentos aplicáveis sejam cumpridos. Esses procedimentos, de acordo com Grance, Kent e Kim (2004), devem ser discutidos previamente com o departamento jurídico da companhia e com as entidades legais, de forma a garantir a admissibilidade da prova.

O processo de resposta e tratamento de incidentes conforme Grance, Kent e Kim (2004), é composto das 4 fases a seguir:

a) Preparação;

b) Detecção e análise;

c) Contenção, Erradicação e Recuperação;

d) Pós-incidente.

Os procedimentos da resposta e tratamento de incidentes são definidos na fase de preparação de forma que as corporações estejam preparadas prontamente e também para a prevenção dos incidentes.

Também faz parte da fase de preparação, as atividades de prevenção de grande relevância na revisão e adequação dos controles de segurança, mas principalmente no sentido de propiciar subsídios para a perícia.

Mandia e Prosise (2001) citam como medidas de prevenção, a geração e registro de hash dos arquivos principais, configuração os registros de eventos de auditorias com detalhe e retenção adequados, reforço da defesa dos computadores, políticas adequadas de backup e contingenciamento e principalmente treinamento.

Segundo Grance, Kent e Kim (2004), um dos maiores desafios do processo de resposta e tratamento de incidentes é detectar incidentes e levantar possíveis problemas de forma mais acurada. Isso se deve basicamente à grande variedade de meios pelas quais os incidentes são detectados, ao alto volume de possíveis sinais da ocorrência de incidentes e da necessidade de equipe especializada em vários segmentos.

Esses autores definem ainda dois tipos de sinais que podem auxiliar no processo detectivo:

a) Sinais precursores - indicam que incidentes podem ocorrer no futuro;

b) Sinais indicativos - apontam os incidentes que ocorreram ou estão ocorrendo.

De acordo com Mandia e Prosise (2001), após a análise inicial onde se detecta a ocorrência do incidente é definida a estratégia de resposta. A estratégia deve considerar aspectos técnicos e de negócios e ser aprovada pela companhia.

Grance, Kent e Kim (2004) definem que na fase de contenção é definida a estratégia de como será contido o problema de forma que não sejam afetados outros sistemas. O tipo de incidente e a severidade definem a estratégia a ser adotada.

Conforme Marcella e Greenfield (2002), a partir da autorização para o prosseguimento da investigação, deverá ser definida a estratégia investigação.

O principal e mais comum tipo de investigação é o que não leva a processos judiciais ou litígios.

Apesar disso, é conveniente que sempre sejam utilizados o mesmo rigor dos procedimentos formais da perícia computacional conduzida no contexto dos processos judiciais, de forma que os vestígios sejam coletados, tratados de forma adequada e de maneira que possam tanto serem apresentados à gerência da companhia quanto a um tribunal.

Entretanto, é possível que a empresa não possua os recursos necessários disponíveis para a condução da investigação nos mesmos moldes da investigação de âmbito judicial. Isso porque esse procedimento consome recursos e tempo e pode exigir profissionais de grande experiência e conhecimento.

No entanto, caso se identifique alguma atividade ilegal durante a investigação, ela deverá ser imediatamente interrompida e todos os procedimentos adotados devem ser documentados e as autoridades devem ser acionadas.

De acordo com Grance, Kent e Kim (2004), o principal motivo do levantamento dos vestígios no processo de tratamento e resposta a incidentes é resolver o incidente, secundariamente é possível que sejam necessários procedimentos para finalidades legais.

Depois da contenção do incidente, deve ser iniciado o processo de erradicação que tem o objetivo de eliminar componentes do incidente como, por exemplo, a exclusão de códigos maliciosos. Em alguns casos, a erradicação não é necessária ou ocorre durante o processo de recuperação.

A recuperação é um processo que está em grande parte relacionado ao gerenciamento do sistema operacional e dos sistemas, e que visa recuperar a operação normal e reforçar os controles de segurança quando possível.

A importância do reforço nos controles e monitoração está relacionada à identificação da vulnerabilidade e, uma vez que um recurso é atacado, geralmente ele é atacado outras vezes ou é utilizada a mesma técnica no ataque de outros recursos do mesmo ambiente.

Na fase final de pós-incidente, as atividades de lições aprendidas produzem um conjunto de informações objetivas e subjetivas por incidente. Embora muito dessas informações sejam destinadas a atividades de análise das vulnerabilidades, tendências dos incidentes ou mesmo ao dimensionamento e orçamento da equipe, uma parte importante está nas informações objetivas coletadas que podem ser utilizadas posteriormente.

As corporações devem estabelecer políticas de retenção de vestígios. A apresentação dos vestígios pode ser necessária em caso de processos judiciais, que podem durar por anos. Indícios ou vestígios que a princípio parecem não ter muita relevância, podem tornar-se importantes posteriormente.

4.2.3 Procedimentos da polícia

Nem todos os incidentes resultam no envolvimento da polícia. Entretanto, o acionamento da polícia é obrigatório nos casos de ações criminosas como a pedofilia.

De acordo com Rocha (2003), devem ser tomadas precauções durante o procedimento policial. A coleta dos vestígios deve ser feita pelo perito criminal com as precauções específicas para o tipo de vestígio.

Além disso, o trabalho pericial deve ser acompanhado por duas testemunhas que assinarão um termo sobre os vestígios coletados juntamente com o delegado, o perito e escrivão, de forma a comprovar que os vestígios não foram forjados.

De acordo com Costa (1999), para que os vestígios possam integrar a prova, o procedimento deve ser seguido rigorosamente e cita as 3 fases:

a) Primeira Fase – descoberta e localização dos vestígios;

b) Segunda Fase – recolhimento e preservação dos vestígios;

c) Terceira Fase – estudo e interpretação dos vestígios.

Na primeira fase, o agente policial, a partir do recebimento da ocorrência, deve se dirigir ao local do crime, desde que não sendo impossível ou inconveniente, e garantir que não seja alterado o local do crime até a chegada dos peritos e execução do exame do local do crime, de acordo com o Código do Processo Penal, art. 6, inciso I.

Após a liberação pelos peritos criminais, a polícia judiciária deverá coletar os vestígios.

De acordo com o Código do Processo Penal, art. 169, além da preservação do local do crime para o trabalho dos peritos, caso ocorram alterações no local, elas deverão ser documentadas, assim como suas implicações.

Além do exame do local, existem outros procedimentos que podem ser conduzidos para a identificação de vestígios:

a) Busca domiciliar – busca de vestígios na residência do indiciado. Devido à inviolabilidade domiciliar, esse procedimento só pode ser executado quando devidamente autorizado pelas autoridades competentes;

b) Busca pessoal – busca de vestígios que possa estar em posse do indiciado;

c) Arrecadação em local estranho – coleta de vestígios em local diferente do crime, por deliberação do indiciado, terceiros, ou ainda por ações meramente fortuitas;

d) Apresentação por terceiros – entregue deliberadamente por terceiros;

e) Apresentação espontânea pelo suspeito ou indiciado - entregue deliberadamente pelo suspeito ou indiciado;

f) Momento da prisão em flagrante – vestígios recolhidos no flagrante.

A segunda fase que é o recolhimento e preservação dos vestígios, segundo Costa (1999), tem por objetivo de permitir que tais vestígios posteriormente para o exame pericial e secundariamente o de devolvê-los, quando possível e permitido por lei, ao proprietário, conforme o artigo 12, § 5º do Código do Processo Penal.

A terceira fase, o estudo e interpretação dos vestígios, são de responsabilidade da perícia criminal que fica responsável pela elaboração do laudo pericial, composto da interpretação dos vestígios e dos elementos relacionados com o delito e tem os objetivos de:

a) Comprovar a existência do crime;

b) Revelar os meios e modos pelos qual o crime foi cometido;

c) Identificar a autoria.

4.2.4 Procedimentos da Perícia Computacional

De acordo com Carrier (2006), as investigações digitais e a forense computacional são conduzidas regularmente por organizações policiais e corporações, mas não há uma teoria formal para o processo.

O processo de investigação digital está focado na tecnologia e ferramentas existentes atualmente, que auxiliam na resolução de crimes, mas é muito limitado a longo prazo, considerando-se a complexidade e rápida evolução tecnológica.

Casey (2004) salienta a importância do processo no que diz respeito ao impacto que a prova apresenta como comprovação ou refutação da alegação pode ocasionar e por isso deve estar fundamentada num método sólido.

Segundo Carrier (2006), muito das fases dos modelos de processos de investigação digital são concebidas com base nas experiências dos investigadores e podem não ser suficientes para todos os tipos de investigação.

O NIJ (U.S. National Institute of Justice) publicou um modelo de processo no *Crime Scene Investigation Guide*. Esse manual é uma referência para a resposta inicial a incidentes visando o tratamento seguro dos vestígios e é voltado aos tratamento do local do crime físico.

Fases desse modelo:

a) Preparação: Preparação de equipamentos e ferramentas para as tarefas da investigação;

b) Coleta: Procura de documentos e coleta ou copias de objetos físicos que contenham vestígios digitais;

c) Exame: Tornar o vestígio eletrônico visível e documentar o conteúdo do sistema. É executada a redução de dados nessa fase para a identificação do vestígio;

d) Análise: Análise do vestígio da fase de exame para determinar a relevância do vestígio e valor probante.

e) Relatório: Relato de todas as fases.

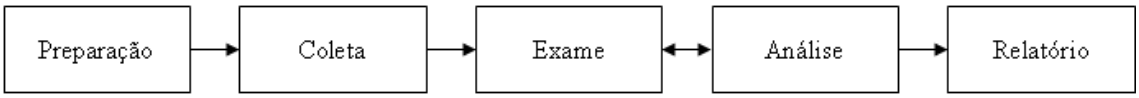

Figura 3. Modelo de Processo Investigativo do NIJ

Como o foco desse modelo é a fase de coleta, não há muitos detalhes das fases de exame e análise e a relação entre o crime e os tipos de dados que possam conter vestígios.

De acordo com Carrier (2006), não fica claro se os requisitos das fases de exame e análise são diferentes e poderia ser entendido que a redução de dados na fase de exame seria uma simplificação da redução que é feita mais detalhes na fase de análise.

Há outros modelos baseados nesse como o definido por Palmer (2001) e o modelo abstrato de processo de Reith, Carr e Gunsh (2002).

Carrier e Spafford (2003) propuseram um modelo de investigação do local físico do crime que possui fases de análises tanto do local físico onde foi localizado o computador quanto do local onde foi encontrado o dado digital.

Fases desse modelo:

a) Preservação: Preservação do estado do local do crime;

b) Pesquisa: Procura de vestígios óbvios relevantes à investigação;

c) Documentação: Documentação do local do crime;

d) Procura: Procura mais detalhada que na fase de pesquisa.

e) Reconstrução de Evento: Reconstrução dos eventos que ocorreram no local do crime.

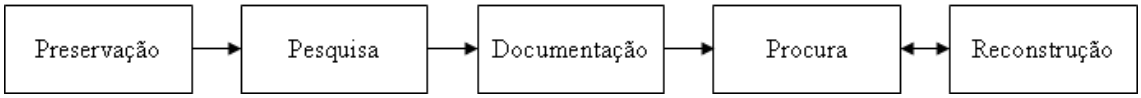

Figura 4. Modelo de Processo Investigativo de Carrier e Spafford (2003)

O modelo Hierárquico Baseado em Objetivos de Beebe e Clark (2004) possui duas camadas, similar ao modelo baseado no local do crime, mas possui fases diferentes.

Fases da primeira camada desse modelo:

a) Preparação: Preparação de equipamentos e equipes para a investigação;
b) Resposta a Incidente: Detecção, validação e levantamento do incidente para definição de estratégia de resposta;
c) Coleta de Dados: Coleta de vestígios que suportem a estratégia de resposta;
d) Análise dos Dados: Pesquisa, extração e reconstrução dos dados coletados;
e) Apresentação: Comunicação do que foi encontrado aos responsáveis;
f) Fechamento: Revisão do processo investigativo e execução de alterações necessária.

Fases da segunda camada do modelo:

a) Pesquisa: Mapeamento do sistema de arquivos e locais relevantes;
b) Extração: Extração de dados com base nos objetivos mapeados;
c) Exame: Exame dos dados extraídos para a reconstrução e confirmação ou refutação das hipóteses.

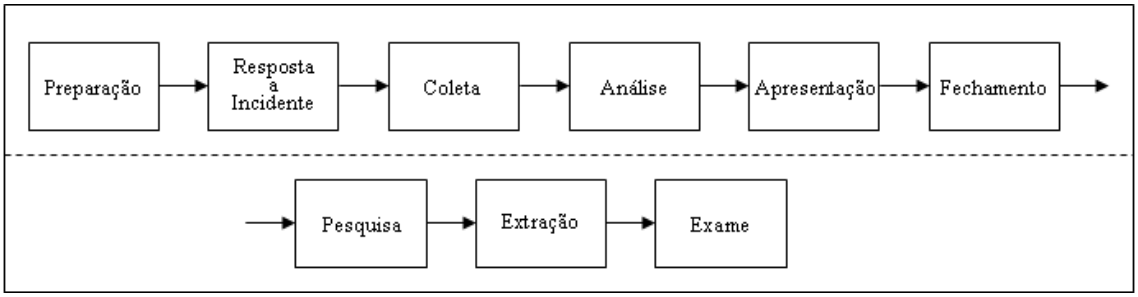

Figura 5. Modelo Hierárquico Baseado em Objetivos

O modelo baseado em hipóteses de Carrier (2006) usa o método científico para formular hipóteses e testá-las. É composto de 4 fases:

a) Observação: Observação e coleta de recursos e informações relevantes para investigação;

b) Formulação de hipóteses: Formulação de hipóteses baseadas na observação. São formulados níveis diferentes de hipóteses durante a investigação;

c) Predição: Predições sobre os vestígios que possam confirmar ou refutar as hipóteses.

d) Teste e Busca: Condução de teste e busca com base nas predições sobre os vestígios.

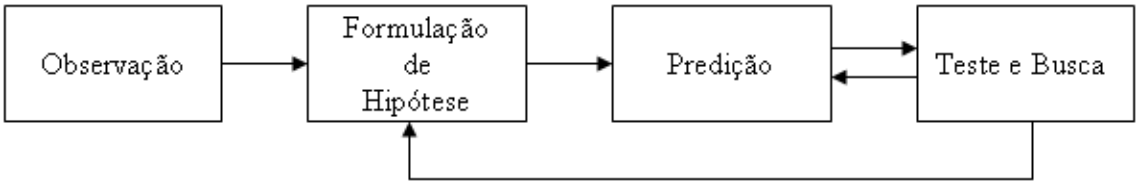

Figura 6. Modelo Baseado em Hipóteses

Segundo Carrier (2006), as investigações iniciam-se com uma série de questões relacionadas ao estado atual do ambiente digital que sofreu ataque. Através da formulação de hipóteses sobre o estado e eventos anteriores ao ataque e testando-se as hipóteses é possível chegar às respostas através de um modelo histórico inferido.

Ainda de acordo com esse autor, há vários tipos de hipóteses as serem formuladas, de hipóteses sobre estados complexos a ocorrência de eventos.

5 A ADMISSIBILIDADE

Nesse capítulo são abordados os processos que lidam com a proposição, análise dos indícios digitais e as provas que podem constituir, assim como os fatores que podem determinar se tais provas podem ser admitidas.

5.1 Admissibilidade da Prova no Brasil

As provas são tratadas em fases distintas nos processos judiciários civis no Brasil, chamadas de momentos da prova, de acordo com Dinamarco (2005):

a) Propositura das provas;

b) Admissão pelo juiz;

c) Realização com a presença de todos os sujeitos processuais;

d) Valoração pelo juiz.

Durante a fase de propositura das provas, inicialmente são feitas as petições para que as provas sejam produzidas e num segundo momento, o autor que possui a responsabilidade por produzi-las, deverá indicar como o meio de prova a ser utilizado e considerar o questionamento do réu.

No momento da admissão, o juiz indicará quais são as provas a serem consideradas no processo. As provas poderão ser indeferidas nessa fase se elas forem consideradas desnecessárias ao processo, inadequadas ou a requisição não ocorreu no prazo.

Na fase da realização é que serão utilizados os meios de prova para a extração dos elementos comprobatórios das fontes de prova relacionadas ao fato a ser provado, constituindo-se na parte mais importante dos momentos de prova. É nessa fase que devem ocorrer as perícias.

O juiz, na fase de valoração faz a avaliação das provas, considerando o poder de convicção dessas provas no processo.

De acordo com Mirabete (2007), a perícia pode ser solicitada assim que a autoridade policial, nos casos criminais, tiver conhecimento da infração, durante o

inquérito, no processo de instrução, solicitada pelo juiz, ou ainda pelas partes, quando obtiverem conhecimento da denúncia ou queixa, ou no prazo de defesa prévia.

Quando a solicitação da perícia é feita pelas partes, a autoridade policial deverá avaliar esse pedido e poderá recusá-la, caso considere desnecessária para a elucidação do caso. É importante lembrar, no entanto, que de acordo com o art. 158 do Código de Processo Penal, é obrigatória a perícia nos casos que deixam vestígios e o seu não cumprimento poderá anular a sentença.

Uma vez realizado o exame pericial, deverá ser permitido às partes e inclusive ao réu, a possibilidade de argüição da incompatibilidade dos peritos, de formulação de quesitos e de crítica ao laudo elaborado. O não cumprimento poderá levar à nulidade do procedimento, sob a argumentação de cerceamento de defesa.

Após a determinação da realização da perícia, as autoridades policial e judiciárias poderão então levantar os pontos a serem esclarecidos através da formulação de quesitos.

Os peritos, de acordo com o art. 160 do Código de Processo Penal, deverão elaborar o relatório com descrição minuciosa do exame e deverão responder aos quesitos. O laudo deve conter:

a) Preâmbulo – introdução com nome dos peritos, títulos dos peritos e o objeto da perícia;
b) Exposição – narração do que foi observado com ordem e método;
c) Discussão – análise critica dos fatos observados;
d) Conclusão – apresentação sintética das respostas aos quesitos propostos.

No âmbito penal, também existem situações onde poderão ser solicitadas novas perícias:

No caso dos dois peritos oficiais divergirem no relatório, as autoridades policiais ou judiciárias deverão indicar um terceiro. Caso esse terceiro ainda conclua de forma divergente dos demais, o juiz poderá solicitar nova perícia com peritos diferentes ou então se decidir por um dos laudos.

Se forem identificadas falhas, omissões, falta de formalidade, obscuridade ou contradições, as autoridades policiais ou judiciais poderão solicitar o esclarecimento ou complementação do laudo e ainda, se for identificado que o relatório não servir ao esclarecimento dos fatos.

5.1.1 Admissibilidade da Prova Pericial

A avaliação da admissibilidade da prova, conduzida pelo juiz, ocorre após as após proposição das provas.

De acordo com Gomes Filho e Grinover (2006), as provas são tratadas em quatro momentos durante o processo judicial:

a) Proposição: quando as provas são indicadas ou requeridas;

b) Admissão: quando o juiz se manifesta quanto à admissibilidade das provas;

c) Produção: quando as prova são introduzidas no processo;

d) Apreciação: quando as provas são valoradas pelo juiz.

As provas periciais são consideradas adequadas quando é necessário o conhecimento técnico específico para esclarecimento do fato, de acordo com art. 145 do Código de Processo Civil.

O art. 335 do Código de Processo Civil, no entanto, dá abertura para que o juiz utilize de sua experiência técnica para análise de fatos que não demandem rigor técnico. Essa experiência é especificada no Código de Processo Civil, como noções que o juiz possa ter em área como psicologia, física, matemática, informática.

Em alguns casos, poderão ser admitidas também as perícias informais quando as questões técnicas a serem esclarecidas forem consideradas mais simples. Nesse processo, não é necessária a elaboração de laudo, bastando apenas o esclarecimento através de depoimentos de testemunhas técnicas em audiência. Caso esse testemunho não seja suficiente para o convencimento, ele poderá solicitar uma segunda testemunha ou ainda uma perícia formal, se considerar que a informal não será satisfatória ao caso.

A prova pericial poderá ser considerada desnecessária também se o fato puder ser provado através de outros meios de prova, como o testemunhal e o documental ou ainda, se a perícia for impraticável.

Após a apresentação do laudo do perito, as partes podem apresentar questionamentos adicionais sobre o relatório, solicitando esclarecimento. Esses quesitos suplementares são encaminhados ao perito por escrito e o perito por sua vez, responderá às perguntas em audiência.

O resultado desse procedimento não invalida a perícia, visto que quem deve decidir sobre o valor da prova é o juiz que, no entanto, poderá afetar a credibilidade sobre o laudo.

No caso do juiz que o primeiro laudo não for suficiente para a conclusão da questão, ele poderá solicitar um outro novo exame, na chamada segunda perícia. O primeiro laudo não é invalidado e o juiz deverá considerar os dois trabalhos no seu trabalho de análise e conclusão.

No Brasil, no âmbito penal, conforme Gomes Filho e Grinover (2006), as provas não podem ser admitidas quando forem contrárias a normas legais ou princípios do direito positivo:

a) Os fatos não foram introduzidos no processo pelo juiz e submetidos para debate entre as pelas partes;
b) Provas formadas fora do processo, sem a presença do juíz;
c) Provas formadas sem a presença das partes;
d) Provas ilícitas.

5.1.2 Regras de Apreciação das Provas

Segundo Dinamarco (2005), tendo em vista a ignorância do juiz aos fatos relevantes do caso e para que ele julgue se os fatos alegados pelas partes ocorreram ou não, é necessário que ele seja instruído, passando a conhecer os fatos para se decidir com firmeza.

Malatesta (2001) apresenta as regras gerais utilizadas pelo judiciário para a apreciação de provas:

a) *Ingraduabilidade da certeza sobre as provas* – A prova não deve apresentar graduação quanto à sua certeza, ou seja, ela deve convencer ou então não deverá ser considerada prova;

b) *Originalidade e oralidade* – deve-se procurar, dentro do possível, apresentar as provas direta e imediatamente à apreciação do juiz, evitando-se impressões alheias. Através da palavra falada, o pensamento pode ser expresso diretamente;

c) *Liberdade objetiva das provas* – A prova não deve possuir limitação preestabelecida de valor quanto ao objeto provado;

d) *Liberdade subjetiva das provas* – O sujeito probante, seja coisa ou pessoa, deve ser respeitado e as suas condições genuínas mantidas;

e) *Publicidade* – as provas devem ser submetidas ao juiz de forma que seja possível tornar a apreciação pública possível, de forma a tornar transparente o processo de convencimento;

f) *Produção da melhor prova* – Para servir de base à condenação, devem ser procuradas as melhores provas que possam existir e não se deve se contentar com provas indiretas;

g) *As provas na matéria penal devem ser substanciais e não formais como no cível* – No âmbito penal, não se pode condenar sem a certeza da culpa e não é possível o equívoco.

Malatesta (2001), em referência à última regra, cita algumas diferenças entre as alçadas cível e penal:

a) São os direitos alienáveis que estão em jogo no campo cível e por isso são admissíveis as renúncias a direitos bem como a aceitação de obrigação pelas partes, ao passo que em matéria penal, os direitos são inalienáveis;

b) No âmbito cível, ao se pronunciar a favor de uma das partes, se condena a outra, sendo que no penal, o juiz não se vê na posição de condenar alguém para absolver outro;

c) Na matéria civil, por tratar de direitos particulares e específicos, caso uma das partes não apresente prova, a parte contrária triunfará através

da verdade formal produzida das provas produzidas. Já no âmbito penal, não pode haver condenação em decorrência de descuido nas provas de inocência, na incerteza deve-se absolver.

Dinamarco (2005) afirma que nos processos cíveis, as provas são necessárias somente em casos controversos. Também confirma que no caso da não apresentação da prova, seja pelo fato não ser considerado controverso, por confissão, ou pelo fato ser considerado notório, a alegação será aceita como existente pelo juiz.

d) Para que um crime seja atribuído como fato certo cometido por um indivíduo, devem ser provados:

    i. Objetividade criminosa – se o fato criminoso realmente ocorreu;

    ii. Subjetividade exterior criminosa – se o fato criminoso ocorreu através da ação do criminoso ou de sua vontade;

    iii. Subjetividade interior criminosa – se houve intenção criminosa.

De acordo com Mirabete (2007), existem 2 sistemas para a apreciação dos laudos periciais. Um é o vinculatório, onde o juiz não pode deixar de aceitar o laudo e o juiz está preso às conclusões do perito.

Pelo sistema liberatório, o juiz pode aceitar ou não o relatório completo ou parte dele. No Brasil, o sistema utilizado é o do livre convencimento, de acordo com o art. 182 do Código de Processo Penal.

Nesse sistema, considera-se o juiz apto a compreender às exposições periciais, podendo levantar e analisar elementos do processo que possam apoiar ou refutar o laudo.

6 LEGISLAÇÃO E PERÍCIA COMPUTACIONAL NO PANORAMA INTERNACIONAL

De acordo com Casey (2004), em 1978 houve a promulgação da primeira lei específica nos Estados Unidos, o Ato de Crimes de Computador da Flórida, após um incidente amplamente divulgado de falsificação utilizando computadores, de tíquetes premiados, feita por funcionários da Flagler Dog Track.

O Canadá foi um dos primeiros países a criarem uma legislação federal para tratar de crimes de informática, como adendo ao seu Código Penal.

Os Estados Unidos contam com várias leis e normativas específicas relacionadas à informática, como a *US Federal Computer Fraud and Abuse Act* de 1984, mas outras regulamentações, como a FRE – Federal Rules of Evidences que determina os critérios Daubert para a aquisição de provas técnicas e que pode determinar a aceitabilidade dos indícios digitais.

A Austrália também incluiu um adendo ao seu Código Penal em 1984 para tratar de crimes relacionados à informática.

Alguns países possuem sistemas legais complexos onde alguns estados podem possuir leis específicas. No caso de crimes que envolvam jurisdição internacional, as questões que envolvam legislação nacional específica e jurisdição são mais complexas.

Nos Estados Unidos, por exemplo, nos casos de processos criminais e litígios civis, a jurisdição deve ser definida de acordo com a localidade onde a audiência e o julgamento ocorrerão. Em alguns casos, a jurisdição é mais clara, mas dependendo de onde e como o crime é cometido, a jurisdição não é, Casey (2004).

Os crimes cibernéticos podem ser perpetrados utilizando-se mecanismos que podem estar localizados em qualquer parte do mundo com o criminoso e vítimas de nações diferentes. Neste caso, o criminoso pode ser processado numa localidade diferente de onde os indícios e provas podem ser adquiridas..

Cada país possui seu próprio sistema legal com processos próprios e que devem seguir procedimentos específicos para assegurar a admissibilidade da prova.

No entanto, os casos que envolvam jurisdição transnacional, as provas deveriam ser aceitas em quaisquer jurisdição.

Entre os muitos desafios que a perícia digital proporciona, a jurisdição transnacional é uma que ainda não foi tratada adequadamente.

Existem poucas iniciativas de sinergia e dentre delas grande parte originam da Europa, muito provavelmente devido às iniciativas da União Européia que levam a diretrizes comuns em várias áreas.

6.1 A União Européia

A União Européia é uma organização política formada de 25 países europeus, cujo objetivo é oferecer um mercado único. A legislação da União Européia emana das Instituições Européias (Parlamento, Conselho e Comissão) e está incorporado em cada lei nacional aplicado pelos tribunais nacionais. Não obstante, cada nação ainda possui jurisdição criminal e sistemas policiais separados.

A European Commission Directorate-General Information Society (2006) patrocinou um projeto cujo objetivo foi o de prover um manual às organizações que trabalham com resposta a incidentes com informações importantes relacionadas aos requisitos e regras sobre crimes cibernéticos nos 25 países que compõem a União Européia.

Outro objetivo foi o de prover um guia de fácil utilização às organizações que lidam com resposta a incidentes, inclusive organizações policiais, com as descrições técnicas de incidentes, assim como a estrutura de segurança e legislação do país em questão e detalhar os procedimentos de trabalho.

Esse documento apresenta uma visão geral do sistema legal de cada um dos 25 países membro e disponibiliza informações relacionadas aos tipos de incidente relevantes descritos na taxonomia e respectiva sanção aplicável no país.

A taxonomia usada pela European Commission Directorate-General Information Society (2006) inclui: 1. Rastreamento (Scan), 2. Acesso não-autorizado a transmissões, 3. Acesso não-autorizado a informações, 4. Modificação não-autorizada de Dado, 5. Código Malicioso, 6. Negação de Serviço, 7.

Comprometimento de conta, 8. Tentativa de Intrusão, 9. Acesso não-autorizado a sistemas, 10. Spam.

a) Rastreamento (Scan)s (Scan)

A Rastreamento (Scan)s são as ações tomadas para coletar informações sobre possível alvo.

Exemplos: Scan, queries de DNS.

b) Acesso Não-Autorizado a Transmissões

O Acesso Não-Autorizado a Transmissões são interferências não autorizadas a transmissões não-públicas de dados de computadores. As técnicas utilizadas nesse incidente incluem interceptação de pacotes de redes, injetar ou remover pacotes do tráfego.

Exemplos: Ataques man-in-the-middle, session hijacking.

c) Acesso Não-Autorizado a Informações

O Acesso Não-Autorizado a Informações são as tentativas de se obter acesso a dados de forma não autorizada que pode ocorrer através da quebra de mecanismos de controle de acesso para ganhar acesso remoto ou local.

Exemplos: SQL injection, manipulação de parâmetro em script CGI.

d) Acesso Não-Autorizado a Dados

O Acesso Não-Autorizado a Dados são alterações não-autorizadas de informações em um sistema computacional. A alteração de dados não autorizada pode ser feita através da criação ou alteração dos dados que residam num computador, de forma remota ou local.

e) Código Malicioso

São códigos que ao serem executados, de forma intencional ou não, ocasionam o comprometimento do computador alvo.

Exemplos: Vírus, worm.

f) Negação de Serviço

A Negação de Serviço são acessos repetidos ao alvo que sobrecarrega sua capacidade ou interrompe um serviço. A técnica geralmente utilizada nesse ataque é

a execução repetida de solicitações de recursos computacionais como memória, tempo de CPU, conexões IP e espaço em disco.

Exemplos: Ataques syn flood, winnuke.

g) Comprometimento de Conta

O Comprometimento de Conta é frequentemente definido como o acesso não-autorizado a um sistema ou recurso do sistema. Esse tipo de ataque pode ser feito através da exploração, de forma remota ou local, de vulnerabilidades do sistema de forma a conseguir acessar contas de usuários.

Exemplos: Buffer overflow, uso de credenciais violadas.

h) Tentativa de Intrusão

São tentativas de acesso não-autorizadas, feitas através de várias técnicas.

Exemplos: a tentativa de quebra de senha, tentativas de execução de buffer overflow, uso de contas ou senhas padrão do sistema, tentativas de exploração de vulnerabilidades antigas, tentativa de uso de contas padrão ou ainda de conexão a portas SNMP.

i) Acesso Não-Autorizado a Sistemas

O Acesso Não-Autorizado a Sistemas são acessos não-autorizados a computadores conectados a uma rede ou sistema de telecomunicações, efetuado a partir da intrusão da rede ou da interferência em equipamento conectado a rede.

Exemplos: DNS Spoofing, war dialing.

j) Spam

Os Spams são a distribuição não-solicitada de mensagens comerciais sem consentimento e é feito através da distribuição, geralmente automatizada de e-mails, sem a opção de recusar o recebimento das mensagens ou ainda que o mecanismo exista, mas não funcione.

Exemplos: scripts, open relays.

Eventualmente, um incidente não pode ser punido como tal, embora possa ser qualificado como uma ação passível de punição, conforme as circunstâncias. O exemplo mais comum é a Rastreamento (Scan) que muitos dos países membros

não a considera como um crime, mas como parte das atividades preparatórias para se cometê-lo.

7 COMPARATIVO

Esse capítulo faz o levantamento dos padrões, modelos de processo investigativo-pericial pesquisados nesse trabalho e então fazendo um comparativo das recomendações, padronizações e procedimentos.

7.1 Padrões

Nesse trabalho, foram identificados documentos que estabelecem princípios e práticas padronizadas nas possíveis atividades investigativas e periciais que podem ser utilizados nos âmbitos corporativo, judicial e extrajudicial.

Alguns dos documentos estabelecem padrões para a aplicação em atividades de contato inicial com o local do incidente ou crime, como as atividades de identificação, coleta e preservação de vestígios.

Essas documentações estabelecem em comum, princípios básicos como a preocupação na identificação e preservação dos vestígios coletados para o periciamento, de forma que possibilite demonstrar a integridade do que foi coletado e novas perícias sobre o material, caso haja necessidade.

O G8 definiu princípios mínimos muito básicos, essenciais para a viabilização de padrões internacionais comuns, mas que demandam procedimentos e normativas para que possam ser aplicados.

A RFC 3227 é uma recomendação básica que cobre boa parte dos princípios mínimos básicos do G8, voltada a ambiente corporativo, nas atividades de respostas a incidentes. Não foram identificadas recomendações para a aplicação obrigatória desse documento em quaisquer segmentos.

O Guia de Melhores Práticas para Vestígios Eletrônicos baseados em Computador da Polícia do Reino Unido possui regras específicas e mais detalhadas baseadas nos procedimentos policiais de busca, apreensão e preservação do local do crime.

Além desses documentos, foram identificados documentos voltados às atividades periciais, como os Guias de melhores práticas em exame forense de

tecnologia digital da ENFSI , que definem requisitos específicos para perícias laboratoriais e estão sendo adotados nos laboratórios europeus.

Uma outra iniciativa, nascida de um projeto promovido pela União Européia que envolveu parceiros comerciais, integrantes meio acadêmico e organizações policiais como a Interpol, a Europol e Unidades de Crimes de Alta Tecnologia da Europa, cujo intuito é definir uma abordagem padrão e implantação comum na Europa.

O modelo CTOSE é um modelo que procurou cobrir princípios básicos de investigação e perícia, desenvolveu métodos e ferramentas técnicas e de apoio, como por exemplo para consultas em aspectos jurídicos.

7.2 Modelos de Processo Investigativo-Pericial

Existem vários modelos de processo investigativo-pericial propostos, alguns reforçam e dão maior importância em determinada fase, como no modelo de Carrier e Spafford (2003) no que diz respeito à preservação dos vestígios, a uma triagem inicial e a uma nova análise mais específica.

Beebe e Clark (2004) consideram em seu modelo, as fases do processo de resposta a incidentes pois podem determinar a estratégia investigativa e técnicas periciais.

O CTOSE definiu um modelo de arquitetura para dar base às demais atividades do processo de perícia computacional.

O Modelo de Processo Investigativo do CTOSE está focado no processo de aquisição de provas e é composto de cinco fases: 1. Preparação; 2. Execução; 3. Levantamento; 4. Investigação; 5. Fase de Aprendizado. Este modelo disponibiliza um guia de ações e decisões a serem considerados em caso de incidente. Em cada passo descrito, são disponibilizadas informações adicionais que incluem funções, conhecimento necessário e aconselhamento legal.

Recomendações, Padronizações e Procedimentos								Modelo de Processo Investigativo			
Item	**RFC 3227**	**ACPO**	**Princípios do G8**	**ENFSI**	**CTOSE**	**CIRT - Grance, Kent e Kim (2004)**	**Procedimentos da Polícia - Brasil**	**Guia de Investigação do Local do Crime - NIJ**	**Modelo de Investigação do Local Físico do Crime - Carrier e Spafford (2003)**	**Modelo Hierárquico Baseado em Objetivos - Beebe e Clark (2004)**	**Modelo Baseado em Hipóteses - Carrier (2006)**
Escopo	Coleta Preservação	Busca Coleta Preservação	Coleta Preservação Análise	Análise Confrontação Documentação Apresentação da Evidência	Identificação de Incidente Coleta Validação Armazenamento Acesso Análise Confrontação Jurídico Documentação Apresentação da Evidência	Busca Coleta	Busca Coleta Preservação	Preparação Coleta Exame Análise Relatório	Preservação Pesquisa Documentação Procura Reconstrução	Preparação Resposta a Incidente Coleta Análise Apresentação Fechamento Pesquisa Extração Exame	Observação Formulação de Hipótese Predição Teste e Busca
Público Alvo	Empresarial	Organizações Policiais	Organizações responsáveis por tratamento de vestígios	Laboratório de Perícia	Organizações responsáveis por tratamento de vestígios Foco Empresarial	Empresarial - Contato inicial com incidentes	Organizações Policiais	Organizações responsáveis por tratamento de vestígios	Organizações responsáveis por tratamento de vestígios	Organizações responsáveis por tratamento de vestígios	Organizações responsáveis por tratamento de vestígios
Análise: Redução - informações relevantes à investigação	N.E.	Sim	N.E.	Sim	Sim	N.A.	N.E	Sim	Sim	Sim	Sim
Análise: Técnicas propostas	N.E	N.E	N.E	Abordagem bayesiana: cálculo de probabilidade da ocorrência das hipóteses levantadas	N.E	N.A.	N.E	N.E	N.E	N.E	Formulção de hipóteses baseadas na observação
Apresentação de Evidências	N.E	N.E	N.E	Sim	Sim	N.E	Sim	N.E	Sim, para time de investigação	Sim	N.E
Busca: Vestígios físicos - o que buscar	N.E.	Sim	N.E.	Sim	N.E	N.A.	Sim	Sim	Sim	N.E	N.E
Busca: Vestígios físicos - procedimento	N.E.	Sim	N.E.	Sim	N.E	N.A.	Sim	Sim	Sim	N.E	N.E
Coleta: Anotações Detalhadas - trilhas (data/hora)	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Coleta: Captura de imagem precisa do sistema	Sim	Sim	N.E.	Sim	Sim	N.E	N.E	Sim	Sim	$	Sim
Coleta: Checksum e assinatura em evidência	Sim	Sim	N.E.	Sim	Sim	N.E.	N.E	N.E	Sim	Sim	Sim
Coleta: Cópia de disco em nível de bit (preservação original)	Sim	Sim	N.E.	Sim	Sim	Sim, nos casos necessários (processo judicial)	N.E	N.E	Sim	Sim	Sim
Coleta: Minimização do Risco de alteração do vestígio	Sim	Sim	N.E.	Sim	Sim	Sim, nos casos necessários (processo judicial)	Sim	Sim	Sim	Sim	Sim
Coleta: Não usar procedimentos que podem destruir dados inadvertidamente	Sim	Sim	Sim	Sim	Sim	Sim, nos casos necessários (processo judicial)	N.E	Sim	Sim	Sim	Sim
Coleta: Ordem de volatilidade	Sim	Sim	N.E.	Sim	Sim	Sim	N.E	N.E	N.E	Sim	Sim

Tabela 1 – Comparativo de Recomendações, Padronizações e Procedimentos
(**) cita somente preservação em mídia. Não é abrangente

Recomendações, Padronizações e Procedimentos								Modelo de Processo Investigativo			
Item	RFC 3227	ACPO	Princípios do G8	ENFSI	CTOSE	CIRT - Grance, Kent e Kim (2004)	Procedimentos da Polícia - Brasil	Guia de Investigação do Local do Crime - NIJ	Modelo de Investigação do Local Físico do Crime - Carrier e Spafford (2003)	Modelo Hierárquico Baseado em Objetivos - Beebe e Clark (2004)	Modelo Baseado em Hipóteses - Carrier (2006)
Coleta: Vestígios físicos: o que apreender	N.E.	Sim	N.E.	Sim	N.E	N.A.	Sim	Sim	Sim	N.E	N.E
Coleta: Vestígios físicos: procedimento de apreensão	N.E.	Sim	N.E.	Sim	N.E	N.E.	Sim	Sim	Sim	N.E	N.E
Controle de Qualidade	N.E	N.E	N.E	Sim	N.E	N.E	N.E	N.E	N.E	N.E	N.E
Especificação de Ferramental	N.E	Recomenda tipos de ferramenta	N.E.	N.E.	Define ferramentas específicas	Recomenda tipos de ferramenta	N.E	Recomenda tipos de ferramenta	Cita tipos de ferramenta	N.E	Cita tipos de ferramenta
Pessoal: Procedimentos executados por pessoal competente	N.E.	Sim	Sim	Sim	Sim	Sim, mas para profissionais de CIRT	Sim	Sim	N.E	Sim	N.E
Preservação: armazenamento adequado e integridade do material coletado	N.E. (**)	Sim	N.E.	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Preservação: controle rígidos específico sobre o material coletado de pedofilia	N.E. (**)	Sim	N.E.	Sim	N.E	N.E	N.E	N.E	N.E	N.E	N.E
Preservação: controles rígidos sobre o material coletado	N.E. (**)	Sim	N.E.	Sim	Sim	N.E	N.E	N.E	N.E	N.E	N.E
Preservação: Mídias protegidas para armazenamento das evidências	Sim	Sim	N.E.	Sim	N.E	Sim, nos casos necessários (processo judicial)	N.E	N.E	N.E	Sim	N.E
Princípios: Cumprimento de Política de Segurança da Organização e engajamento do CIRT	Sim	N.E.	N.E.	Não	Sim	Sim	N.A.	N.E	N.A.	Sim	N.E
Princípios: Cumprimento dos princípios estabelecidos pelo documento	NE	Sim	Sim	Sim	Sim	Sim	Sim	Sim	N.E	N.E	N.E
Princípios: Cumprimento dos princípios gerais da perícia	N.E.	N.E.	Sim	Sim	Sim	N.A.	Sim	Sim	Sim	Sim	Sim
Princípios: cumprir normas e leis de privacidade	Sim	Sim	N.E.	Sim	Sim	Sim	Sim	Sim	N.E	Sim	Sim
Princípios: cumprir requisitos legais aplicáveis	NE	Sim	N.E.	Sim	Sim	Sim	Sim	Sim	N.E	Sim	Sim
Relatório: documentação detalhada e clara, sem ambiguidades	Sim	Sim	N.E.	Sim	Sim	N.E.	N.E	Sim	Sim	Sim	Sim
Revisão de resultados	N.E	N.E	N.E	Sim. Recomenda revisões independentes.	N.E	N.E	N.E	N.E	Sim. Recomenda revisões internas	Sim. Recomenda revisões internas	N.E

Tabela 1 – Comparativo de Recomendações, Padronizações e Procedimentos
(**) cita somente preservação em mídia. Não é abrangente

7.3 Cooperação Internacional

A estrutura legal existente em nível nacional e internacional ainda são muito fragmentados de forma a distinguir claramente a aplicação e abordagem nos âmbitos penal, civil e administrativos. Existem situações para as quais não existem leis ou então a legislação existente não é específica aos crimes relacionados a computadores.

Os países europeus possuem sistemas legais próprios e podem lidar de forma diferente quanto aos crimes que envolvem informática. Os crimes podem ser incorporados ao código penal como adendos, ou ainda podem ser introduzidos em novas leis específicas.

Tabela 2 – Visão Geral das Infrações Cibernéticas nos países da União Européia

País	Rastreamento (Scan)	Acesso não autorizado a transmissões	Acesso não autorizado a informações	Modificação não autorizada de Informações	Código Malicioso	Negação de Serviço	Comprometimento de conta	Tentativa de Intrusão	Acesso não-autorizado a sistemas	Spam
Alemanha	n.e.	n.e.	penal	n.e.	n.e.	penal	penal	penal	penal	n.e.
Áustria	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal
Bélgica	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal
Chipre	penal	penal	penal	penal	penal	penal	penal	penal	penal	penal +adm
Dinamarca	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal +adm
Eslováquia	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal +adm
Eslovênia	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal
Espanha	n.e.	penal	penal	n.e.	n.e.	n.e.	penal	penal	penal	penal
Estônia	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal
Finlândia	penal	penal	penal	penal	penal	penal	penal	penal	penal	penal
França	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal +adm
Grécia	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	n.e.
Holanda	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	adm.
Hungria	penal	penal	penal	penal	penal	penal	penal	penal	penal	adm.
Irlanda	n.e.	penal	penal	adm.	adm.	penal +adm	n.e.	n.e..	penal +adm	adm.
Itália	penal	penal	penal	penal	penal	penal	penal	penal	penal	penal
Letônia	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	n.e.
Lituânia	n.e.	penal +adm	penal	penal	penal	penal	penal	penal	penal	adm.
Luxemburgo	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal
Malta	penal	penal	penal	penal	penal	penal	penal	penal	penal	adm.
Polônia	penal	penal	penal	penal	penal	penal	penal	penal	penal	penal
Portugal	penal	penal	penal	penal	penal	penal	penal	penal	penal	adm.
Reino Unido	penal	penal	penal	penal	penal	n.e.	penal	penal	penal	Adm.
Rep. Checa	n.e.	penal	penal	penal	penal	penal	penal	penal	penal	penal +adm
Suécia	penal	penal	penal	penal	penal	penal	penal	penal	penal	adm.

Legenda	
penal	Sanção Penal
adm.	Sanção Administrativa
n.e.	Não Específico – Não há legislação específica, mas dependendo das circunstâncias pode ser considerado um tipo diferente de crime ou a tentativa de cometê-lo.

Fonte: EUROPEAN COMISSION, 2006, p.17

A tabela 2 demonstra a cada tipo de mau uso, a respectiva sanção criminal ou administrativa em cada país.

Mostram também as discrepâncias entre os diferentes sistemas legais, incluindo os procedimentos periciais de cada país.

A European Commission Directorate-General Information Society (2006) considerou os documentos que são referência na Europa: A Convenção em Crime Cibernético do Conselho da Europa e o Framework de Decisão em Ataques contra Sistemas da Informação do Conselho Europeu.

“A Convenção em Crime Cibernético do Conselho da Europa é considerada uma das principais referências na definição de uma diretriz comum para o tratamento dos crimes relacionados a computadores, assim como uma série de medidas que incentivam a cooperação internacional.”

O texto foi finalizado em 2001 e aguardou o processo de assinatura dos países membro do Conselho e dos países que participaram da elaboração, mas que não são membros desse grupo, como o Canadá, o Japão e os Estados Unidos. Esse conselho dá abertura para a adesão a outros países que não sejam membros do Conselho da Europa.

Para que a convenção entre em vigor, foram definidas as condições em seu art. 36, onde, inicialmente deve ser ratificado por 5 países, dentre eles 3 devem ser países membro do Conselho da Europa. O documento entraria em vigor, então, no primeiro dia do mês após 3 meses a partir da sua ratificação. A Lituânia, quinto país ratificante, assinou o documento em 18 de março de 2004 e portanto, tornou-se vigente em 1 de julho de 2004.

Em 2003, foi incluído um protocolo à convenção, referente à tipificação criminal dos atos de racismo e xenofobia que utilizem meios computacionais.

Outra iniciativa nesse sentido é a Estrutura de Decisão em Ataques Contra Sistemas de Informação do Conselho Europeu, adotado em 2005, cujo objetivo é melhorar a cooperação entre o judicial dos países membros no que se refere a ataques contra os sistemas da informação.

A Estrutura de Decisão visa complementar o trabalho das organizações internacionais, como por exemplo, as iniciativas do G8, e em especial a Convenção

em Crime Cibernético do Conselho da Europa e por isso, os conteúdos desses dois documentos são complementares e sincronizados.

A Convenção em Crime Cibernético, junto do protocolo adicional, lidam com alguns crimes que não são especificamente cobertos pela Estrutura de Decisão, como é o caso da falsificação, fraude e conteúdo ofensivo.

A Convenção em Crime Cibernético define três grupos de infrações:

a) Infrações relacionadas à informática – são subdivididas nas seguintes tipologias:
    i. Falsificação por computador – é definida como a inclusão, modificação, exclusão ou supressão de dados, resultando em dados falsificados com o intuito de fazerem-se passar por dados autênticos.
    ii. Fraude por computador – é definida como a causa da perda de propriedade através de quaisquer inclusão, modificação, exclusão ou supressão de dados, e qualquer interferência no funcionamento de um sistema de computador.
b) Infrações relacionadas a conteúdo – inclui atividades relacionadas à distribuição de material com conteúdo ilegal, como:
    i. Produção de material digital de pornografia infantil;
    ii. Disponibilização de material de pornografia infantil através de recursos computacionais;
    iii. Distribuição ou transmissão de material de pornografia infantil através de recursos computacionais;
    iv. Aquisição de material de pornografia infantil para si ou para terceiros;
    v. Posse de material de pornografia infantil em sistema de computador ou mídia de armazenamento de dados.
c) Infrações relacionadas a violação de direitos autorais e outros direitos relacionados – inclui a violação de direitos autorais em escala comercial, através de recursos computacionais. A Convenção em

> Crime Cibernético aborda todos os tratados internacionais e convenções existentes em nível internacional.

De acordo com o European Comission (2003), existem diferenças significantes entre as estruturas legislativas aplicáveis às infrações por computador em cada país membro da União Européia, como será visto na próxima seção.

A falta de conceitos e abordagens comuns ou harmonizadas dificultam se chegar a um acordo de que pode ser considerado como crime quando ocorre uma infração que envolva recursos computacionais. E a questão pode ficar crítica quando envolve mais de um país.

Segundo a European Comission (2003), a Convenção em Crime Cibernético aplicada aos países membros da União Européia, como um framework legal internacional comum, em nível nacional poderá mudar essa situação.

As informações coletadas sobre a legislação dos países membros da União Européia são provenientes do estudo realizado pelo Rand Europe para a Comissão Européia (European Comission (2006)).

Alguns países possuem sistemas legais complexos onde suas subdivisões territoriais podem possuir leis específicas. No caso de crimes que envolvam jurisdição internacional, as questões que envolvam legislação e jurisdição são ainda mais complexas.

Os crimes cibernéticos podem ser perpetrados utilizando-se mecanismos que podem estar localizados em qualquer parte do mundo com o criminoso e vítimas de nações diferentes. Neste caso, o criminoso pode ser processado numa localidade diferente de onde os vestígios e provas podem ser coletados.

Cada país possui seu próprio sistema legal com processos próprios e que adotam procedimentos específicos para assegurar a admissibilidade da prova. No entanto, os casos que envolvam jurisdição transnacional, as provas deveriam ser aceitas em quaisquer jurisdições.

Entre os muitos desafios que a perícia digital proporciona, a jurisdição transnacional é um que ainda não foi tratado adequadamente.

Existem poucas iniciativas de sinergia e muitas delas originam da Europa, muito provavelmente devido às iniciativas da União Européia que levam a diretrizes comuns em várias áreas.

No levantamento efetuado sobre os países da União Européia, assim como no Brasil, foi verificado que não há definições ou dispositivos específicos para a prova digital, mas utilizam a aplicação analógica das regras existentes sobre prova em geral. O mesmo ocorre para os procedimentos de apresentação de provas em juízo e para outros mecanismos como a busca e apreensão.

Foi verificado também no levantamento que os países europeus e os Estados Unidos, embora não possuam referências específicas às provas digitais, eles possuem dispositivos específicos para infrações de informática, sejam através de atualizações em seus códigos penais ou de processo penal, como leis específicas.

O Brasil não possui legislação específica para delitos cibernéticos ou normatizações e métodos específicos para os procedimentos investigativos e periciais digitais. Alguns autores, como Casey (2004), no entanto, consideram que quaisquer crimes cibernéticos podem ser enquadrados em leis existentes caso eles sejam uma manifestação de tipos conhecidos de crimes, mas que usem nova tecnologia.

8 CONCLUSÃO

Nesse trabalho foram pesquisados materiais e documentações relacionados aos processos investigativos e periciais computacionais aplicáveis aos diversos âmbitos e que tenham relação com a admissibilidade de provas.

Como resultado dessa pesquisa, foram encontradas documentações em grande maioria no idioma inglês e provenientes principalmente dos Estados Unidos e de países europeus.

Foram identificadas poucas iniciativas com abordagem internacional e muitos se originaram na Europa. A União Européia e outras comunidades européias patrocinam grupos de trabalho e projetos de forma a facilitar a colaboração entre os membros.

Dentre os documentos analisados, foi verificado que não há um consenso entre os profissionais e organizações envolvidos nos processos investigativos e periciais para algumas questões: do uso de alguns termos aos métodos de investigação e perícia.

Assim, esse trabalho discorreu sobre conceitos fundamentais e adotou algumas convenções procurando-se evitar equívocos.

Na etapa seguinte foram feitas as comparações entre as Recomendações, Padronizações e Procedimentos e os Modelo de Processo Investigativo identificados, onde pôde-se perceber que os princípios fundamentais, como os definidos pelo G8, são observados por praticamente todas as padronizações e modelos analisados.

8.1 Análise dos Resultados

Nesse trabalho foram identificados padrões, melhores práticas e modelos publicados sobre investigação e forense digital, mas ainda não há um consenso.

Apesar da existência dessas padronizações e métodos, foi verificado que os documentos são direcionados a públicos distintos e não é garantido que esses documentos sejam aplicados pelas organizações às quais se destinam.

Além disso, esses documentos cobrem parcialmente os processos investigativos e periciais.

No entanto, foi observado que os documentos são consistentes em grande parte com os princípios do G8, que definem fundamentos básicos para tais processos, com intuito de sinergia entre nações.

Os princípios do G8, ou a aplicação dos Modelos de Processo Investigativo podem viabilizar a admissibilidade, mas não garantem que os indícios digitais e as provas constituídas sejam aceitas nos diversos países.

Ao se identificar requisitos técnicos e legais atualmente estabelecidos no Brasil e em países da União Européia e Estados Unidos, percebeu-se que também não há uma harmonização dos requisitos, o que dificulta a aceitabilidade de provas em se tratando de casos que envolvam mais de uma nação.

8.2 Análise Geral e Contribuições

Os vestígios são fundamentais nos processo investigativo e criminal e a apresentação da prova pode ser necessária para suportar ou refutar uma alegação.

Devido a essa responsabilidade crítica, a garantia de qualidade dos processos relacionados às provas possuem uma importância vital aos sistemas legais ao redor do mundo.

Um dos principais desafios da forense computacional é a admissibilidade da prova em juízo e, a falha na coleta e manipulação do vestígio pode minar a investigação, Casey (2004).

Os padrões e modelos podem possibilitar processos mais sólidos para a aquisição de provas e fortalece a possibilidade de que as provas sejam admitidas. No entanto, deve ser ressaltado que a padronização, se não utilizada em contexto adequado, pode gerar conclusões equivocadas e além disso, o uso de requisitos muito restritivos podem justamente reduzir as possibilidades de admissibilidade de provas em processos, a exemplo dos critérios Frye.

Para lidar com delitos que atravessam as fronteiras nacionais, os países precisam ter a habilidade de tratar os vestígios de forma que sejam admissíveis nos tribunais e também devem estar preparados para trocar as provas com outros países

Uma abordagem comum harmonizada incluindo procedimentos que sejam aceitos nos países seria fundamental para viabilizar essa troca de provas.

8.3 Sugestão para Trabalhos Futuros

Durante o desenvolvimento desse trabalho, percebeu-se que seria possível identificar soluções preventivas que possibilitem uma maior geração de vestígios, ou seja, de uma maior quantidade de insumos de qualidade que viabilizem a identificação de indícios e constituição de provas, à luz dos requisitos de admissibilidade.

9 REFERÊNCIAS BIBLIOGRÁFICAS

ACPO. **Good Practice Guide for Computer based Electronic Evidence**. Reino Unido: ACPO, 2007. Disponível em: <http://www.devon-cornwall.police.uk/v3/ShowPDF.cfm?PDFName=ElecEvid.pdf >. Acesso em: 15 mar. 2007

BEEBE, N. L.; CLARK, J.G. **A Hierarchical, Objectives-based Framework for the Digital Investigation Process**. In: Proceedings of the 2004 Digital Forensic Research Workshop (DFRWS), 2004.

BERGER, M. A. **The Supreme Court's Trilogy on the Admissibility of Expert Testimony**. In: FEDERAL JUDICIAL CENTER. Reference Manual on Scientific Evidence. 2. ed. Nova York: FJC, 2000, Disponível em: < http://air.f jc.gov/public/f jcweb.nsf/pages/16>. Acesso em: 04 jun. 2006.

BREYER, S. **Introduction**. In: FEDERAL JUDICIAL CENTER. Reference Manual on Scientific Evidence. 2. ed. Nova York: FJC, 2000, Disponível em: < http://air.f jc.gov/public/f jcweb.nsf/pages/16>. Acesso em: 04 jun. 2006.

CABRAL, A.F**. Manual da Prova Pericial**. Rio de Janeiro: Editora Impetus, 2003.

CARRIER, B. D. **A Hypothesis-based Approach to Digital Forensic Investigations**. 2006. 169f. Tese (Doutorado em Information Assurance and Security) - Purdue University, West Lafayette, EUA, 2006.

CARRIER, B. D., **Defining Digital Forensic Examination and Analysis Tools**. In: Digital Forensics Research Workshop II, Agosto 2002, Disponível em <URL: http://www.dfrws.org/dfrws2002/papers/Papers/Brian_carrier.pdf> Acesso em: 10.02.2005.

CARRIER, B. D.; SPAFFORD, E. H. **Getting Physical with the Digital Investigation Process**. International Journal of Digital Evidence (IJDE), 2(2), Outono 2003.

CASEY, E. **Digital Evidence and Computer Crime**, Londres: Academic Press, 2001.

CASEY, E. **Digital Evidence and Computer Crime**, 2. ed. Londres: Academic Press, 2004.

CECIL, J.S.; SCHWARZER, W.W. **Management of Expert Evidence**. In: FEDERAL JUDICIAL CENTER. Reference Manual on Scientific Evidence. 2. ed. Nova York: FJC, 2000, Disponível em: < http://air.f jc.gov/public/f jcweb.nsf/pages/16>. Acesso em: 04 jun. 2006.

CINTRA, A.C.A.; GRINOVER, A.P., DINAMARCO, C.R., **Teoria Geral do Processo**, 3. ed. São Paulo: Editora Revista dos Tribunais, 1995.

CORNELL UNIVERSITY, **Federal Rules of Evidence**. Disponível em: <URL: htttp://www.law.cornell.edu/rules/fre/overview.html>. Acesso em: 04 jun. 2006.

COSTA, J.A. **Manual de Polícia Judiciária**. São Paulo: Editora Forense, 1999.

CRAIGER, J. P. **Computer Forensics Procedures and Methods**. Disponível em: <URL: http://www.ncfs.ucf.edu/craiger.forensics.methods.procedures.final.pdf>. Acesso em: 04 jun. 2006

CYBEX. **The Admissibility of Electronic Evidence in court**. Espanha: CYBEX, 2007. Disponível em: <http://www.cybex.es/agis2005/elegir_idioma_pdf.htm>. Acesso em: 15 mar. 2007

DEPARTAMENTO DO PRIMEIRO MINISTRO IRLANDES, **New Connections: A strategy to realise the potential of the Information Society**. Irlanda: DEPARTAMENTO DO PRIMEIRO MINISTRO IRLANDES, 2007. Disponível em: < http://www.taoiseach.gov.ie/attached_files/Pdf%20files/NewConnectionsMarch2002.pdf>. Acesso em: 15 mar. 2007.

_____, **List of Enacted Laws by date with explanations of what these laws do**. Irlanda: DEPARTAMENTO DO PRIMEIRO MINISTRO IRLANDES, 2007. Disponível em: < http://www.taoiseach.gov.ie/index.asp?locID=243&docID=-1>. Acesso em: 15 mar. 2007.

DINAMARCO, C.R. **Instituições de Direito Processual Civil**. Vol. III, 5. ed. São Paulo: Editores Malheiros, 2005.

EESTI POLITSEI. **Estonian law enforcement system**. Estônia: EESTI POLITSEI, 2007. Disponível em: < http://www.pol.ee/?id=8286>. Acesso em: 15 mar. 2007

ESPÍNDULA, **A. Perícia Criminal e Cível: uma visão geral para peritos e usuários da perícia**. 2. ed. Campinas, SP: Millenium Editora, 2005.

EUROPEAN ANTI-FRAUD OFFICE. **Insight Of OLAF's Partners.** Bélgica: OLAF, 2007. Disponível em: < http://ec.europa.eu/anti_fraud/partners/tribune/eu/finlande/pol/en.html>. Acesso em: 15 mar. 2007.

EUROPEAN COMISSION. **Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for Assisting Computer Security Incident Response Teams (CSIRTs)**. Bélgica: Rand Europe, 2003. Disponível em: <http://europa.eu.int/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf>. Acesso em: 11 jun. 2006.

_____. **Handbook of Legal Procedures of Computer and Network Misuse in EU Countries**, Bélgica: Rand Europe, 2006. Disponível em: <http://www.rand.org/pubs/technical_reports/2006/RAND_TR337.pdf>. Acesso em: 11 jun. 2006.

FARMER, D.; VENEMA, W. **Perícia Forense Computacional**. Tradução de Edson Furmankiewicz, Carlos Schafranski. Revisão Técnica de Pedro Luis Próspero Sanchez. São Paulo: Pearson Prentice Hall, 2007.

FERNANDES, A.S.; GOMES FILHO, A.M.; GRINOVER, A.P. **As Nulidades do Processo Penal**. 9. ed. rev. atual. e ampl. São Paulo: Editores Revista dos Tribunais, 2006.

GOLDSTEIN, D. **How Science Works**. In: FEDERAL JUDICIAL CENTER. Reference Manual on Scientific Evidence. 2. ed. Nova York: FJC, 2000, Disponível em: < http://air.f jc.gov/public/f jcweb.nsf/pages/16>. Acesso em: 04 jun. 2006.

GRANCE, T.; KENT, K.; KIM, B. **Computer Security Incident Handling Guide**. NIST National Institute of Standards and Technology. Gaithersburg, 2004.

HOUAISS. **Dicionário Eletrônico Houaiss da Língua Portuguesa**. Uol, São Paulo, 04 jun. 2006. Disponível em: <http://houaiss.uol.com.br >. Acesso em: 04 jun. 2006.

INFORMATION SOCIETY COMMISSION. **Building Trust through the Legal Framework**. Irlanda: ISC, 2007. Disponível em: <http://www.isc.ie/about/reports.html >. Acesso em: 15 mar. 2007

INTERPOL. **European police and judicial systems**. INTERPOL, França, 11 jun. 2006. Disponível em: < http://www.interpol.int/Public/Region/Europe/pjsystems/Default.asp >. Acesso em: 11 jun. 2006.

KRUSE,W.G.; HEISER, J.G. **Computer Forensics : Incident Response Essentials**. Indianapolis: Addison Wesley, 2001.

MALATESTA, N.F., **Lógica das Provas em Matéria Criminal, 3. ed**. São Paulo: Editora Bookseller, 2004.

MANDIA, K; PROSISE, C. **Hackers: Resposta e Contra-Ataque**. Rio de Janeiro: Editora Campus, 2001.

MARCELLA, A.J.; GREENFIELD, R.S. **Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.** Boca Raton: Auerbach Publication, 2002.

MARSICO, C.V. **Computer Evidence V. Daubert: The Coming Conflict**. Purdue University, West Lafayette, 2005.

MEUWLY, D. **L'Apport d'une Approche Automatique**. 2001. 272f. Tese (Doutorado em Ciências Forenses), Universidade de Lausanne, Lausanne - Suiça, 2001.

MINISTÉRIO DA JUSTIÇA FINLANDÊS. **The Penal Code of Finland**, Finlândia: FINLEX, 2007. Disponível em: <http://www.finlex.fi/en/laki/kaannokset/1889/en18890039?search%5Btype%5D=pika&search%5Bpika%5D=Rikoslaki>. Acesso em: 15 mar. 2007

MINISTÉRIO DA JUSTIÇA GREGO. **The Constitution of Greece**, Grécia: MINISTÉRIO DA JUSTIÇA GREGO, 2007. Disponível em: <http://www.ministryofjustice.gr/eu2003/indexENG.php>. Acesso em: 15 mar. 2007

MINISTÉRIO DA JUSTIÇA E INTERIOR MALTES. **Malta Laws**. Malta: MJIM, 2007. Disponível em: < http://www2.justice.gov.mt/lom/analytical_index.asp>. Acesso em: 15 mar. 2007

MINISTERIO DEL INTERIOR. **Dirección General de la Policía y de la Guardia Civil**. Espanha: MIR, 2007. Disponível em:

<http://www.mir.es/MIR/estrorganica/estructura/secestseg/dgpcivil1.html>. Acesso em: 15 mar. 2007

MINISTÉRIO DO INTERIOR FRANCES. **La lutte contre la cyber-criminalité et les fraudes aux cartes bancaires**. França: MINISTÉRIO DO INTERIOR FRANCES, 2007. Disponível em: <http://www.interieur.gouv.fr/sections/a_l_interieur/la_police_nationale/organisation/dcpj/cyber-criminalite >. Acesso em: 15 mar. 2007

MIRABETE, J. F. **Processo Penal. 18. ed. rev. atual. até 31 de dezembro de 2005. 3. reimpr**. São Paulo: Atlas, 2007.

MONET, J. C. **Polícias e Sociedades na Europa. 2. ed. 1. reimpr**. São Paulo: Editora da Universidade de São Paulo, 2007.

NISTIR 6014. **General Test Methodology for Computer Forensic Tools**. National Institute of Standards and Technology, Gaithersburg, MD, Novembro 2001, 8f.

NOLAN, R., et. Al. **First Responders Guide to Computer Forensics.** US-CERT: Pittisburg, 2005.

NOTÍCIAS AGÊNCIA FAPESP. **Mais fraudes na internet**. Agência FAPESP, São Paulo, 06 jan. 2006. Disponível em: <http://www.agencia.fapesp.br/boletim_dentro.php?data[id_materia_boletim]=4884>. Acesso em: 12 Abr. 2006

PALMER, G. **A Road Map for Digital Forensic Research**. In:Technical Report

DTR-T001-01, DFRWS, Novembro 2001

POLÍCIA FINLANDESA. **The Finnish Police**. Finlândia: POLIISI, 2007. Disponível em: < http://www.poliisi.fi/poliisi/home.nsf/ExternalFiles/THE%20FINNISH%20POLICE%20KORJ/$file/THE%20FINNISH%20POLICE%20KORJ.pdf>. Acesso em: 15 mar. 2007

POLÍCIA LITUANA. **Police Department under the Ministry of Interior**. Lituânia: POLÍCIA LITUANA, 2007. Disponível em: <http://www.policija.lt/En/>. Acesso em: 15 mar. 2007

PROCURADORIA GERAL DA IRLANDA, **European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy)**

Regulations 2003. Irlanda: OAG, 2007. Disponível em: < http://www.irishstatutebook.ie/ZZSI535Y2003.html>. Acesso em: 15 mar. 2007

PROENÇA, L.R. **Inquérito Civil: atuação investigativa do Ministério Público a serviço da ampliação do acesso à justiça**. São Paulo: Editora Revista dos Tribunais, 2001.

ROCHA, L.C. **Investigação Policial: teoria e prática**. 2. ed. São Paulo: Edipro, 2003.

REITH, M.; CARR, C.; GUNSH, G. **An Examination of Digital**

Forensics Models. In: International Journal of Digital Evidence (IJDE), 1(3),

Outono 2002.

SMITH, F.C.; BACE, R.G. **A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness**. Boston: Addison Wesley, 2003.

STEPHENSON, P. **Modeling of Post-Incident Root Cause Analysis**. International Journal of Digital Evidence (IJDE), 2(2), 2003.

STEPHENSON, P. **The Application of Formal Methods to Root Cause Analysis of Digital Incidents**. In: International Journal of Digital Evidence (IJDE), 3(1), 2004.

TRANSLATIONS AND TERMINOLOGY CENTRE – LAW. **Laws**. Letônia: TTC, 2007. Disponível em: < http://www.ttc.lv/index.php?id=50>. Acesso em: 15 mar. 2007

TRIBUNAIS DOS ESTADOS UNIDOS. **Commonly Used Terms**. U.S. Courts, Estados Unidos, 11 jun. 2006. Disponível em: < http://www.uscourts.gov/library/glossary.html#E>. Acesso em: 11 jun. 2006.

U.S. DOJ. **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.** United States Department of Justice, 2002.

VACCA, J.R. **Computer Forensics: Computer Crime Scene Investigation**. Massachusetts: Charles River Media, 2005.

10 ANEXO A – LEGISLAÇÃO APLICÁVEL NA UNIÃO EUROPÉIA

1. Alemanha

As infrações contra os pilares da segurança da informação, ou seja, contra a confidencialidade, a integridade e a disponibilidade são tratadas principalmente em seis artigos do código penal alemão (*Strafgesetzbuch-StGB*), promulgado em 1871, com última atualização em 2005, registrado até o momento da elaboração desse documento:

a) Espionagem digital – StGB art. 202 a;

b) Modificação de dados – StGB art. 303 a;

c) Sabotagem por Computador – StGB art. 303 b;

d) Fraude por Computador – StGB art. 263 a;

e) Falsificação de dados legais relevantes – StGB art. 269;

f) Fraude em Relações Legais através do Processamento de dados – StGB art. 270.

As infrações relacionadas a conteúdo ilícito, são tratadas nos seguintes artigos:

a) Incitação do povo – StGB art. 130;

b) Glorificação da Violência – StGB art. 131;

c) Disseminação de material pornográfico – StGB art. 184.

Os alemães dispõem de um tratado que lida com conteúdo prejudicial aos usuários da Internet, em especial aos menores de idade, o Tratado de Proteção de Menores na Mídia (*Jugendmedienschutz-Staatsvertrag - JMStV*).

Na taxonomia adotada pelo European Comission (2006), a Rastreamento (Scan) (Scan), os Códigos Maliciosos, o Comprometimento de conta e a Tentativa de Intrusão são consideradas atividades preparatórias para se cometer crime e por isso não considerados crimes passíveis de punição na Alemanha.

A Negação de Serviço, o acesso não-autorizado a transmissões, a modificação não-autorizada de informações e o acesso não-autorizado a sistemas de comunicações são crimes previstos pelo Código Penal Alemão, conforme art. 303

a, com pena de prisão de até 2 anos ou multa ou se no art. 303 b, prisão de até 5 anos ou multa.

O acesso não-autorizado a informações pode ainda estar previsto no artigo 202 a com pena de até 3 anos ou multa.

O Acesso não-autorizado a transmissões pode também ser tratado no art. 263 a, como dano a propriedade de outros resultando em processamento de dados com programas configurados de forma incorreta ou com dados incompletos, ou a influência não autorizada no fluxo de trabalho de forma a obter algum benefício de forma ilegal, com pena de até 5 anos ou multa.

O acesso não autorizado a transmissões pode também ser interpretado como uso da rede de telecomunicações pública não autorizado e sem a intenção de pagamento do serviço utilizado, com penda de até 1 ano ou multa.

O Spam não é considerado crime previsto em código penal, mas pode ser objeto de processo civil.

2. Áustria

A Áustria incluiu uma emenda no Código Penal Austríaco (*Strafgesetzbuch* - StGB) em 2002, constituída de novas tipificações e sanções aos crimes por computador já existentes no código como:

a) Acesso ilegal aos sistemas de computadores – StGB art. 118 a;

b) Violação do sigilo de telecomunicações – StGB art. 119;

c) Interceptação de dados – StGB art. 119 a;

d) Danos dos dados e aos sistemas de computadores – StGB art. 126 a;

e) Abuso de software ou direitos de acesso – StGB art. 126 b;

f) Abuso fraudulento do processamento automatizado de dados – StGB art. 148 a;

g) Falsificação de dados de computador – StGB art. 225 a.

Além dos crimes previstos no Código Penal, a Áustria dispõe de leis que contêm dispositivos específicos relacionados à informática, como por exemplo:

a) Na Lei de Proteção de Dados (DSG - Datenschutzgesetz):
    i. Art. 1 e 15 dispõem sobre o sigilo dos dados pessoais;
    ii. Art. 52 trata das penas administrativas relacionadas ao sigilo e segurança de dados pessoais;
    iii. Art. 51 dispõe sobre o uso de dados pessoais com a intenção de obter lucro ou ocasionar danos.
b) Na Lei de Telecomunicações (TKG - Telekommunikationsgesetz):
    i. Art. 90 Abs 6 – Deveres da divulgação (duty of disclosure);
    ii. Art. 93 – Sigilo da comunicação;
    iii. Art. 107 – Spam;
    iv. Arts. 96 a 99 – Sigilo de dados;
    v. Arts. 108 a 111 – Dispõem sobre as sanções.
c) Na Lei de Mídias (MedienG - Mediengesetz): Art. 28 - Delitos por conteúdo de mídia;
d) Na Lei de e-Commerce (ECG - E-Commerce-Gesetz):
    i. Art. 13 a 19 – Tratam das obrigações dos provedores;
    ii. Art. 6 a 7 e 26 – Spam;
    iii. Art. 18 - Deveres da divulgação (duty of disclosure).
e) Na Lei de Direitos Autorais (UrhG - Urheberrechtsgesetz): Arts. 90 b a 90 d e 91 – proteção de software e controles técnicos.
f) Lei de Controle de Acesso (ZuKG - Zugangskontrollgesetz): Art. 10.
g) Lei de Assinatura Digital (SigG - Signaturgesetz): O art. 26 dispõe sobre o mau uso de chaves privadas.

Os delitos que são cometidos com o auxílio de computadores podem ser enquadrados em leis que não são específicas, principalmente nos crimes que se utilizam da Internet para divulgação de conteúdo proibido, como por exemplo:

a) Pedofilia, conforme art. 207a do Código Penal Austríaco, o StGB – Strafgesetzbuch;

b) Delitos relacionados ao nazismo, de acordo com o art. 3 da Lei de Delitos do Nazismo (VerbotsG – Verbotsgesetz);

c) Fraude, conforme o art. 146 do Código Penal Austríaco (StGB – Strafgesetzbuch);

d) Chantagem, de acordo com o art. 144 do Código Penal Austríaco (StGB – Strafgesetzbuch).

Os incidentes levantados pela European Comission (2006) podem ser enquadrados pela legislação austríaca da seguinte forma:

a) Rastreamento (Scan) – não é considerado delito, uma vez que não ocorreu intrusão;

b) Acesso não-autorizado a transmissões

   i. art. 119a do Código Penal – Interceptação abusiva de dados, com pena prevista de prisão até 6 meses ou de multa de até 360 tarifas diárias;

   ii. art. 119a do Código Penal – Violação do sigilo de telecomunicação. A pena prevista para esse delito é de prisão de até 6 meses ou de multa de até 360 tarifas diárias;

   iii. art. 120 parágrafo 2a do Código Penal – Uso abusivo da comunicação. Prisão de até 3 meses ou multa de até 180 tarifas diárias;

   iv. Dependendo do objetivo de uso do código malicioso, a infração poderá ser enquadrada de acordo com as ações resultantes, como por exemplo, quebra de sigilo de informações pessoais, previsto no art. 51, 52 da Lei de Proteção de dados (DSG – Datenschutzgesetz) ou art. 123 do Código Penal Austríaco.

c) Acesso não-autorizado a informações

   i. art. 118 do StGB – se considerado acesso não autorizado a sistema de computador com a intenção de obter ganho ou ocasionar dano, com pena de prisão de até 6 meses ou de multa de até 360 tarifas diárias;

ii. art. 13 da Lei de Controle de Acesso (ZuKG) – Uso profissional de forma intencional ou propaganda para o uso de medidas para ludibriar controles de acesso. Sanção administrativa com multa de até 15000 euros.

iii. art. 51 da Lei de Proteção de Dados (DSG) – uso de dados pessoais com a intenção de obter ganho ou ocasionar dano, com pena de prisão de até 1 ano;

iv. art. 52 da Lei de Proteção de Dados (DSG) – Acesso não autorizado de sistemas de dados pessoais. Sanção administrativa com multa em até 18890 euros;

v. art. 123 do StGB – exploração de segredos de negócios, com pena de prisão de até 2 anos ou de multa de até 360 tarifas diárias.

d) Modificação não-autorizada de Informação

i. art. 126a do StGB – Ação deliberada que ocasione danos a dados, com pena de até 6 meses ou de multa de até 360 tarifas diárias. Se o delito for enquadrado na qualificação 1, ou seja, a vítima foi prejudicada em perda de mais de 3000 euros, a pena é de prisão de até 6 anos ou multa de até 360 tarifas diárias. Caso seja considerado de qualificação 2, ou seja, a vítima teve perda de mais de 50000 euros, a sanção é composta somente de prisão, de 6 meses a 5 anos.

ii. art. 148a do StGB – Abuso fraudulento do processamento de dados. As sanções previstas incluem prisão de até 6 meses ou de multa de até 360 tarifas diárias. Se o delito for enquadrado na qualificação 1, ou seja, a ação foi profissional ou a vítima foi prejudicada em perda de mais de 3000 euros, a pena é de prisão de até 6 anos ou multa de até 360 tarifas diárias. Caso seja considerado de qualificação 2, ou seja, a vítima teve perda de mais de 50000 euros, a sanção é composta somente de prisão, de 1 a 10 anos;

iii. art. 225ª do StGB – Falsificação de dados, a sanção é de prisão de até 1 ano;

iv. Dependendo do objetivo de uso do código malicioso, a infração poderá ser enquadrada de acordo com as ações resultantes, como por exemplo, a falsificação de documentos, prevista no art. 223 ou fraude previsto no art. 148 do Código Penal Austríaco.

e) Código Malicioso

i. art. 118 do StGB – se considerado acesso não autorizado a sistema de computador com a intenção de obter ganho ou ocasionar dano, com pena de prisão de até 6 meses ou de multa de até 360 tarifas diárias. Na Áustria, as multas podem ser cobradas em tarifas unitárias (como a Ufir no Brasil) que podem variar de 2 a 500 euros, aplicados de acordo com a situação financeira do infrator;

ii. art. 126a do StGB – Ação deliberada que ocasione danos a dados, com pena de até 6 meses ou de multa de até 360 tarifas diárias. Se o delito for enquadrado na qualificação 1, ou seja, a vítima foi prejudicada em perda de mais de 3000 euros, a pena é de prisão de até 6 anos ou multa de até 360 tarifas diárias. Caso seja considerado de qualificação 2, ou seja, a vítima teve perda de mais de 50000 euros, a sanção é composta somente de prisão, de 6 meses a 5 anos.

iii. Dependendo do objetivo de uso do código malicioso, a infração poderá ser enquadrada de acordo com as ações resultantes, como por exemplo, quebra de sigilo de informações pessoais, previsto no art. 51 da Lei de Proteção de dados (DSG – Datenschutzgesetz) ou a interrupção da operacionabilidade de computadores, previsto no art. 126 do Código Penal Austríaco.

f) Negação de Serviço – é crime previsto no art. 126 do Código Penal Austríaco, considerado interrupção da operacionabilidade de sistemas, com pena de prisão de até 6 meses ou multa de até 360 tarifas diárias.

g) Comprometimento de conta

i. art. 118 do StGB – se considerado acesso não autorizado a sistema de computador com a intenção de obter ganho ou ocasionar dano, com pena de prisão de até 6 meses ou de multa de até 360 tarifas diárias;

ii. art. 126c do StGB – Abuso no acesso a dados, com pena de até 6 meses ou de multa de até 360 tarifas diárias.

iii. art. 52 da Lei de Proteção de Dados (DSG) – Acesso não autorizado de sistemas de dados pessoais. Sanção administrativa com multa em até 18890 euros.

iv. art. 10 da Lei de Controle de Acesso (ZuKG) – Venda ou locação de mecanismos para ludibriar controles de acesso. Multa de até 15000 euros.

v. art. 13 da Lei de Controle de Acesso (ZuKG) – Uso profissional de forma intencional ou propaganda para o uso de medidas para ludibriar controles de acesso. Sanção administrativa com multa de até 15000 euros.

vi. art. 26 Lei de Assinatura Digital (SigG - Signaturgesetz) – mau uso de assinatura digital em criação de dados. Sanção administrativa com multa de até 4000 euros.

h) Tentativa de Intrusão – na legislação austríaca, pode ser considerada ações preparatórias previstas no art. 126c do Código Penal e nos arts. 10 e 13 da Lei de Controle de Acesso.

i) Acesso não-autorizado a sistemas

i. art. 119a do Código Penal – Interceptação abusiva de dados, com pena prevista de prisão até 6 meses ou de multa de até 360 tarifas diárias;

ii. art. 119a do Código Penal – Violação do sigilo de telecomunicação. A pena prevista para esse delito é de prisão de até 6 meses ou de multa de até 360 tarifas diárias;

iii. art. 120 parágrafo 2a do Código Penal – Uso abusivo da comunicação. Prisão de até 3 meses ou multa de até 180 tarifas diárias;

iv. art. 93 do Código Penal e art. 108 da Lei de Telecomunicações – Violação do sigilo da comunicação pelo provedor de comunicações. A pena prevista é de até 6 meses de prisão ou de multa de até 360 tarifas diárias;

v. Dependendo do objetivo de uso do código malicioso, a infração poderá ser enquadrada de acordo com as ações resultantes, como por exemplo, acesso não autorizado a sistemas, previsto no art. 118 do Código Penal Austríaco.

j) Spam – art. 107 parágrafo 2 em conjunto com o art. 109 parágrafo 3, num. 19 a 21 da Lei de Telecomunicações (TKG) – Correio eletrônico não solicitado. Multa de até 37.000 euros.

3. Bélgica

A Bélgica possui alguns dispositivos legais específicos quando os mecanismos tradicionais não são suficientes nos crimes que envolvem informática.

A falsificação por informática, fraude por informática, manipulação de dados e hacking, além de medidas como apreensão de dados, busca em rede e perícia e também a obrigatoriedade na retenção de dados nas operações dos provedores de serviço de comunicações foram recentemente introduzidas na legislação belga.

A legislação belga conta também com leis específicas como por exemplo, as que tratam de spam, da interferência nas comunicações militares e do acesso não-autorizado e deliberado às informações da base de dados da segurança social nacional.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação belga:

a) Rastreamento (Scan) – se considerada interceptação de dados ou comunicação privada sem o consentimento das partes envolvidas, é

crime previsto no Código Pena Belga, art. 314bis. A pena é de prisão de 1 ano ou 2 anos se o infrator for oficial do governo e/ou multa de até 50.000 euros;

b) Código Malicioso

   i. art. 210bis do Código Penal – se considerado modificação ou exclusão de dados eletrônicos de forma que o escopo legal seja alterado e o uso deliberado de tais dados. Pena de 6 meses a 5 anos e/ou multa de até 500.000 euros. Se forem considerados apenas tentativas, a pena cairá para 6 meses a 3 anos e / ou multa de até 250.000 euros;

   ii. art. 550bis do Código Penal – se considerado danos em sistema de computador ou nos dados armazenados, causados por modificação em sistema através de acesso não autorizado, mesmo sem a intenção. Pena de 1 a 3 anos e/ou multa de até 250.000 euros;

c) Negação de Serviço – art. 210bis do Código Penal, se considerado modificação ou exclusão de dados eletrônicos de forma que o escopo legal seja alterado e o uso deliberado de tais dados. Pena de 6 meses a 5 anos e/ou multa de até 500.000 euros. Se forem considerados apenas tentativas, a pena cairá para 6 meses a 3 anos e / ou multa de até 250.000 euros;

d) Comprometimento de conta - art. 550bis do Código Penal – se considerado danos em sistema de computador ou nos dados armazenados, causados por modificação em sistema através de acesso não autorizado, mesmo sem a intenção. Pena de 1 a 3 anos e/ou multa de até 250.000 euros;

e) Tentativa de Intrusão – se forem consideradas medidas preparatórias visando o acesso não autorizado, podem ser enquadradas no art. 550bis do Código Penal Pena de 6 meses a 3 anos e/ou multa de até 500.000 euros.

f) Acesso não-autorizado a informações

i. art. 550bis do Código Penal:

1. Se considerado acesso ou manutenção de acesso não autorizado a sistemas de computadores, mesmo que não intencional. Pena de prisão de 3 meses a 1 ano (2 anos se o delito for considerado intencional) e/ou multa de até 125.000 euros;

2. Se considerado abuso intencional dos direitos de acesso por usuário que possua acesso autorizado ao sistema. Pena de 6 meses a 2 anos de prisão ou multa de até 125.000 euros;

ii. art. 314bis do Código Penal, – se considerada interceptação de dados ou comunicação privada sem o consentimento das partes envolvidas. A pena é de prisão de 1 ano ou 2 anos se o infrator for oficial do governo e/ou multa de até 50.000 euros;

g) Acesso não-autorizado a transmissões

i. art. 314bis do Código Penal:

1. Se considerado acesso ou manutenção de acesso não autorizado a sistemas de computadores, mesmo que não intencional. Pena de prisão de 3 meses a 1 ano (2 anos se o delito for considerado intencional) e/ou multa de até 125.000 euros;

2. Se considerado abuso intencional dos direitos de acesso por usuário que possua acesso autorizado ao sistema. Pena de 6 meses a 2 anos de prisão ou multa de até 125.000 euros;

h) Modificação não-autorizada de Informação: se considerado modificação ou exclusão de dados eletrônicos de forma que o escopo legal seja alterado e o uso deliberado de tais dados. Pena de 6 meses a 5 anos e/ou multa de até 500.000 euros. Se forem considerados apenas tentativas, a pena cairá para 6 meses a 3 anos e / ou multa de até 250.000 euros, conforme o art. 210bis do Código Penal;

i) Acesso não-autorizado a sistemas de comunicações

i. art. 550bis do Código Penal:

3. Se considerado acesso ou manutenção de acesso não autorizado a sistemas de computadores, mesmo que não intencional. Pena de prisão de 3 meses a 1 ano (2 anos se o delito for considerado intencional) e/ou multa de até 125.000 euros;

1. Se considerado abuso intencional dos direitos de acesso por usuário que possua acesso autorizado ao sistema. Pena de 6 meses a 2 anos de prisão ou multa de até 125.000 euros;

j) Spam - O uso de correio eletrônico para propaganda sem o consentimento específico, livre e antecipado do destinatário é proibido de acordo com o art. 14 da Lei de 11 de Março de 2003, com multa prevista de até 125.000 euros.

4. Chipre

O Chipre conta com várias leis específicas para lidar com infrações que envolvam informática.

Além de ter sido sancionada em 2004 uma lei de ratificação da Convenção de Crimes Cibernéticos de 2001, o Chipre conta com, entre outros:

a) Lei de Proteção do Sigilo das Comunicações Privadas, de 1996, que proíbe a interceptação não autorizada de comunicações privadas;

b) Lei de Regulamentação das Comunicações e Serviços Postais Eletrônicos, que proíbe a escuta, interceptação, armazenamento e quaisquer outros tipos de monitoração da comunicação sem o consentimento das pessoas que estão se comunicando;

c) Lei de Processamento de Dados Pessoais – penaliza spam e a interferência não autorizada nos registros de dados pessoais. No entanto, em investigações, essa lei dá poderes aos oficiais de proteção de dados pessoais para a busca e checagem de informações necessárias à investigação;

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação cipriota:

a) Rastreamento (Scan) – é considerada ilegal exceto se efetuada por autoridade competente em cumprimento da legislação, como por exemplo, para monitoramento do acesso a informações confidenciais. A pena é multa de até 8.700 euros (CYP 5.000);

b) Código Malicioso

    i. Seção 4 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado acesso ilegal, sem autorização e com a intenção de ganhar acesso ao todo ou parte de sistema computacional através da quebra de mecanismos de segurança. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

    ii. Seção 6 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado interferência em informações intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

    iii. Seção 7 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado interferência em sistema computacional de forma intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

    iv. Seção 8 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerada produção, venda, aquisição para uso, importação, distribuição ou ainda a disponibilização de:

        i. Dispositivos concebidos ou adaptados com o propósito de cometer infrações relacionadas ao acesso, interceptação ou interferências de dados ou sistemas de forma ilegal. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

ii. Senhas, códigos de acesso ou dados similares para acesso ao todo ou parte de sistema computacional para cometer infrações relacionadas ao acesso, interceptação ou interferências de dados ou sistemas de forma ilegal. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

v. Seção 10 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerada a inclusão, modificação, exclusão ou supressão de dados computacionais que ocasione danos à propriedade alheia com intenção desonesta ou fraudulenta, resultando em aquisições não autorizadas em benefício próprio ou de terceiros. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

c) Negação de Serviço

i. Seção 6 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado interferência em informações intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

ii. Seção 7 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado interferência em sistema computacional de forma intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

d) Comprometimento de conta - Seção 4 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético: se considerado acesso ilegal, sem autorização e com a intenção de ganhar acesso ao todo ou parte de sistema computacional através da quebra de mecanismos de

segurança. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

e) Tentativa de Intrusão

   i. Seção 4 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético - acesso ilegal, sem autorização e com a intenção de ganhar acesso ao todo ou parte de sistema computacional através da quebra de mecanismos de segurança. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

   ii. Seção 14 da Lei de Proteção do Sigilo das Comunicações Privadas

      i. Interceptação de comunicação privada intencionalmente. Pena de até 3 anos;

      ii. Uso de mecanismos eletromagnéticos, mecânicos, eletrônicos ou quaisquer máquinas com a finalidade de interceptação de comunicação privada. Pena de até 3 anos;

      iii. Tentativa de ou divulgação intencional de informação de comunicação privada. Pena de até 3 anos;

      iv. Tentativa de ou uso intencional de informação de comunicação privada. Pena de até 3 anos;

f) Acesso não-autorizado a informações

   i. Seção 4 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético - acesso ilegal, sem autorização e com a intenção de ganhar acesso ao todo ou parte de sistema computacional através da quebra de mecanismos de segurança. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

   ii. Seção 9 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético - acesso ilegal, sem autorização e com a intenção de fraude. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

iii. Seção 14 da Lei de Proteção do Sigilo das Comunicações Privadas

i. Interceptação de comunicação privada intencionalmente. Pena de até 3 anos;

ii. Uso de mecanismos eletromagnéticos, mecânicos, eletrônicos ou quaisquer máquinas com a finalidade de interceptação de comunicação privada. Pena de até 3 anos;

iii. Tentativa de ou divulgação intencional de informação de comunicação privada. Pena de até 3 anos;

iv. Tentativa de ou uso intencional de informação de comunicação privada. Pena de até 3 anos;

g) Acesso não-autorizado a transmissões

i. Seção 5 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado interferência em informações intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

ii. Seção 14 da Lei de Proteção do Sigilo das Comunicações Privadas

i. Uso de mecanismos eletromagnéticos, mecânicos, eletrônicos ou quaisquer máquinas com a finalidade de interceptação de comunicação privada. Pena de até 3 anos;

iii. Seção 99 da Lei de Comunicações Eletrônicas – a interceptação ou quaisquer formas de vigilância de comunicações sem o consentimento dos envolvidos. Pena de até 6 meses de prisão e/ou multa de até 1.740 euros (CYP 1.000);

h) Modificação não-autorizada de Informação: Seção 6 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado

interferência em informações intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

i) Acesso não-autorizado a sistemas de comunicações

   i. Seção 7 da Lei de 2004 da Ratificação da Convenção em Crime Cibernético – se considerado interferência em sistema computacional de forma intencional e sem permissão de acesso, ocasionando dano, exclusão, deterioração, modificação ou supressão de dados. Pena de até 5 anos de prisão e/ou multa de até 34.000 euros (CYP 20.000);

   ii. Seção 14 da Lei de Proteção do Sigilo das Comunicações Privadas

      i. Interceptação de comunicação privada intencionalmente. Pena de até 3 anos;

      ii. Uso de mecanismos eletromagnéticos, mecânicos, eletrônicos ou quaisquer máquinas com a finalidade de interceptação de comunicação privada. Pena de até 3 anos;

      iii. Tentativa de ou divulgação intencional de informação de comunicação privada. Pena de até 3 anos;

      iv. Tentativa de ou uso intencional de informação de comunicação privada. Pena de até 3 anos;

j) Spam

   i. Seção 106 da Lei de Comunicações Eletrônicas – uso de sistemas automatizados de chamada sem a intervenção humana, fax, correio eletrônico ou mensagens SMS para finalidades de marketing direto sem o consentimento prévio do destinatário. Pena de até 6 meses de prisão e/ou multa de até 1.740 euros (CYP 1.000);

ii. Seção 15 da Lei de Proteção de Dados – Processamento de dados para promoção, venda ou disponibilização de serviços sem consentimento. Multa de até 8.700 euros (CYP 5.000) e/ou aviso para encerrar a violação em prazo determinado e/ou destruição dos registros ou suspensão e destruição de dados.

5. Dinamarca

A Dinamarca possui leis específicas que tratam de crimes de informática, mas também possui atualizações em seu Código Penal, efetuadas em 2002, que incluem dispositivos sobre crime cibernético.

Apesar da atualização efetuada que introduziu novos tipos de atividades criminais, a legislação existente e que não é específica à informática pode cobrir crimes cibernéticos.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação dinamarquesa:

a) Rastreamento (Scan) – não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

   i. Art. 193 do Código Penal – se o código malicioso ocasionar grandes distúrbios nas operações de meios de comunicações públicos, incluindo serviços telefônicos, instalações e sistemas de informação, é considerado crime com pena de até 6 anos de prisão. A pena pode ser reduzida a 6 meses se for identificado que houve negligência em vez de intenção ou multa;

   ii. Art. 291 do Código Penal – a destruição ou exclusão de objetos de terceiros é considerado crime com pena de 6 meses a 1 ano de prisão. Se houve dano significante, de natureza sistemática ou organizada, a pena pode ser ampliada para 6 anos. Se for identificado que houve negligência em vez de intenção a pena poderá ser reduzida para 6 meses de prisão ou multa;

c) Negação de Serviço

i. Art. 193 do Código Penal – se o código malicioso ocasionar grandes distúrbios nas operações de meios de comunicações públicos, incluindo serviços telefônicos, instalações e sistemas de informação, é considerado crime com pena de até 6 anos de prisão. A pena pode ser reduzida a 6 meses se for identificado que houve negligência em vez de intenção ou multa;

ii. Art. 263(2) do Código Penal – o acesso ilegal a informações ou a programas de sistemas de informação de terceiros é crime com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

d) Comprometimento de conta

i. Art. 169(a) do Código Penal – a produção, obtenção ou a distribuição de dinheiro falso com o intuito de utilizá-lo como autêntico é crime com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

ii. Art. 263(2) do Código Penal – o acesso ilegal a informações ou a programas de sistemas de informação de terceiros é crime com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

e) Tentativa de Intrusão

i. Art. 263(2) do Código Penal – o acesso ilegal a informações ou a programas de sistemas de informação de terceiros é crime com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

ii. Art. 293(2) do Código Penal – a obstrução ilegal do acesso de uma pessoa a um objeto é crime com pena de 1 ano de prisão que pode ser aumentada para 2 anos;

f) Acesso não-autorizado a informações

i. Art. 263(a) do Código Penal:

a. a venda ou distribuição ilegal de código ou outro meio de acesso a sistema de informações privado, cujo acesso é protegido;

b. passar adiante códigos ou outros meios de acesso a sistema de informações privado, cujo acesso é protegido;

c. a aquisição ou distribuição de códigos ou outros meios de acesso a sistema de informações público vital ou sistema de processamento de informações pessoais sigilosas ou informações pessoais de vários indivíduos.

São crimes com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

ii. Art. 263(1) do Código Penal:

a. Privar um indivíduo de comunicação confidencial, quebrar o sigilo dessa comunicação ou divulgar o conteúdo da comunicação;

b. Obter acesso a local de armazenamento de propriedade pessoal;

c. Escuta ou gravação de comunicação de forma ilegal;

São crimes com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

iii. Art. 263(2) do Código Penal – obter acesso ilegalmente a informações ou programas de terceiros com o intuito de ser utilizado em um sistema de informação (medidas preparatórias para acesso não autorizado). A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

iv. Art. 301 do Código Penal - Produção, aquisição ou distribuição de informação que identifique um meio de pagamento de terceiros ou números de cartão, com o propósito de uso ilegal dessas informações. A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

v. Art. 301(a) do Código Penal - obter acesso ou distribuir informações ilegalmente relacionados a códigos ou outros meios de acesso a um sistema de informação, cujo acesso é reservado para pagamentos de usuários, onde o acesso é protegido por código ou outros requisitos de acesso específicos. A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

g) Acesso não-autorizado a transmissões

i. Art. 263(1) do Código Penal:

a. Privar um indivíduo de comunicação confidencial, quebrar o sigilo dessa comunicação ou divulgar o conteúdo da comunicação;

b. Obter acesso a local de armazenamento de propriedade pessoal;

c. Escuta ou gravação de comunicação de forma ilegal;

São crimes com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

ii. Art. 263(2) do Código Penal – obter acesso ilegalmente a informações ou programas de terceiros com o intuito de ser utilizado em um sistema de informação (medidas preparatórias para acesso não autorizado). A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

h) Modificação não-autorizada de Informação

i. Art. 171 do Código Penal – uso de documento falso como prova, inclusive documentos eletrônicos. A pena é de até 2 anos de prisão que pode ser aumentada para 6 anos;

ii. Art. 175 do Código Penal – uso de declarações falsas, que podem estar em qualquer tipo de mídia. A pena é de até 3 anos de prisão ou multa;

iii. Art. 263(2) do Código Penal – obter acesso ilegalmente a informações ou programas de terceiros com o intuito de ser

utilizado em um sistema de informação (medidas preparatórias para acesso não autorizado). A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

iv. Art. 279(a) do Código Penal – modificar ou excluir informações ou programas para o processamento de dados eletrônico com o intuito ilegal de obter lucro ou qualquer outro resultado que afete o resultado desse processamento;

i) Acesso não-autorizado a sistemas de comunicações

i. Art. 263(a) do Código Penal:

a. a venda ou distribuição ilegal de código ou outro meio de acesso a sistema de informações privado, cujo acesso é protegido;

b. passar adiante códigos ou outros meios de acesso a sistema de informações privado, cujo acesso é protegido;

c. a aquisição ou distribuição de códigos ou outros meios de acesso a sistema de informações público vital ou sistema de processamento de informações pessoais sigilosas ou informações pessoais de vários indivíduos.

São crimes com pena de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

ii. Art. 263(2) do Código Penal – obter acesso ilegalmente a informações ou programas de terceiros com o intuito de ser utilizado em um sistema de informação (medidas preparatórias para acesso não autorizado). A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

iii. Art. 301 do Código Penal - Produção, aquisição ou distribuição de informação que identifique um meio de pagamento de terceiros ou números de cartão, com o propósito de uso ilegal dessas informações. A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

iv. Art. 301(a) do Código Penal - obter acesso ou distribuir informações ilegalmente relacionados a códigos ou outros meios de acesso a um sistema de informação, cujo acesso é reservado para pagamentos de usuários, onde o acesso é protegido por código ou outros requisitos de acesso específicos. A pena é de 6 meses a 1 ano de prisão que poderá ser aumentada para 6 anos;

j) Spam – Art. 6ª da Lei de Marketing – não é permitida a abordagem via correio eletrônico, sistemas automáticos de chamada ou fax, sem o consentimento do consumidor. Os processos contra esse tipo atividade poderá ocorrer no âmbito civil.

6. Eslováquia

Na Eslováquia, o código penal sofreu reformas iniciadas em 1991 para a inclusão de crimes cibernéticos.

Não há legislação específica para spams na Eslováquia, mas essa atividade pode estar sujeita aos regulamentos da Lei de Propaganda, do Código Comercial ou a processo civil.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação eslovaca:

a) Rastreamento (Scan) – não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

i. Seção 257a do Código Penal – o acesso, alteração ou exclusão de dados armazenados ou ainda modificações efetuadas nos sistemas de forma intencional e não autorizada com o intuito de ocasionar danos ou lucro para si mesmo ou para terceiros. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500

vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

ii. Seção 249 do Código Penal – o uso não autorizado de pertences de terceiros. A pena pode ser de até 1 ano de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

iii. Seção 182(1)(a) do Código Penal – prejudicar ou colocar em risco a operação de instalações de telecomunicações. A pena pode ser de até 6 anos de prisão ou multa de até SKK 5.000.000 ou 130.000 euros;

c) Negação de Serviço

i. Seção 257a do Código Penal – o acesso, alteração ou exclusão de dados armazenados ou ainda modificações efetuadas nos sistemas de forma intencional e não autorizada com o intuito de ocasionar danos ou lucro para si mesmo ou para terceiros. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

ii. Seção 182(1)(a) do Código Penal – prejudicar ou colocar em risco a operação de instalações de telecomunicações. A pena pode ser de até 6 anos de prisão ou multa de até SKK 5.000.000 ou 130.000 euros;

d) Comprometimento de conta

i. Seção 257a do Código Penal – o acesso, alteração ou exclusão de dados armazenados ou ainda modificações efetuadas nos sistemas de forma intencional e não autorizada com o intuito de ocasionar danos ou lucro para si mesmo ou para terceiros. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

ii. Seção 249 do Código Penal – o uso não autorizado de pertences de terceiros. A pena pode ser de até 1 ano de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

e) Tentativa de Intrusão

i. Seção 257a junto da seção 8 do Código Penal – Tentativa de ganhar acesso e uso de dados sem autorização de acesso. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

ii. Seção 249 junto da seção 8 do Código Penal – o uso não autorizado de pertences de terceiros. A pena pode ser de até 1 ano de prisão. Se o crime for cometido por um grupo organizado

ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

f) Acesso não-autorizado a informações

   i. Seção 257a junto com a Seção 8 do Código Penal – Tentativa de acesso e uso de dados sem autorização com a intenção de causar dano, destruir ou tornar os dados inúteis. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

   ii. Seção 257a junto com a Seção 8 do Código Penal – Tentativa de quebrar o sigilo de comunicação privada ou dados dessa comunicação com a intento de ocasionar danos. A pena pode variar de 6 meses a 3 anos e multa de até SKK 5.000.000 ou 130.000 euros;

g) Acesso não-autorizado a transmissões

   i. Seção 257a do Código Penal – Tentativa de ganhar acesso e uso de dados sem autorização com a intenção de causar dano. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

ii. Seção 239 do Código Penal – Quebra do sigilo de mensagens transmitidas por telefone, telégrafo ou serviços públicos similares. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

iii. Seção 240 do Código Penal – Divulgação de conteúdo confidencial de mensagens ou abuso de tais mensagens. Prisão de até 1 ano e multa de até SKK 5.000.000 ou 130.000 euros;

iv. Seção 240(a) do Código Penal – Produção ou receptação de dispositivos técnicos que possibilitem a quebra do sigilo de mensagens transmitidas por telefone, telégrafo ou serviços públicos similares. A pena pode ser de até 3 anos de prisão e multa de até SKK 5.000.000 ou 130.000 euros;

v. Seção 182(1)(a) do Código Penal – prejudicar ou colocar em risco a operação de instalações de telecomunicações. A pena pode ser de até 6 anos de prisão ou multa de até SKK 5.000.000 ou 130.000 euros;

h) Modificação não-autorizada de Informação

i. Seção 257a do Código Penal – Tentativa de ganhar acesso e uso de dados sem autorização com a intenção de causar dano. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

i) Acesso não-autorizado a sistemas de comunicações

i. Seção 257a do Código Penal – Ganhar acesso e uso de dados sem autorização com a intenção de causar dano com hardware ou software de computador particular. A pena pode ser de 6 meses a 3 anos de prisão. Se o crime for cometido por um grupo organizado ou se a infração causou dano sérios (mais de 100 vezes o salário mínimo, ou seja, um valor de SKK 650.000 ou aproximadamente 16.600 euros), a pena poderá ser aumentada para 1 a 5 anos. Se ocasionar dano maior que 500 vezes o salário mínimo, então a pena de prisão poderá ser de 2 a 8 anos e multa de até SKK 5.000.000 ou 130.000 euros;

ii. Seção 182(1)(a) do Código Penal – prejudicar ou colocar em risco a operação de instalações de telecomunicações. A pena pode ser de até 6 anos de prisão ou multa de até SKK 5.000.000 ou 130.000 euros;

j) Spam

i. Seção 3(6) da Lei de Propaganda – não é permitido o uso de correio eletrônico para comunicação comercial sem o prévio consentimento do destinatário. Para essa infração, podem incorrer multas de até SKK 2.000.000 (aproximadamente 2.000 euros).

ii. Seção 178(1) do Código Penal – Se considerado processamento não autorizado de dados pessoais. A pena pode chegar a 1 ano de prisão e multa de até SKK 5.000.000 (aproximadamente 130.000 euros).

7. Eslovênia

A Eslovênia possui modificações no Código Penal que incluíram dispositivos específicos para crimes que envolvem informática, como o acesso não autorizado a sistemas de informação, a interrupção de sistemas de informação e a fabricação e aquisição de armas e instrumentos para cometer crime.

Além dessas inclusões no Código Penal, a Eslovênia possui leis específicas como a Lei de Comunicações Eletrônicas e a Lei de Proteção do Consumidor que podem ser aplicadas ao spam e a Lei de Assinatura

Eletrônica e Comércio eletrônico que penaliza infrações relacionadas às autoridades certificadoras.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Eslovênia:

a) Rastreamento (Scan) – não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;
b) Código Malicioso
    i. Art. 309, §3 do Código Penal – a posse, fabricação, venda, disponibilização, importação, exportação ou quaisquer outros meios para o provimento de dispositivos para a invasão ou acesso ilegal de um sistema com a intenção de cometer crime. A pena pode chegar a 1 no de prisão;
c) Negação de Serviço
    i. Art. 225, §2 do Código Penal – obstrução da transferência de dados ou da operação de sistemas sem autorização. A pena é de prisão de até 2 anos e pode ser aumentada para 5 anos de acordo o dano material ocasionado;
    ii. Art. 242, §1 do Código Penal – obstrução da transferência de dados ou da operação de sistemas sem autorização com a intenção de obter benefício pecuniário próprio ou de dano pecuniário a terceiro. A pena é de prisão de até 2 anos e pode ser aumentada para 5 anos de acordo o dano material ocasionado;
d) Comprometimento de conta – De acordo com o art. 225, §1 do Código Penal esloveno, o acesso a um sistema de informação sem autorização é infração com multa de 125 a 12.500 euros e pode ser aumentado em até 37.500 euros conforme a intenção do crime;
e) Tentativa de Intrusão - De acordo com o art. 225, §3 do Código Penal esloveno, a tentativa de cometer quaisquer das infrações descritas no art. 225, §2 é crime com acesso com pena de prisão de até 2 anos que pode ser aumentada para 5 anos de acordo o dano material ocasionado;

f) Acesso não-autorizado a informações

   i. Art. 154, §2 do Código Penal – invadir base de dados de computador para ter acesso a dados pessoais. A pena é de até 1 ano ou multa;

   ii. Art. 225, §2 do Código Penal – uso sem autorização de dados de sistemas de informação. A pena é de prisão de até 2 anos e pode ser aumentada para 5 anos de acordo o dano material ocasionado;

   iii. Art. 242, §1 do Código Penal – obstrução da transferência de dados ou da operação de sistemas sem autorização com a intenção de obter benefício pecuniário próprio ou de dano pecuniário a terceiro. A pena é de prisão de até 2 anos e pode ser aumentada para 5 anos de acordo o dano material ocasionado;

g) Acesso não-autorizado a transmissões

   i. Art. 225, §1 do Código Penal – a interceptação de dados de natureza privada transferidos através de sistema de informação é infração suscetível a multa de 125 a 12.500 euros e pode ser aumentado em até 37.500 euros conforme a intenção do crime;

   ii. Art. 150, §2 do Código Penal – ter acesso intencional ao conteúdo de mensagem transmitida por telefone ou quaisquer outros meios de telecomunicações através de meios técnicos. A pena é de até 1 ano ou multa;

h) Modificação não-autorizada de Informação

   i. Art. 225, §2 do Código Penal – alteração de dados armazenados ou obstruir a transmissão de dados sem autorização. A pena é de prisão de até 2 anos e pode ser aumentada para 5 anos de acordo o dano material ocasionado;

   ii. Art. 242, §1 do Código Penal – alteração de dados armazenados ou obstruir a transmissão de dados sem autorização com a intenção de obter benefício pecuniário próprio ou de dano

pecuniário a terceiro. A pena é de prisão de até 2 anos e pode ser aumentada para 5 anos de acordo o dano material ocasionado;

i) Acesso não-autorizado a sistemas de comunicações – De acordo com o art. 225, §1 do Código Penal esloveno, o acesso a um sistema de informação sem autorização é infração com multa de 125 a 12.500 euros e pode ser aumentado em até 37.500 euros conforme a intenção do crime;

j) Spam

   i. Art. 109, §1 da Lei de Comunicação Eletrônica – o uso de correio eletrônico visando o marketing direto só é permitido com o consentimento prévio do remetente. A multa para a infração pode chegar a 41.667 euros para pessoas jurídicas e 8.333 euros para pessoas físicas.

   ii. Art. 45.a, §1 da Lei de Proteção do Consumidor – o uso de correio eletrônico comercial encaminhado por empresas só é permitido com o consentimento prévio do consumidor. A multa para a infração pode chegar a 12.500 euros para pessoas jurídicas e 4.167 euros para pessoas físicas.

8. Espanha

O Código Penal Espanhol sofreu alterações para a inclusão de crimes de computador como o mau uso de dispositivos, posse de imagens de pornografia infantil (pornografia virtual infantil), fraudes por computador e proteção de dados pessoais em sistemas computacionais.

A Espanha conta também com leis específicas como a Lei Orgânica de Proteção de Dados Pessoais que penaliza spams. Outra lei específica que aguarda o decreto real é a Lei de Serviços da Sociedade da Informação e do Comércio Eletrônico que regula a retenção de dados em provedores de serviços e comunicações eletrônicas.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Espanha:

a) Rastreamento (Scan) – não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

   i. Art. 264 do Código Penal Espanhol - a destruição, modificação, inutilização ou quaisquer danos a dados, programas ou documentos em redes, sistema e mídias é crime com pena de prisão de 1 a 3 anos e multa de até 288.000 euros;

   ii. Art. 560 do Código Penal Espanhol – ocasionar danos que interrompam, impeçam ou destruam linhas ou instalações de telecomunicações é crime com pena de prisão de 1 a 5 anos;

   iii. Art. 413 do Código Penal Espanhol – remover, destruir, inutilizar ou esconder total ou parcialmente documentos (funcionários públicos) é crime com pena de prisão de 1 a 4 anos, multa de até 288.000 euros e destituição do direito de exercer funções públicas por 3 a 6 anos;

   iv. Art. 584 do Código Penal Espanhol – inutilizar informação classificada como secreta ou reservada, podendo ocasionar o detrimento da segurança ou defesa nacional, perpetrada por cidadão espanhol é crime com pena de prisão de 6 a 12 anos;

c) Negação de Serviço

   i. Art. 264.2 do Código Penal Espanhol - a destruição, modificação, inutilização ou quaisquer danos a dados pessoais, programas ou documentos em redes, sistema e mídias de terceiros é crime com pena de prisão de 1 a 3 anos e multa de até 288.000 euros;

   ii. Art. 560 do Código Penal Espanhol – ocasionar danos que interrompam, impeçam ou destruam linhas ou instalações de telecomunicações é crime com pena de prisão de 1 a 5 anos;

   iii. Art. 413 do Código Penal Espanhol – remover, destruir, inutilizar ou esconder total ou parcialmente documentos (funcionários públicos) é crime com pena de prisão de 1 a 4 anos, multa de até

288.000 euros e destituição do direito de exercer funções públicas por 3 a 6 anos;

iv. Art. 584 do Código Penal Espanhol – inutilizar informação classificada como secreta ou reservada, podendo ocasionar o detrimento da segurança ou defesa nacional, perpetrada por cidadão espanhol é crime com pena de prisão de 6 a 12 anos;

v. Art. 598 do Código Penal Espanhol – inutilizar informação classificada como secreta ou reservada, podendo ocasionar o detrimento da segurança ou defesa nacional é crime com pena de prisão de 1 a 4 anos;

d) Comprometimento de conta – só poderá ser punível se for tentado ou cometido crime subsequentemente;

e) Tentativa de Intrusão - só poderá ser punível se for tentado ou cometido crime subsequentemente;

f) Acesso não-autorizado a informações

i. Art. 197 do Código Penal Espanhol – a pena pode variar de 1 a 7 anos e multa de até 288.000 euros;

a. a apreensão de papéis, cartas, correios eletrônicos, mensagens ou quaisquer outros documentos de terceiros com a intenção de descobrir segredos ou brechas na privacidade da vítima;

b. acesso não autorizado por quaisquer meios, apreensão ou uso de dados reservados pessoais ou familiares armazenados em arquivos, sistemas de computadores, meios eletrônicos ou em cópias de segurança ou registros públicos ou privados, ocasionando danos aos dados ou a terceiros;

c. acesso não autorizado a informação, de acordo com o art. 197, cometido pelos responsáveis ou encarregados pelos arquivos, computadores, meios eletrônicos, cópias de segurança ou registros;

ii. Art. 198 do Código Penal Espanhol – acesso não autorizado a informação, de acordo com o art. 197, cometido por funcionários públicos. A pena pode variar de 1 a 7 anos, multa de até 288.000 euros e destituição do direito de exercer funções públicas por 6 a 12 anos;

iii. Art. 200 do Código Penal Espanhol – cometer crimes descritos no art. 197 que resultem em descoberta, revelação ou divulgação de dados reservados de pessoas jurídicas sem o consentimento de seus representantes legais. A pena pode variar de 1 a 4 anos que pode ser aumentada para 3 a 4 anos se o infrator for o responsável pelo material divulgado ou de 4 a 5 anos se houver a intenção de ganho com o delito e multa de até 288.000 euros e destituição do direito de exercer funções públicas por 6 a 12 anos;

iv. Art. 278 do Código Penal Espanhol – apreensão de dados, documentos, meios eletrônicos ou outros objetos com a intenção de revelar segredo de negócios. A pena pode variar de 2 a 4 anos, multa de até 288.000 euros;

v. Art. 415 do Código Penal Espanhol – acesso não autorizado e intencional a documentos sigilosos por funcionário público. A multa para essa infração é de até 144.000 euros e destituição do direito de exercer funções públicas por 1 a 3 anos;

vi. Art. 416 do Código Penal Espanhol – acesso não autorizado e intencional a documentos sigilosos por pessoas físicas por intermédio de funcionário público. A multa para essa infração é de até 72.000 euros;

vii. Art. 584 e 586 do Código Penal Espanhol – acesso a informações classificadas como confidenciais ou reservadas, capazes de causar danos à segurança ou defesa nacional com a intenção de ajudar países estrangeiros ou organizações estrangeiras. A pena é de 6 a 12 anos quando cometido por cidadão espanhol e 3 a 6 anos quando cometido por estrangeiro residente na Espanha;

viii. Art. 598 do Código Penal Espanhol – acesso a informações classificadas como confidenciais ou reservadas, capazes de causar danos à segurança ou defesa nacional. A pena é de 1 a 4 anos;

g) Acesso não-autorizado a transmissões

i. Art. 197.1 do Código Penal – a interceptação de telecomunicações e o uso de meios técnicos para escutar, transmitir ou registrar qualquer sinal de comunicação com o objetivo de descobrir segredos ou brechas na privacidade da vítima. A pena pode variar de 1 a 7 anos e multa de até 288.000 euros;

ii. Art. 198 do Código Penal Espanhol – acesso não autorizado a transmissões, de acordo com o art. 197, cometido por funcionários públicos. A pena pode variar de 1 a 7 anos, multa de até 288.000 euros e destituição do direito de exercer funções públicas por 6 a 12 anos;

iii. Art. 278 do Código Penal Espanhol – a interceptação de telecomunicações e o uso de meios eletrônicos ou outros objetos com a intenção de revelar segredo de negócios. A pena pode variar de 2 a 4 anos, multa de até 288.000 euros ;

iv. Art. 536 do Código Penal Espanhol – a interceptação de telecomunicações e o uso de meios eletrônicos ou outros objetos para escutar, transmitir ou registrar qualquer sinal de comunicação por uma autoridade pública ou funcionários públicos infringindo as leis. A pena pode variar de 2 a 6 anos;

h) Modificação não-autorizada de Informação

i. Art. 264 do Código Penal Espanhol - a destruição, modificação, inutilização ou quaisquer danos a dados, programas ou documentos em redes, sistema e mídias é crime com pena de prisão de 1 a 3 anos e multa de até 288.000 euros ;

ii. Art. 197 do Código Penal Espanhol - a apreensão de papéis, cartas, correios eletrônicos, mensagens ou quaisquer outros documentos de terceiros com a intenção de descobrir segredos ou brechas na privacidade da vítima. A pena pode variar de 1 a 4 anos e multa de até 288.000 euros ;

iii. Art. 390 e 391 do Código Penal Espanhol – adulterar elementos essenciais de um documento existente ou incluir declarações falsas por autoridades ou funcionários públicos. A pena pode variar de 3 a 6 anos e multa de até 288.000 euros ;

iv. Art. 392 do Código Penal Espanhol – adulterar elementos essenciais de um documento existente ou incluir declarações falsas. A pena pode variar de 6 meses a 3 anos e multa de até 144.000 euros;

v. Art. 395 do Código Penal Espanhol – adulterar elementos essenciais de um documento existente ou incluir declarações falsas com a intenção de prejudicar. A pena pode variar de 6 meses a 2 anos;

vi. Art. 413 do Código Penal Espanhol – remover, destruir, inutilizar ou esconder total ou parcialmente documentos (funcionários públicos) é crime com pena de prisão de 1 a 4 anos, multa de até 288.000 euros se destituição do direito de exercer funções públicas por 3 a 6 anos;

i) Acesso não-autorizado a sistemas de comunicações

i. Art. 255 do Código Penal Espanhol – fraude em telecomunicações utilizando-se de mecanismos ou quaisquer outros meios clandestinos ocasionando danos maiores que 400 euros é crime com multa de até 144.000 euros;

ii. Art. 256 do Código Penal Espanhol – o uso não autorizado de equipamento de telecomunicações ocasionando danos maiores que 400 euros é crime com multa de até 144.000 euros;

iii. Art. 286 do Código Penal Espanhol – o uso de equipamento ou programas que permitam o acesso não autorizado a equipamentos de telecomunicações é crime com multa de até 144.000 euros ;

j) Spam – de acordo com o art. 21 da Lei de Serviços da Sociedade da Informação e do Comércio Eletrônico, o uso de correio eletrônico ou sistemas similares visando o marketing direto sem o consentimento prévio do consumidor é uma infração que pode levar a multa que pode chegar a 150.000 euros.

9. Estônia

A Estônia possui leis específicas que lidam com crimes cibernéticos, como a Lei de Proteção de Dados Pessoais, a Lei de Serviços da Sociedade da Informação e a Lei de Telecomunicações, além de dispositivos específicos em seu Código Penal.

O Parlamento Estoniano ratificou a Convenção em Crime Cibernético do Conselho da Europa em 2003.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Estônia:

a) Rastreamento (Scan) – não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

i. Art. 206 do Código Penal Estoniano – a substituição, exclusão dano ou bloqueio de dados ou programas de computador que ocasionem danos significativos ou a introdução ilegal de dados ou programa em computador que ocasionem danos significativos é crime com pena de prisão de 1 a 3 anos e multa de até 500 unidades de multa diárias, cada taxa diária é equivalente a EEK 50 ou 3,20 euros;

ii. Art. 208 do Código Penal Estoniano – disseminação de vírus de computador. A pena é de prisão de até 1 e multa de até 500

unidades de multa diárias. Se houver reincidência ou ocasionar danos significativos, a pena de prisão poderá chegar a 3 anos;

iii. Art. 213 do Código Penal Estoniano – obter benefícios através da introdução, substituição, exclusão ou bloqueio de programas ou de dados de computador de forma ilegal ou outra interferência ilegal que influencie no resultado de uma operação de processamento de dados. Pena de até 5 anos ou multa de até 500 unidades de multa diárias;

iv. Art. 207 do Código Penal Estoniano – dano ou obstrução de uma conexão a rede ou sistema de computadores. Multa de até 500 unidades de multa diárias;

c) Negação de Serviço

i. Art. 208 do Código Penal Estoniano – disseminação de vírus de computador. A pena é de prisão de até 1 e multa de até 500 unidades de multa diárias. Se houver reincidência ou ocasionar danos significativos, a pena de prisão poderá chegar a 3 anos;

ii. Art. 213 do Código Penal Estoniano – obter benefícios através da introdução, substituição, exclusão ou bloqueio de programas ou de dados de computador de forma ilegal ou outra interferência ilegal que influencie no resultado de uma operação de processamento de dados. Pena de até 5 anos ou multa de até 500 unidades de multa diárias;

d) Comprometimento de conta – de acordo com o art. 217(1), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. Só poderá ser punível se for tentado ou cometido crime subsequentemente. Multa de até 500 unidades de multa diárias;

e) Tentativa de Intrusão –

i. art. 217(1), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. só poderá ser punível se for tentado ou

cometido crime subsequentemente. Multa de até 500 unidades de multa diárias;

ii. art. 217(2), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. Se for utilizado segredo ou computador do estado, ou sistema ou rede de computadores que contenham informação para uso oficial exclusivo. Só poderá ser punível se for tentado ou cometido crime subsequentemente. Prisão de até 3 anos ou multa de até 500 unidades de multa diárias;

f) Acesso não-autorizado a informações

i. art. 217(1), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. só poderá ser punível se for tentado ou cometido crime subsequentemente. Multa de até 500 unidades de multa diárias;

ii. art. 217(2), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. Se for utilizado segredo ou computador do estado, ou sistema ou rede de computadores que contenham informação para uso oficial exclusivo. Só poderá ser punível se for tentado ou cometido crime subsequentemente. Prisão de até 3 anos ou multa de até 500 unidades de multa diárias;

g) Acesso não-autorizado a transmissões

i. art. 217(1), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. só poderá ser punível se for tentado ou cometido crime subsequentemente. Multa de até 500 unidades de multa diárias;

ii. art. 217(2), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. Se for utilizado segredo ou computador do estado, ou sistema ou rede de computadores que contenham

informação para uso oficial exclusivo. Só poderá ser punível se for tentado ou cometido crime subsequentemente. Prisão de até 3 anos ou multa de até 500 unidades de multa diárias;

h) Modificação não-autorizada de Informação

   i. Art. 206 do Código Penal Estoniano – a substituição, exclusão dano ou bloqueio de dados ou programas de computador que ocasionem danos significativos ou a introdução ilegal de dados ou programa em computador que ocasionem danos significativos é crime com pena de prisão de 1 a 3 anos e multa de até 500 unidades de multa diárias, cada taxa diária é equivalente a EEK 50 ou 3,20 euros;

   ii. Art. 208 do Código Penal Estoniano – disseminação de vírus de computador. A pena é de prisão de até 1 e multa de até 500 unidades de multa diárias. Se houver reincidência ou ocasionar danos significativos, a pena de prisão poderá chegar a 3 anos;

i) Acesso não-autorizado a sistemas de comunicações

   i. art. 217(1), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. só poderá ser punível se for tentado ou cometido crime subsequentemente. Multa de até 500 unidades de multa diárias;

   ii. art. 217(2), O uso ilegal de computador, sistema de computador ou rede de computador através da remoção de código, senha ou outra medida de proteção. Se for utilizado segredo ou computador do estado, ou sistema ou rede de computadores que contenham informação para uso oficial exclusivo. Só poderá ser punível se for tentado ou cometido crime subsequentemente. Prisão de até 3 anos ou multa de até unidades de multa diárias;

j) Spam – de acordo com o art. 6 e 15 da Lei de Serviços da Sociedade da Informação e do Comércio Eletrônico, a transmissão de comunicação comercial sem o consentimento prévio do consumidor é

uma infração que pode levar a multa que pode chegar a 300 unidades de multa diárias.

10. Finlândia

A Finlândia possui algumas referências específicas de informática em seu código penal, como o Cap. 34, seção 9a – Dano Criminosos por Computador, o Cap. 38 Delitos de Comunicações e Dados e o Cap. 28, seção 7 – Uso não autorizado, conforme o Ministério da Justiça da Finlândia (2007) e de acordo com o European Comission, (2006), a Finlândia promulgou poucas leis específicas relacionadas à informática, aplicando os dispositivos da legislação existente.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Finlândia:

a) Rastreamento (Scan)

   i. Cap. 38, seção 8 (1) do Código Penal Finlandês – o acesso não autorizado por quebra de proteção de sistema de informação ou a parte do sistema. Pena de prisão de até 1 ano ou multa;

   ii. Cap. 38, seção 8 (2) do Código Penal Finlandês – Obter ilegalmente informação de sistema de computador ou parte dele, através de dispositivos técnicos especiais. Pena de prisão de até 1 ano ou multa;

   iii. Cap. 38, seção 8 (3) do Código Penal Finlandês – as tentativas são puníveis;

b) Código Malicioso

   i. Cap. 34, seção 9a (1) do Código Penal Finlandês – Produzir programas ou instruções para causar danos intencionalmente a processamento de dados, funcionamento de sistema ou danificar os dados ou software do sistema é crime com pena de prisão de até 2 anos ou multa;

   ii. Cap. 34, seção 9a (2) do Código Penal Finlandês – Disponibilizar ou distribuir instruções para a produção de programas ou instruções para causar danos intencionalmente a processamento de dados, funcionamento de sistema ou danificar os dados ou

software do sistema é crime com pena de prisão de até 2 anos ou multa;

De acordo com o European Comission (2006), em algumas circunstâncias, o código malicioso pode se enquadrar em dispositivos do Código Penal Finlandês que não são específicos para crimes cibernéticos, como o cap. 35, seção 2 – Dano Criminoso Agravado, o cap. 36, seção 1 – Fraude, o cap. 38:5 – Interferência ou o cap. 38, seção 6 – Interferência Agravada.

Outra possibilidade é a aplicação do Cap. 34, seção 9a – Dano Criminosos por Computador ou a Lei de Proteção da Privacidade das Comunicações Eletrônicas;

c) Negação de Serviço – de acordo com o Cap. 38, seção 5 do Código Penal Finlandês, a adulteração da operação de dispositivos utilizados em correio, telecomunicações ou rádio é delito com pena de prisão de até 2 anos ou multa. Em certas circunstâncias, de acordo com o European Comission (2006), o Cap./ 38, seção 6 – Interferência Agravada ou o Cap. 38, seção 7 – Interferência de Menor significância;

d) Comprometimento de conta

   i. Cap. 38, seção 8 (1) do Código Penal Finlandês – o acesso não autorizado por quebra de proteção de sistema de informação ou a parte do sistema. Pena de prisão de até 1 ano ou multa;

   ii. Cap. 38, seção 8 (2) do Código Penal Finlandês – Obter ilegalmente informação de sistema de computador ou parte dele, através de dispositivos técnicos especiais. Pena de prisão de até 1 ano ou multa;

   iii. Cap. 28, seção 7 do Código Penal Finlandês – Usar ilegalmente dispositivo móvel, máquina ou equipamento de terceiros. Pena de prisão de até 1 ano ou multa. A tentativa é punível;

e) Tentativa de Intrusão –

i. Cap. 38, seção 8 (1) do Código Penal Finlandês – o acesso não autorizado por quebra de proteção de sistema de informação ou a parte do sistema. Pena de prisão de até 1 ano ou multa;

ii. Cap. 38, seção 8 (2) do Código Penal Finlandês – Obter ilegalmente informação de sistema de computador ou parte dele, através de dispositivos técnicos especiais. Pena de prisão de até 1 ano ou multa;

iii. Cap. 28, seção 7 do Código Penal Finlandês – Usar ilegalmente dispositivo móvel, máquina ou equipamento de terceiros. Pena de prisão de até 1 ano ou multa. A tentativa é punível;

f) Acesso não-autorizado a informações

i. Cap. 38, seção 8 (1) do Código Penal Finlandês – o acesso não autorizado por quebra de proteção de sistema de informação ou a parte do sistema. Pena de prisão de até 1 ano ou multa;

ii. Cap. 38, seção 8 (2) do Código Penal Finlandês – Obter ilegalmente informação de sistema de computador ou parte dele, através de dispositivos técnicos especiais. Pena de prisão de até 1 ano ou multa;

iii. Cap. 28, seção 7 do Código Penal Finlandês – Usar ilegalmente dispositivo móvel, máquina ou equipamento de terceiros. Pena de prisão de até 1 ano ou multa. A tentativa é punível;

iv. Cap. 38, seção 3 (1) do Código Penal Finlandês – Violação de mensagem ou outras comunicações fechadas ou violar o conteúdo de mensagens armazenadas endereçadas a terceiros. Pena de prisão de até 1 ano ou multa. A tentativa é punível;

v. Cap. 38, seção 3 (2) do Código Penal Finlandês – Obter ilegalmente informações do conteúdo de ligações, telegramas, transmissões de texto, imagens ou dados ou quaisquer outras mensagens similares. Pena de prisão de até 1 ano ou multa. A tentativa é punível;

vi. Cap. 38, seção 4 (1) do Código Penal Finlandês – Se utilizar do privilégio da função no serviço de companhia de telecomunicações ou outra função de confiança para a interceptação de mensagens descritas no cap. 38, seção 3. Pena de prisão de até 3 anos. A tentativa é punível;

vii. Cap. 38, seção 4 (2) do Código Penal Finlandês – Usar programa de computador ou dispositivos técnicos concebidos, modificados ou outros métodos especiais para a interceptação de mensagens descritas no cap. 38, seção 3. Pena de prisão de até 1 ano. A tentativa é punível;

viii. Cap. 38, seção 4 (3) do Código Penal Finlandês – Interceptação de mensagem descrita no cap. 38, seção 3 que possua conteúdo sigiloso ou caso a interceptação constitua uma séria violação da privacidade ou cuja ação no todo seja considerada grave. Pena de prisão de até 1 ano. A tentativa é punível;

ix. Cap. 30, seção 4 do Código Penal Finlandês – Obter segredos de negócios acessando locais de acesso restrito ou acessando sistemas de informação protegidos, tomando posse ou copiando documento ou outros registros ou usando mecanismos técnicos com o intuito de revelar ou usar os segredos de negócios. Pena de prisão de até 2 anos. A tentativa é punível;

g) Acesso não-autorizado a transmissões

i. Cap. 38, seção 5 do Código Penal Finlandês - Adulteração da operação de dispositivos utilizados em correio, telecomunicações ou rádio. Pena de prisão de até 2 anos ou multa;

ii. Cap. 38, seção 6 (1) do Código Penal Finlandês – Interferir nas comunicações conforme descrito no Cap. 38, seção 5, se aproveitando de função de confiança. Pena de prisão de 4 meses a 4 anos;

iii. Cap. 38, seção 6 (2) do Código Penal Finlandês – Interferir nas comunicações conforme descrito no Cap. 38, seção 5, em transmissões efetuadas para a proteção de vida humana e a

interferência é agravada no todo. Pena de prisão de 4 meses a 4 anos;

h) Modificação não-autorizada de Informação

   i. Cap. 35, seção 1 do Código Penal Finlandês – Excluir, desfigurar ou ocultar informações armazenadas em dispositivos de armazenamento. Pena de prisão de até 1 ano ou multa;

   ii. Cap. 36, seção 1 (1) do Código Penal Finlandês – Enganar ou se aproveitar do erro de terceiros, compelindo a pessoa a causar perda financeira para obter ganho financeiro ilícito ou para causar danos. Pena de prisão de até 2 anos. A tentativa é punível;

   iii. Cap. 36, seção 1 (2) do Código Penal Finlandês – Cometer o descrito no Cap. 36, seção 1 (1) através da inclusão, modificação, destruição ou exclusão de dados ou por outra interferência na operação do sistema, modificando os resultados do processamento dos dados. Pena de prisão de até 2 anos. A tentativa é punível;

   iv. Cap. 36, seção 2 do Código Penal Finlandês – Cometer o descrito no Cap. 36, seção 1 (2), procurando benefício considerável, causando perdas consideráveis, se aproveitando de posição de confiança ou se aproveitando de vulnerabilidade ou da posição de confiança de outros e a fraude é agravada no todo. Pena de prisão de 4 meses a 4 anos. A tentativa é punível;

i) Acesso não-autorizado a sistemas de comunicações

   i. Cap. 28, seção 7 do Código Penal Finlandês – Usar ilegalmente dispositivo móvel, máquina ou equipamento de terceiros. Pena de prisão de até 1 ano ou multa. A tentativa é punível;

   ii. Cap. 38, seção 8 (1) do Código Penal Finlandês – o acesso não autorizado por quebra de proteção de sistema de informação ou a parte do sistema. Pena de prisão de até 1 ano ou multa;

   iii. Cap. 38, seção 8 (2) do Código Penal Finlandês – Obter ilegalmente informação de sistema de computador ou parte dele,

através de dispositivos técnicos especiais. Pena de prisão de até 1 ano ou multa;

j) Spam – de acordo com o cap. 42, seção 2 (8) da Lei de Proteção da Privacidade das Comunicações Eletrônicas, o uso de correio eletrônico para marketing direto é proibido quando não houver o consentimento prévio do consumidor e quando a pessoa física tiver proibido o recebimento de tais mensagens. Essa infração é passível de multa.

11. França

A França foi um dos primeiros países a adotarem dispositivos específicos para crimes por computador através da promulgação da Lei de Tecnologia da Informação e Liberdades (privacidade) de 1978 e da atualização do Código Penal Francês em 1988 com dispositivos sobre intrusão de sistemas de informação.

O Código Penal Francês ainda sofreu outras atualizações abrangendo infrações relacionadas a informação como fraude, distribuição de pornografia infantil, comunicações comerciais (spam) e interceptação de comunicações privadas.

O Código de Processo Penal Francês também sofreu atualizações relacionadas a criptografia, monitoração de comunicações e apreensão de dados.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da França:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

   i. Art. 323-1 do Código Penal Francês – A penetração ou manutenção de acesso fraudulento a um sistema de informação. A pena de prisão é de até 2 anos ou multa de até 30.000 euros que podem ser aumentados se em conseqüência desses atos os dados forem excluídos ou modificados;

ii. Art. 323-2 do Código Penal Francês – Impedir o funcionamento apropriado de um sistema de informação. A pena de prisão é de até 5 anos ou multa de até 75.000 euros;

iii. Art. 323-3 do Código Penal Francês – A introdução, modificação ou exclusão fraudulenta de dados em um sistema de informação. A pena de prisão é de até 5 anos ou multa de até 75.000 euros;

c) Negação de Serviço

i. Art. 323-2 do Código Penal Francês – Impedir o funcionamento apropriado de um sistema de informação. A pena de prisão é de até 5 anos ou multa de até 75.000 euros;

ii. Art. 323-3 do Código Penal Francês – A introdução, modificação ou exclusão fraudulenta de dados em um sistema de informação. A pena de prisão é de até 5 anos ou multa de até 75.000 euros;

d) Comprometimento de conta

i. Art. 323-1 do Código Penal Francês – A penetração ou manutenção de acesso fraudulento a um sistema de informação. A pena de prisão é de até 2 anos ou multa de até 30.000 euros que podem ser aumentados se em conseqüência desses atos os dados forem excluídos ou modificados;

ii. Art. 323-3 do Código Penal Francês – A introdução, modificação ou exclusão fraudulenta de dados em um sistema de informação. A pena de prisão é de até 5 anos ou multa de até 75.000 euros;

iii. Art. 313-1 do Código Penal Francês – Usar nome ou credenciais falsas para enganar pessoas físicas ou jurídicas através de manipulação fraudulenta fazendo com sejam entregues fundos, valores, quaisquer bens ou serviços. A pena de prisão é de até 5 anos ou multa de até 375.000 euros;

e) Tentativa de Intrusão –

i. Art. 323-1 do Código Penal Francês – A penetração ou manutenção de acesso fraudulento a um sistema de informação. A pena de prisão é de até 2 anos ou multa de até 30.000 euros

que podem ser aumentados se em conseqüência desses atos os dados forem excluídos ou modificados;

f) Acesso não-autorizado a informações

   i. Art. 323-1 do Código Penal Francês – A penetração ou manutenção de acesso fraudulento a um sistema de informação. A pena de prisão é de até 2 anos ou multa de até 30.000 euros que podem ser aumentados se em conseqüência desses atos os dados forem excluídos ou modificados;

   ii. Art. 226-15 do Código Penal Francês – Interceptar, ocasionar lentidão ou usar mensagens de telecomunicação de terceiros com má fé ou instalar dispositivos para esse fim. A pena de prisão é de até 1 ano ou multa de até 45.000 euros que podem ser aumentados se em conseqüência desses atos serem cometidos por funcionários públicos ou por funcionário da operadora de telecomunicações;

g) Acesso não-autorizado a transmissões

   i. Art. 226-15 do Código Penal Francês – Interceptar, ocasionar lentidão ou usar mensagens de telecomunicação de terceiros com má fé ou instalar dispositivos para esse fim. A pena de prisão é de até 1 ano ou multa de até 45.000 euros que podem ser aumentados se em conseqüência desses atos serem cometidos por funcionários públicos ou por funcionário da operadora de telecomunicações;

h) Modificação não-autorizada de Informação

   i. Art. 323-1 do Código Penal Francês – A penetração ou manutenção de acesso fraudulento a um sistema de informação. A pena de prisão é de até 2 anos ou multa de até 30.000 euros que podem ser aumentados se em conseqüência desses atos os dados forem excluídos ou modificados;

ii. Art. 323-3 do Código Penal Francês – A introdução, modificação ou exclusão fraudulenta de dados em um sistema de informação. A pena de prisão é de até 5 anos ou multa de até 75.000 euros;

i) Acesso não-autorizado a sistemas de comunicações

i. Art. 323-1 do Código Penal Francês – A penetração ou manutenção de acesso fraudulento a um sistema de informação. A pena de prisão é de até 2 anos ou multa de até 30.000 euros que podem ser aumentados se em conseqüência desses atos os dados forem excluídos ou modificados;

ii. Art. 226-15 do Código Penal Francês – Interceptar, ocasionar lentidão ou usar mensagens de telecomunicação de terceiros com má fé ou instalar dispositivos para esse fim. A pena de prisão é de até 1 ano ou multa de até 45.000 euros que podem ser aumentados se em conseqüência desses atos serem cometidos por funcionários públicos ou por funcionário da operadora de telecomunicações;

j) Spam

i. Art. L. 34-5 do Código de Telecomunicações e Correios – Contatar clientes em potencial diretamente através de dispositivos automatizados de chamados, fax e correios eletrônicos sem prévio consentimento. A multa é de 750 euros por mensagem enviada ilicitamente;

ii. Art. 226-16 do Código Penal Francês – Processar ou fazer processar dados de natureza pessoal dispensando formalidades prévias. A pena de prisão é de até 5 anos ou multa de até 300.000 euros;

iii. Art. 226-18 do Código Penal Francês – Coletar dados de caráter pessoal por meios fraudulentos, desleais ou ilícitos. A pena de prisão é de até 5 anos ou multa de até 300.000 euros;

12. Grécia

A Grécia atualizou sua Constituição em 2001 e incluiu dispositivos relacionados à sociedade da informação e novas tecnologias em sua Constituição. O art. 5a dispõe sobre o direito e deveres do cidadão e do estado grego quanto à sociedade da informação. O art. 9 A estabelece o direito de proteção dos dados pessoais inclusive em meios eletrônicos aos cidadãos gregos, Ministério da Justiça Grego (2007).

De acordo com o European Commission (2006), a Grécia atualizou o Código Penal, incluindo dispositivos sobre fraudes por computadores e acessos ilegais, mas não promulgou leis específicas sobre Internet. Os legisladores tratam os crimes ligados à Internet como os atos cobertos pelo Código penal que se utilizam de documentos físicos (papel) ou informações divulgadas em mídia.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Grécia:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;
b) Código Malicioso
    i. Art. 381 do Código Penal Grego – Dano intencional de propriedade de terceiros, incluindo dados eletrônicos, no todo ou parte, ou de quaisquer formas, impedindo o seu uso. A pena de prisão é de até 2 anos;
    ii. Art. 386A do Código Penal Grego – A tentativa de enriquecimento próprio ou de outros através do dano a terceiros, afetando dados de computadores pela execução incorreta de programa de computador ou pelo uso de dados errados ou incompletos ou por danos aos dados através de algum outro meio. A pena de prisão é de 2 anos a 10 anos ou multa de 15.000 euros que pode chegar a 73.000 euros;
c) Negação de Serviço
    i. Art. 381 do Código Penal Grego – Dano intencional de propriedade de terceiros, incluindo dados eletrônicos, no todo ou

parte, ou de quaisquer formas, impedindo o seu uso. A pena de prisão é de até 2 anos;

ii. Art. 370 C §2 do Código Penal Grego – Acesso ilegal de dados armazenados em computador ou em memória externa do computador transmitido por sistema de telecomunicações, especialmente violando medidas de segurança. A pena de prisão é de até 3 meses ou multa de 29 euros a 15.000 euros;

d) Comprometimento de conta

i. Art. 370 C §2 do Código Penal Grego – Acesso ilegal de dados armazenados em computador ou em memória externa do computador transmitido por sistema de telecomunicações, especialmente violando medidas de segurança. A pena de prisão é de até 3 meses ou multa de 29 euros a 15.000 euros;

ii. Art. 370 B do Código Penal Grego – Acesso e manutenção de acesso ilegal a dados sigilosos armazenados em sistema de computador. A pena de prisão é de até 3 meses a 5 anos;

e) Tentativa de Intrusão –

i. Art. 370 C §2 do Código Penal Grego – Acesso ilegal de dados armazenados em computador ou em memória externa do computador transmitido por sistema de telecomunicações, especialmente violando medidas de segurança. A pena de prisão é de até 3 meses ou multa de 29 euros a 15.000 euros;

ii. Art. 370 B do Código Penal Grego – Acesso e manutenção de acesso ilegal a dados sigilosos armazenados em sistema de computador. A pena de prisão é de até 3 meses a 5 anos;

f) Acesso não-autorizado a informações – de acordo com o art. 370 C §2 do Código Penal Grego, o acesso ilegal de dados armazenados em computador ou em memória externa do computador transmitido por sistema de telecomunicações, especialmente violando medidas de segurança é infração com pena de prisão de até 3 meses ou multa de 29 euros a 15.000 euros. Se o infrator for funcionário do dono da

informação, então a pena só será aplicável se houver regulamentação interna ou por uma decisão por escrito;

g) Acesso não-autorizado a transmissões

   i. Art. 370 §1 do Código Penal Grego – Obtenção de acesso ilegal e intencional ao conteúdo de documentos selados ou violação da privacidade de terceiros através da leitura, transcrição ou cópia de carta ou documento. A pena de prisão é de até 1 ano;

   ii. Art. 370 A do Código Penal Grego –Acesso ilegal a ligações telefônicas e sistemas de secretária eletrônica particulares. A pena de prisão é de 10 dias a 5 anos;

h) Modificação não-autorizada de Informação

   i. Art. 370 C §2 do Código Penal Grego – Acesso ilegal de dados armazenados em computador ou em memória externa do computador transmitido por sistema de telecomunicações, especialmente violando medidas de segurança. A pena de prisão é de até 3 meses ou multa de 29 euros a 15.000 euros;

   ii. Art. 381 do Código Penal Grego – Dano intencional de propriedade de terceiros, incluindo dados eletrônicos, no todo ou parte, ou de quaisquer formas, impedindo o seu uso. A pena de prisão é de até 2 anos;

i) Acesso não-autorizado a sistemas de comunicações

   i. Art. 370 C §2 do Código Penal Grego - o acesso ilegal de dados armazenados em computador ou em memória externa do computador transmitido por sistema de telecomunicações, especialmente violando medidas de segurança é infração com pena de prisão de até 3 meses ou multa de 29 euros a 15.000 euros. Se o infrator for funcionário do dono da informação, então a pena só será aplicável se houver regulamentação interna ou por uma decisão por escrito;

   ii. Art. 370 §1 do Código Penal Grego – Obtenção de acesso ilegal e intencional ao conteúdo de documentos selados ou violação da

privacidade de terceiros através da leitura, transcrição ou cópia de carta ou documento. A pena de prisão é de até 1 ano;

iii. Art. 370 A do Código Penal Grego –Acesso ilegal a ligações telefônicas e sistemas de secretária eletrônica particulares. A pena de prisão é de 10 dias a 5 anos;

j) Spam – não há regulamentação específica para spam no código penal ou em outras leis gregas. O código penal grego no entanto, dispõe de um artigo sobre o uso de propagandas, números de telefone, correio eletrônicos ou quaisquer outros meios com o intuito de facilitar atividade de pedofilia. A pena é de 10 meses a 5 anos e multa de até 100.000 euros.

13. Holanda

Na Holanda, a maioria dos regulamentos relacionados a crimes por computador foram introduzidos através da Lei Crime de Computador de 1993 que incorporou novos dispositivos tanto no Código Penal quanto no Código de Processo Penal.

O Código Penal passou a considerar as infrações de invasão de dispositivos automatizados, interrupção do processamento ou funcionamento de dispositivo automatizada, alteração ou inutilização de dados e interceptação de dados.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Holanda:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

i. Art. 161(6) do Código Penal – Destruir, danificar ou interromper o processamento ou o funcionamento de um dispositivo automatizado ou danificar medidas de segurança implementados em tal dispositivo. Pena de prisão de até 9 anos ou multa, que pode variar de acordo com os danos ocasionados;

ii. Art. 161(7) do Código Penal – Destruir, danificar ou interromper de forma não intencional o processamento ou funcionamento de um dispositivo automatizado ou danificar medidas de segurança implementados em tal dispositivo. Pena de prisão de até 1 ano ou multa, que pode variar de acordo com os danos ocasionados;

iii. Art. 350a(1) do Código Penal – Modificar ou excluir intencional e ilegalmente dados armazenados ou processados em dispositivo automatizado ou inutilizar ou indisponibilizar os dados. Pena de prisão de até 2 anos ou multa;

iv. Art. 350a(2) do Código Penal – Cometer infração descrita na seção 1 usando rede de telecomunicações pública e danificando seriamente os dados envolvidos. Pena de prisão de até 4 anos ou multa;

v. Art. 350a(3) do Código Penal – Distribuir intencional e ilegalmente dados com o objetivo de causar danos, através da replicação desses dados em dispositivo automatizado. Pena de prisão de até 4 anos ou multa;

vi. Art. 350b(1) do Código Penal – Causar a modificação ou exclusão sem intenção de dados armazenados ou processados em dispositivo automatizado ou inutilizar ou indisponibilizar os dados, se ocasionar danos sérios aos dados. Pena de prisão de até 1 mês ou multa;

vii. Art. 350b(2) do Código Penal – Causar a distribuição não intencional de dados com o objetivo de causar danos, através da replicação desses dados em dispositivo automatizado. Pena de prisão de até 1 mês ou multa;

c) Negação de Serviço

i. Art. 161(6) do Código Penal – Destruir, danificar ou interromper o processamento ou o funcionamento de um dispositivo automatizado ou danificar medidas de segurança implementados em tal dispositivo. Pena de prisão de até 9 anos ou multa, que pode variar de acordo com os danos ocasionados;

ii. Art. 161(7) do Código Penal – Destruir, danificar ou interromper de forma não intencional o processamento ou funcionamento de um dispositivo automatizado ou danificar medidas de segurança implementados em tal dispositivo. Pena de prisão de até 1 ano ou multa, que pode variar de acordo com os danos ocasionados;

iii. Art. 350a(1) do Código Penal – Modificar ou excluir intencional e ilegalmente dados armazenados ou processados em dispositivo automatizado ou inutilizar ou indisponibilizar os dados. Pena de prisão de até 2 anos ou multa;

iv. Art. 350a(2) do Código Penal – Cometer infração descrita na seção 1 usando rede de telecomunicações pública e danificando seriamente os dados envolvidos. Pena de prisão de até 4 anos ou multa;

v. Art. 350b(1) do Código Penal – Causar a modificação ou exclusão sem intenção de dados armazenados ou processados em dispositivo automatizado ou inutilizar ou indisponibilizar os dados, se ocasionar danos sérios aos dados. Pena de prisão de até 1 mês ou multa;

d) Comprometimento de conta

i. Art. 138a Seção 1, Subseção (a) do Código Penal – Invadir um dispositivo automatizado intencional e ilegalmente, sobrepujando medidas de segurança. Pena de prisão de até 6 meses ou multa;

ii. Art. 138a Seção 1, Subseção (b) do Código Penal – Invadir um dispositivo automatizado intencional e ilegalmente, utilizando-se chaves ou identificadores falsos. Pena de prisão de até 6 meses ou multa;

e) Tentativa de Intrusão

i. Art. 138a Seção 1, Subseção (a) do Código Penal – Tentar invadir um dispositivo automatizado intencional e ilegalmente, sobrepujando medidas de segurança. Pena de prisão de até 6 meses ou multa;

ii. Art. 138a Seção 1, Subseção (b) do Código Penal – Tentar invadir um dispositivo automatizado intencional e ilegalmente, utilizando-se chaves ou identificadores falsos. Pena de prisão de até 6 meses ou multa;

f) Acesso não-autorizado a informações

i. Art. 138a Seção 1, Subseção (a) do Código Penal – Invadir um dispositivo automatizado intencional e ilegalmente, sobrepujando medidas de segurança. Pena de prisão de até 6 meses ou multa;

ii. Art. 138a Seção 1, Subseção (b) do Código Penal – Invadir um dispositivo automatizado intencional e ilegalmente, utilizando-se chaves ou identificadores falsos. Pena de prisão de até 6 meses ou multa;

g) Acesso não-autorizado a transmissões – de acordo com o art. 139c, usar dispositivo técnico intencionalmente para interceptar ou registrar dados não pertinentes ao infrator utilizando-se redes públicas de telecomunicações. Pena de prisão de até 6 meses ou multa;

h) Modificação não-autorizada de Informação

i. Art. 350a(1) do Código Penal – Modificar ou excluir intencional e ilegalmente dados armazenados ou processados em dispositivo automatizado ou inutilizar ou indisponibilizar os dados. Pena de prisão de até 2 anos ou multa;

ii. Art. 350a(2) do Código Penal – Cometer infração descrita na seção 1 usando rede de telecomunicações pública e danificando seriamente os dados envolvidos. Pena de prisão de até 4 anos ou multa;

i) Acesso não-autorizado a sistemas de comunicações

i. Art. 138a Seção 1, Subseção (a) do Código Penal – Tentar invadir um dispositivo automatizado intencional e ilegalmente, sobrepujando medidas de segurança. Pena de prisão de até 6 meses ou multa;

ii. Art. 138a Seção 1, Subseção (b) do Código Penal – Invadir um dispositivo automatizado intencional e ilegalmente, utilizando-se chaves ou identificadores falsos. Pena de prisão de até 6 meses ou multa;

iii. Art. 139c - Usar dispositivo técnico intencionalmente para interceptar ou registrar dados não pertinentes ao infrator utilizando-se redes públicas de telecomunicações. Pena de prisão de até 6 meses ou multa;

iv. Art. 350a(1) do Código Penal – Modificar ou excluir intencional e ilegalmente dados armazenados ou processados em dispositivo automatizado ou inutilizar ou indisponibilizar os dados. Pena de prisão de até 2 anos ou multa;

v. Art. 350a(2) do Código Penal – Cometer infração descrita na seção 1 usando rede de telecomunicações pública e danificando seriamente os dados envolvidos. Pena de prisão de até 4 anos ou multa;

j) Spam

i. Art. 11.7, Seção 1 da Lei de Telecomunicações – Uso de mensagens comerciais sem o consentimento prévio do destinatário é infração passível de multa;

ii. Art. 11.7, Seção 3 da Lei de Telecomunicações – Uso de identificação falsa ou não incluir dispositivo de remoção de lista (opt-out) é infração passível de multa.

14. Hungria

A Hungria atualizou o seu Código Penal em 2001, adotando as medidas da Convenção em Crimes Cibernéticos do Conselho da Europa e dessa forma introduziu tipificações de delitos relacionados à informática como acesso ilegal, manipulação de dados, interferência em sistemas, mau uso de dispositivos, falsificações e fraudes em informática e interceptações ilegais.

Além desses dispositivos, o código penal húngaro possui dispositivos relacionados a crimes de conteúdo como a pornografia infantil e violação de direitos autorais.

O Código de Processo Penal Húngaro também define medidas regulatórias de retenção de informações para provedoras e operadoras de serviços de comunicações eletrônicas.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Hungria:

a) Rastreamento (Scan)
    i. Seção 178 (1) e (3) do Código Penal Húngaro – violação do sigilo de mensagens através de equipamentos de telecomunicações. Multa em grande parte dos casos e em casos de circunstâncias agravantes, pena de prisão de até 3 anos;
    ii. Seção 178/A (1)d e 178/A (2) e (3) do Código Penal Húngaro – interceptação e gravação de dados pessoais ou transmissão do conteúdo por equipamento de comunicação eletrônico ou sistema de computador com o objetivo de coletar informações sigilosas sem consentimento prévio. Pena de prisão de até 5 anos que pode chegar a 8 anos se cometido em circunstâncias agravantes;
b) Código Malicioso – de acordo com a seção 300/C (2)b do Código Penal Húngaro, inserir, transmitir, danificar, excluir, deteriorar ou modificar dados eletrônicos causando mau funcionamento de sistemas de computador é infração com pena de até 2 anos, prestação de serviço à comunidade ou multa;
c) Negação de Serviço
    i. Seção 300/C (2)b do Código Penal Húngaro - inserir, transmitir, danificar, excluir, deteriorar ou modificar dados eletrônicos causando mau funcionamento de sistemas de computador. Pena de até 2 anos, prestação de serviço à comunidade ou multa;
    ii. Seção 300/C (3)b do Código Penal Húngaro - inserir, transmitir, ou excluir dados processados, armazenados ou transmitidos em

sistema de computador ou quaisquer outras ações com o intuito de ganho de benefício ilícito e que cause mau funcionamento de sistemas de computador e danos. Pena de até 3 anos, podendo ter a pena aumentada conforme o dano causado;

d) Comprometimento de conta - seção 300/C (1) do Código Penal Húngaro, o acesso e manutenção não autorizado em sistema de computador por intrusos, mesmo sem a intenção de causar dano. Pena de até 1 ano, prestação de serviço à comunidade ou multa;

e) Tentativa de Intrusão

   i. Seção 300/E §(1) do Código Penal Húngaro – comprometer integridade de um sistema ou dispositivo de proteção de sistema. Pena de prisão de até 2 anos ou multa;

   ii. Seção 300/C (1) do Código Penal Húngaro - acesso e manutenção não autorizado em sistema de computador por intrusos, mesmo sem a intenção de causar dano. Pena de até 1 ano, prestação de serviço à comunidade ou multa;

f) Acesso não-autorizado a informações - seção 178/A (1)d do Código Penal Húngaro, interceptação e gravação de dados pessoais ou transmissão do conteúdo por equipamento de comunicação eletrônico ou sistema de computador com o objetivo de coletar informações sigilosas sem consentimento prévio. Pena de prisão de até 5 anos que pode chegar a 8 anos se cometido em circunstâncias agravantes;

g) Acesso não-autorizado a transmissões - seção 178/A (1)d do Código Penal Húngaro, interceptação e gravação de dados pessoais ou transmissão do conteúdo por equipamento de comunicação eletrônico ou sistema de computador com o objetivo de coletar informações sigilosas sem consentimento prévio. Pena de prisão de até 5 anos que pode chegar a 8 anos se cometido em circunstâncias agravantes;

h) Modificação não-autorizada de Informação

   i. Seção 300/C (2)b do Código Penal Húngaro - inserir, transmitir, danificar, excluir, deteriorar ou modificar dados eletrônicos

causando mau funcionamento de sistemas de computador. Pena de até 2 anos, prestação de serviço à comunidade ou multa;

ii. Seção 300/C (3)b do Código Penal Húngaro - inserir, transmitir, ou excluir dados processados, armazenados ou transmitidos em sistema de computador ou quaisquer outras ações com o intuito de ganho de benefício ilícito e que cause mau funcionamento de sistemas de computador e danos. Pena de até 3 anos, podendo ter a pena aumentada conforme o dano causado;

i) Acesso não-autorizado a sistemas de comunicações - seção 300/C (1) do Código Penal Húngaro, o acesso e manutenção não autorizado em sistema de computador por intrusos, mesmo sem a intenção de causar dano. Pena de até 1 ano, prestação de serviço à comunidade ou multa;

j) Spam – de acordo com a seção 14 §(1) da Lei n° 108 de 2001 de Serviços de Comércio Eletrônico e de Serviços da Sociedade da Informação - o uso de correio eletrônico para propaganda é proibido quando não houver o consentimento prévio do consumidor. Essa infração é passível de multa.

15. Irlanda

A legislação irlandesa é composta de inúmeras leis segmentadas e dentre elas, algumas que lidam especificamente com crimes relacionados à informática, como a Lei de Justiça Penal (Infrações de Roubo e Fraude) de 2001, a Lei de Danos Criminais de 1991, a Lei de Regulamentação de Comunicações de 2002, a Lei de Comércio Eletrônico de 2000, a Lei de Direitos Autorais e Direitos Relacionados de 2000 e a Lei de Pornografia e Tráfico de Crianças de 1998, de acordo com o Departamento do Primeiro Ministro Irlandês (2007b).

A Irlanda também assinou em fevereiro de 2002 a Convenção em Crimes Cibernéticos do Conselho da Europa.

A Irlanda criou em 2001 a Comissão de Sociedade da Informação (Information Society Commission), um corpo consultivo ligado diretamente ao Departamento do Primeiro Ministro, para desenvolver uma estrutura de política pública para a Sociedade da Informação na Irlanda.

Na definição da Information Society Commission (2007), o termo Sociedade da Informação representa a influência contemporânea crescente das tecnologias da informação e comunicação na sociedade.

A Comissão da Sociedade da Informação criou grupos de trabalho e dentre eles o Grupo de Trabalho de Assuntos Jurídicos, que teve como foco desenvolver uma abordagem que possibilitasse ao sistema legal irlandês, promover a confiabilidade necessária para suportar o desenvolvimento da estrutura de sua Sociedade da Informação.

O trabalho consistiu em identificar estrutura legal e regulatória relacionada à informática e elaborar recomendações a serem encaminhadas ao governo irlandês.

Dentre as recomendações efetuadas pelo Grupo de Trabalho de Assuntos Jurídicos, encontram-se pontos específicos para crimes cibernéticos, a seguir conforme a Information Society Commission (2007):

a) Condução de análises qualitativas e quantitativas aprofundadas da extensão do problema dos crimes cibernéticos na Irlanda;
b) A Polícia Nacional Irlandesa, a Garda Síochána, deve considerar a possibilidade de firmar acordos de confidencialidade para encorajar que as empresas notifiquem infrações relacionadas à informática;
c) Prioridade, recursos adequados e preparação da Garda Síochána para lidar com crimes cibernéticos
d) Revisão do sistema judicial de forma que os casos de crimes cibernéticos possam ser julgados;
e) Reforço do contato internacional;
f) Prevenção e conscientização em crimes cibernéticos da população.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Irlanda:

a) Rastreamento (Scan) – de acordo com a Seção 9 da Lei de Justiça Penal (Lei de Infrações de Roubo e Fraude), pessoa dentro ou fora do país que desonestamente opere ou faz com que um computador seja

operado no país com a intenção de obter ganho a si mesmo ou a outros em detrimento de terceiros é infração com pena de prisão de até 10 anos ou multa;

b) Código Malicioso – de acordo com a Lei de Dano Criminal, Seção 5 (1), operar computador sem autorização judicial a partir do território do país para acessar quaisquer dados ou operar computador sem autorização judicial fora do território do país para acessar quaisquer dados mantidos no país é infração com multa prevista de até £500;

c) Negação de Serviço – de acordo com a Lei de Dano Criminal, Seção 5 (1), operar computador sem autorização judicial a partir do território do país para acessar quaisquer dados ou operar computador sem autorização judicial fora do território do país para acessar quaisquer dados mantidos no país é infração com multa prevista de até £500;

d) Comprometimento de conta – de acordo com a Lei de Dano Criminal, Seção 5 (2) Subseção 1, se aplica nas infrações definidas na seção 5 (1) quando o acesso é feito em quaisquer dados pessoais, quaisquer categorias pessoais de dados ou dados armazenados por quaisquer pessoas país é infração com multa prevista de até £500;

e) Tentativa de Intrusão

   i. Lei de Dano Criminal, Seção 5 (1) - operar computador sem autorização judicial a partir do território do país para acessar quaisquer dados ou operar computador sem autorização judicial fora do território do país para acessar quaisquer dados mantidos no país. Multa prevista de até £500;

   ii. Lei de Dano Criminal, Seção 5 (2) Subseção 1, se aplica nas infrações definidas na seção 5 (1) quando o acesso é feito em quaisquer dados pessoais, quaisquer categorias pessoais de dados ou dados armazenados por quaisquer pessoas país é infração com multa prevista de até £500;

f) Acesso não-autorizado a informações

i. Lei de Dano Criminal, Seção 5 (1) - operar computador sem autorização judicial a partir do território do país para acessar quaisquer dados ou operar computador sem autorização judicial fora do território do país para acessar quaisquer dados mantidos no país. Multa prevista de até £500;

ii. Lei de Dano Criminal, Seção 5 (2) Subseção 1, se aplica nas infrações definidas na seção 5 (1) quando o acesso é feito em quaisquer dados pessoais, quaisquer categorias pessoais de dados ou dados armazenados por quaisquer pessoas país é infração com multa prevista de até £500;

g) Acesso não-autorizado a transmissões – Regulamentos das Comunidades Européias de 2003 (Serviços e Redes de Comunicações Eletrônicas; Proteção e Privacidade de Dados), - o uso de correio eletrônico para marketing direto é proibido quando não houver o consentimento prévio do consumidor. Essa infração é passível de multa;

h) Modificação não-autorizada de Informação – não há dispositivos específicos;

i) Acesso não-autorizado a sistemas de comunicações – não há dispositivos específicos;

j) Spam – não há dispositivos específicos.

A seção 13 dos Regulamentos das Comunidades Européias de 2003 (Serviços e Redes de Comunicações Eletrônicas; Proteção e Privacidade de Dados) também se aplica ao item spam, Procuradoria Geral da Irlanda (2007).

16. Itália

A legislação italiana sofreu atualizações em 1993 para a inclusão de dispositivos relacionados aos crimes cibernéticos tanto nos Códigos Penal e de Processo Penal quanto a algumas leis específicas como as leis n. 269 de 1998, com dispositivos sobre pedofilia e n. 364, referente a terrorismo. Dispositivos do Código de Proteção de Dados.

No Código Penal Italiano, o artigo 615 refere-se ao acesso não autorizado a sistema de computadores cuja pena varia de 1 a 3 anos e pode chegar a 5 anos.

O art. 615 (4) define que a posse e a distribuição de código de acesso a sistemas de Computador ou de Telecomunicações é infração passível de prisão de até 1 ano ou multa de até 5.164 euros. A pena pode ser aumentada em decorrência de fatores agravantes.

De acordo com o art. 615 (5) do Código Penal Italiano, a distribuição de programas de computadores com a intenção de causar dano ou interromper um sistema de computador é infração com pena de prisão até 2 anos ou multa de até 10.329 euros.

A instalação de equipamentos para a interceptação, interrupção ou impedimento de comunicações telemáticas ou de informática é infração de acordo com o Código Penal Italiano, com previsão de prisão de 1 a 4 anos que em caso de circunstâncias agravantes pode ser aumentada em até 5 anos.

Conforme o artigo 617 (6), as infrações relacionadas ao conteúdo de telecomunicações são delitos com penas prevista de 1 a 4 anos podendo chegar a 5 anos.

As fraudes cometidas através de informática, ou a interferência em quaisquer formas em dados, informações ou softwares em sistemas de computadores ou telecomunicações para obtenção de ganho para si ou para ocasionar danos a terceiros constituem delitos segundo o Código Penal Italiano com penas previstas de prisão de 6 meses a 3 anos e multa de 51 euros a 1.032 euros. A pena poderá ser aumentada em caso de circunstância agravante do delito.

Os danos às infra-estruturas públicas de informática e a sistemas de computadores também constituem delitos previstos no código penal com penas previstas de até 8 anos.

O art. 167 do Código de Privacidade que dispõe sobre o processamento ilegal de dados é uma regra abrangente e que pode ser aplicada na maioria dos casos referentes à informática.

O art. 130 trata das comunicações não solicitadas incluindo-se o spam.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Italiana:

a) Rastreamento (Scan) – de acordo com o art. 615 (4) do Código Penal, a distribuição, comunicação ou disponibilização a terceiros de softwares produzidos com o objetivo de danificar, interromper ou modificar sistemas de computador, telecomunicações ou programa de computador. Pena de prisão de até 1 ano e multa de até 5.164 euros, podendo aumentar para 1 a 2 anos de prisão e multa de até 10.329 euros em situações agravantes;

b) Código Malicioso

   i. Art. 420 § 2 e 3 do Código Penal Italiano – Danificar ou destruir infra-estrutura de informática de interesse público ou bases de dados públicos ou programas de utilidade pública ou interromper seus serviços. Pena de prisão de 3 a 8 anos;

   ii. Art. 615 (5) do Código Penal Italiano – Distribuir, transmitir ou entregar um programa de computador com o intuito de ocasionar dano ou danificar sistema de computador ou telecomunicações, os dados ou software neles contidos ou impedir o seu funcionamento total ou parcial. Pena de prisão de até 2 anos e multa de ate 10.329 euros;

   iii. Art. 635 (2) do Código Penal Italiano – Destruir, danificar ou inutilizar total ou parcialmente sistemas de computadores ou telecomunicações, programa de computador ou dados. Pena de prisão de 6 meses a 3 anos que podem ser aumentados se houver circunstância agravante do delito;

   iv. Art. 640 (3) do Código Penal Italiano – Alterar a funcionalidade de um sistema de computador ou telecomunicações ou interferir de quaisquer maneiras os dados, informações ou softwares com o intuito de obter ganho para si ou para ocasionar danos a terceiros. Pena de prisão de 1 a 3 anos e multa de 51 euros a 1.032 euros

que podem ser aumentados se houver circunstância agravante do delito;

c) Negação de Serviço – de acordo com o art. 420 § 2 e 3 do Código Penal Italiano – Danificar ou destruir infra-estrutura de informática de interesse público ou bases de dados públicos ou programas de utilidade pública ou interromper seus serviços. Pena de prisão de 3 a 8 anos;

d) Comprometimento de conta – de acordo com o art. 615 (3) do Código Penal Italiano – Acessar sem autorização sistema de computador ou telecomunicação protegido por medidas de segurança. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito;

e) Tentativa de Intrusão – de acordo com o art. 615 (3) do Código Penal Italiano – Acessar sem autorização sistema de computador ou telecomunicação protegido por medidas de segurança. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito;

f) Acesso não-autorizado a informações

   i. Art. 615 (4) do Código Penal Italiano – Distribuir, comunicar ou disponibilizar programa de computador com o intuito de ocasionar dano, interromper ou modificar programa de computador, sistemas de telecomunicações ou de computador. Pena de prisão de até 1 ano e multa de ate 164 euros que podem ser aumentados se houver circunstância agravante do delito;

   ii. art. 615 (3) do Código Penal Italiano – Acessar sem autorização sistema de computador ou telecomunicação protegido por medidas de segurança. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito;

g) Acesso não-autorizado a transmissões

   i. Art. 615 (4) do Código Penal Italiano – Distribuir, comunicar ou disponibilizar programa de computador com o intuito de ocasionar

dano, interromper ou modificar programa de computador, sistemas de telecomunicações ou de computador. Pena de prisão de até 1 ano e multa de ate 164 euros que podem ser aumentados se houver circunstância agravante do delito;

ii. Art. 617 (4) do Código Penal Italiano – Interceptação, interrupção ou parada fraudulenta de comunicações de sistema de computadores ou telecomunicações ou da comunicação de um ou mais sistemas. Pena de prisão de 6 meses a 4 anos que podem ser aumentados se houver circunstância agravante do delito;

iii. Art. 617 (5) do Código Penal Italiano – Instalar equipamento para interceptar ou interromper telecomunicações sem autorização. Pena de prisão de 1 a 4 anos que podem ser aumentados se houver circunstância agravante do delito;

iv. Art. 617 (6) do Código Penal Italiano – Inclusão, modificação ou exclusão fraudulenta de todo ou parte do conteúdo interceptado da comunicação original com o intuito de ganho próprio ou de terceiros ou para ocasionar dano a terceiros. Pena de prisão de 1 a 4 anos que podem ser aumentados se houver circunstância agravante do delito;

h) Modificação não-autorizada de Informação - art. 615 (3) do Código Penal Italiano, acessar sem autorização sistema de computador ou telecomunicação protegido por medidas de segurança. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito;

i) Acesso não-autorizado a sistemas de comunicações - art. 615 (3) do Código Penal Italiano, acessar sem autorização sistema de computador ou telecomunicação protegido por medidas de segurança. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito;

j) Spam - art. 130 e 161 do Código de Privacidade Italiano, o uso de comunicações eletrônicas como e-mail, SMS e MMS para finalidades de marketing sem o consentimento prévio do destinatário, esconder a

identidade do remetente ou usar identidade falsa no remetente é infração com pena de prisão de 6 a 24 meses e/ou multa de até 54.000 euros.

17. Letônia

O Código Penal da Letônia foi atualizado em 2002 para a inclusão de dispositivos sobre crimes relacionados à informática como a interceptação de comunicações, a interceptação ilegal de sistemas de computador, o uso ilegal de software de computadores, danos em software de computador, a disseminação de vírus e violação de medidas de segurança de sistemas de informação.

A Letônia conta com legislações específicas como a Lei de Documentos Eletrônicos de 2002, que regulamenta o uso de documentos eletrônicos e a Lei sobre os Serviços da Sociedade da Informação de 2004, que define os regulamentos para provedores de serviço em informática e privacidade de dados.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Letônia:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso – de acordo com o art. 420 § 2 e 3 do Código Penal da Letônia, disseminar vírus conscientemente ocasionando destruição ou modificação de software ou informação ou danos a equipamentos de informação ou destruição de sistemas de proteção. Pena de prisão de até 2 anos ou multa de até 2 salários. A pena pode ser aumentada para até 10 anos se o delito ocasionar danos substanciais;

c) Negação de Serviço

    i. Art. 288 do Código Penal da Letônia – Danificar negligenciando equipamento de telecomunicações, transmissões de rádio ou televisão ou correio e ocasionando a interrupção do serviço. Pena de prisão de até 2 anos, prisão de curta duração, serviços à comunidade ou multa de até 40 salários;

Destruir ou danificar equipamentos de telecomunicações, rádio, televisão ou correio. Pena de prisão de 3 a 10 anos;

ii. Art. 243 do Código Penal da Letônia – Modificar, danificar ou excluir sem autorização informações armazenadas em sistemas baseados em computadores ou inserir conscientemente informação num sistema automatizado ou destruir informações contidas em dispositivos, softwares de computadores ou sistemas de informação. Pena de prisão de até 5 anos ou multa de até 150 salários;

iii. Destruir ou danificar equipamentos de telecomunicações, rádio, televisão ou correio. Pena de prisão de 3 a 10 anos;

d) Comprometimento de conta – de acordo com o art. 241 do Código Penal da Letônia – Acessar arbitrariamente sistema de computador, permitindo que um intruso consiga acessar informações desse sistema. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito;

e) Tentativa de Intrusão - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

f) Acesso não-autorizado a informações

i. Art. 144 do Código Penal da Letônia – Violação intencional da confidencialidade da informação, inclusive através do uso de programas para o processamento eletrônico das informações. Pena de prisão de serviços à comunidade ou multa de até 5 salários. A pena pode ser aumentada prisão de até 3 anos ou prisão de curta duração ou multa de até 60 salários se o crime for cometido com a intenção de obtenção de propriedade;

ii. Art. 241 do Código Penal da Letônia – Acesso arbitrário de informação ocasionando a oportunidade de intruso a acessar informações do sistema. Pena de prisão de curta duração ou multa de até 80 salários. A pena poderá ser aumentada em até 1 ano de prisão ou multa de até 150 salários se o crime for

cometido através quebra de mecanismos de proteção de sistemas ou através do acesso a comunicações;

iii. Art. 242 do Código Penal da Letônia – Cópia não autorizada de software de computador, arquivos ou base de dados armazenadas em sistema de computadores que resultem em dano substancial. Pena de prisão de curta duração ou multa de até 80 salários. A pena poderá ser aumentada em até 2 anos de prisão ou multa de até 150 salários se o crime for cometido através quebra de mecanismos de proteção de sistemas ou através do acesso a comunicações;

g) Acesso não-autorizado a transmissões – de acordo com o art. 144, seções 1 e 2 do Código Penal da Letônia, a violação intencional da confidencialidade de correspondência pessoal ou da transmissão de rede de telecomunicações. Pena de prisão de serviços à comunidade ou multa de até 5 salários. A pena pode ser aumentada prisão de até 3 anos ou prisão de curta duração ou multa de até 60 salários se o crime for cometido com a intenção de obtenção de propriedade;

h) Modificação não-autorizada de Informação – de acordo com o art. 243 do Código Penal da Letônia, modificar, danificar ou excluir informação sem autorização de informação armazenada em sistema de computador ou inserir intencionalmente informações falsas em sistema automatizado ou danificando ou destruindo intencionalmente informações em dispositivos, software ou sistemas de proteção se ocorrerem danos substanciais. Pena de prisão de até 5 anos de prisão ou multa de até 150 salários;

i) Acesso não-autorizado a sistemas de comunicações - Art. 242 do Código Penal da Letônia – Cópia não autorizada de software de computador, arquivos ou base de dados armazenadas em sistema de computadores que resultem em dano substancial. Pena de prisão de curta duração ou multa de até 80 salários. A pena poderá ser aumentada em até 2 anos de prisão ou multa de até 150 salários se o crime for cometido através quebra de mecanismos de proteção de sistemas ou através do acesso a comunicações;

j) Spam – Lei de Serviços da Sociedade da Informação, o uso de mensagens comerciais sem o consentimento prévio do destinatário e mensagens sem a opção de cancelamento do serviço de envio de e-mails.

A prisão de curta duração (custodial arrest) definida no Código Penal da Letônia é uma prisão compulsória de curta duração, que pode ser determinada por um período de 3 dias a 6 meses, de acordo com a Seção 39, do Cap. IV.

18. Lituânia

O Código Penal da Lituânia de 2000 inclui dispositivos sobre crimes por computador, como destruição ou modificação de informação ou programas de computadores.

Infrações como spams e acesso não autorizado a transmissões podem ser penalizados através do Código Administrativo da Letônia.

A Lituânia possui legislação específica para atividades que cobrem alguns serviços de informática, como a Lei de Direitos Autorais, a Lei de Proteção Legal de Dados Pessoais e a Lei de Propaganda da República da Lituânia.

A Lituânia promulgou um decreto sobre o Controle de Informações que não publicáveis em redes públicas e os requisitos para a publicação de informações restritas para dar respaldo à Decisão n° 276/1999/EC do Conselho Europeu de 1999 que promove o uso seguro da Internet, combatendo conteúdos ilícitos e prejudiciais.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Lituânia:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

   i. Art. 196 do Código Penal da Lituânia – Causar dano por apagar, destruir, eliminar ou modificar informações de computador ou usar programas ou dispositivos de computadores com o intuito de

limitar o uso de tais informações ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa ou serviços comunitários;

ii. Art. 197 do Código Penal da Lituânia – Causar dano por apagar, destruir, eliminar ou modificar programa de computador ou interromper ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa;

iii. Art. 153(1), parte 1 do Código Administrativo da Lituânia – Danificar comunicação eletrônica ou acessar rede de comunicações de forma não autorizada é infração passível de multa;

c) Negação de Serviço

i. Art. 197 do Código Penal da Lituânia – Causar dano por apagar, destruir, eliminar ou modificar programa de computador ou interromper ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa;

ii. Art. 196 do Código Penal da Lituânia – Usar programas ou dispositivos de computadores com o intuito de limitar o uso de tais informações ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa ou serviços comunitários;

d) Comprometimento de conta – de acordo com o art. 198(1) do Código Penal da Lituânia – Acessar de forma não autorizada sistema de computador. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito Pena de prisão de até 1 ano ou multa ou serviços comunitários;

e) Tentativa de Intrusão

i. Art. 198(2) do Código Penal da Lituânia – Ações preparatórias visando acesso mão autorizado. Pena de prisão de até 1 ano ou multa ou serviços comunitários;

ii. Art. 153(1), parte 1 do Código Administrativo da Lituânia – Danificar comunicação eletrônica ou acessar rede de comunicações de forma não autorizada é infração passível de multa;

f) Acesso não-autorizado a informações

i. Art. 198(1) do Código Penal da Lituânia – Acessar de forma não autorizada sistema de computador. Pena de prisão de até 3 anos que podem ser aumentados se houver circunstância agravante do delito Pena de prisão de até 1 ano ou multa ou serviços comunitários;

ii. Art. 153(1), parte 1 do Código Administrativo da Lituânia – Danificar comunicação eletrônica ou acessar rede de comunicações de forma não autorizada é infração passível de multa;

g) Acesso não-autorizado a transmissões

i. Art. 166 do Código Penal da Lituânia – Interceptação Ilegal de comunicação privada. Pena de prisão de até 2 anos, multa ou serviços comunitários;

ii. Art. 198(2) do Código Penal da Lituânia – Ações preparatórias visando acesso mão autorizado. Pena de prisão de até 1 ano ou multa ou serviços comunitários;

iii. Art. 153(1), parte 1 do Código Administrativo da Lituânia – Danificar comunicação eletrônica ou acessar rede de comunicações de forma não autorizada é infração passível de multa;

h) Modificação não-autorizada de Informação

i. Art. 196 do Código Penal da Lituânia – Usar programas ou dispositivos de computadores com o intuito de limitar o uso de tais informações ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa ou serviços comunitários;

ii. Art. 197 do Código Penal da Lituânia – Causar dano por apagar, destruir, eliminar ou modificar programa de computador ou interromper ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa;

i) Acesso não-autorizado a sistemas de comunicações

i. Art. 197 do Código Penal da Lituânia – Causar dano por apagar, destruir, eliminar ou modificar programa de computador ou interromper ou alterar redes de computadores, dados ou sistema de computadores. Pena de prisão de até 3 anos ou multa;

ii. Art. 153(1), parte 3 do Código Administrativo da Lituânia – Conexão não autorizada de equipamento resultando em obstrução de comunicações eletrônicas é infração passível de multa;

iii. Art. 153(23) do Código Administrativo da Lituânia – Danificar comunicação eletrônica ou acessar rede de comunicações de forma não autorizada é infração passível de multa;

j) Spam

i. Art. 214(1), parte 3 do Código Administrativo da Lituânia – uso de mensagens comerciais sem o consentimento prévio do destinatário é infração passível de multa;

ii. Art. 22, parte 6 da Lei de Propaganda da Lituânia – propaganda por correio eletrônico sem o consentimento prévio do destinatário é infração passível de multa;

iii. Art. 189(14), do Código Administrativo da Lituânia – a recusa em seguir as definições do Comitê Nacional de Proteção dos Direitos do Consumidor para encerramento de veiculação propaganda que tenham infringido os dispositivos da lei é infração passível de multa.

19. Luxemburgo

Grande parte dos dispositivos relacionados aos crimes por computador na legislação de Luxemburgo foi introduzida pela Lei de Combate à

Criminalidade Econômica e Fraude de Informática de 1993 e incorporados ao Código Penal de Luxemburgo.

Esses dispositivos tratam da proteção de telecomunicações, intrusões e danos decorrentes de intrusão, fraude por computador e obstrução do funcionamento de sistemas computacionais.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação de Luxemburgo:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

    i. Art. 509-2 do Código Penal de Luxemburgo – Obstruir intencional e ilegalmente o funcionamento de sistema de processamento de dados automatizado. Pena de prisão de 3 meses a 3 anos ou multa;

    ii. Art. 509-3 do Código Penal de Luxemburgo – Introduzir, modifica ou excluir dados intencional e ilegalmente em sistema de processamento de dados automatizado. Pena de prisão de 3 meses a 3 anos ou multa;

c) Negação de Serviço

    i. Art. 509-2 do Código Penal de Luxemburgo – Obstruir intencional e ilegalmente o funcionamento de sistema de processamento de dados automatizado. Pena de prisão de 3 meses a 3 anos ou multa;

    ii. Art. 509-3 do Código Penal de Luxemburgo – Introduzir, modifica ou excluir dados intencional e ilegalmente em sistema de processamento de dados automatizado. Pena de prisão de 3 meses a 3 anos ou multa;

d) Comprometimento de conta

    i. Art. 509-1 Seção 1 do Código Penal de Luxemburgo – Acesso ou manutenção de acesso fraudulento a sistema de processamento

de dados automatizado. Pena de prisão de 2 meses a 2 anos ou multa;

ii. Art. 196 do Código Penal de Luxemburgo – Falsificação de credenciais eletrônicas. Pena de prisão de 5 a 10 anos;

iii. Art. 488 do Código Penal de Luxemburgo – Falsificação de chaves eletrônicas. Pena de prisão de 5 a 10 a de 2 meses a 2 anos ou multa;

e) Tentativa de Intrusão – de acordo com o art. 509-1 Seção 1 e 509-6 do Código Penal de Luxemburgo, a tentativa de acesso a sistema de processamento de dados é infração com pena prevista de prisão de 2 meses a 2 anos ou multa;

f) Acesso não-autorizado a informações – de acordo com o art. 509-1 Seção 1 e 509-6 do Código Penal de Luxemburgo, o acesso ou manutenção de acesso fraudulento a sistema de processamento de dados automatizado é infração com pena prevista de prisão de 2 meses a 2 anos ou multa;

g) Acesso não-autorizado a transmissões

i. Art. 509-1 Seção 1 do Código Penal de Luxemburgo – Acesso ou manutenção de acesso fraudulento a sistema de processamento de dados automatizado. Pena de prisão de 2 meses a 2 anos ou multa;

ii. Art. 2 Sub-seção 3 da Lei de Proteção da Privacidade de Luxemburgo – Acesso voluntário a conteúdo de mensagem privada sem consentimento do remetente ou destinatário. Pena de prisão de 8 dias a 1 ano ou multa;

iii. Art. 3 da Lei de Proteção da Privacidade de Luxemburgo – Instalação intencional de dispositivo com o propósito de acessar o conteúdo de mensagem privada sem consentimento do remetente ou destinatário. Pena de prisão de 8 dias a 1 ano ou multa;

h) Modificação não-autorizada de Informação – de acordo com o art. 509-1 Seção 2 do Código Penal de Luxemburgo, o acesso ou manutenção

de acesso fraudulento a sistema de processamento de dados automatizado ou a obstrução do seu bom funcionamento é infração com pena prevista de prisão de 2 meses a 2 anos ou multa;

i) Acesso não-autorizado a sistemas de comunicações

   i. Art. 509-1 Seção 1 do Código Penal de Luxemburgo – Acesso ou manutenção de acesso fraudulento a sistema de processamento de dados automatizado. Pena de prisão de 2 meses a 2 anos ou multa;

   ii. Art. 509-1 Seção 2 do Código Penal de Luxemburgo - Acesso ou manutenção de acesso fraudulento a sistema de processamento de dados automatizado ou a obstrução do seu bom funcionamento. Pena de prisão de 2 meses a 2 anos ou multa;

j) Spam – Art. 48 da Lei de Comércio Eletrônico de Luxemburgo – Enviar comunicações de natureza comercial sem consentimento prévio do destinatário. Pena de prisão de 8 dias a 1 ano ou multa.

20. Malta

Malta possui dispositivos específicos para crimes que envolvem informática em seu Código Penal que incluem acesso e uso ilegal de informação e uso indevido de hardware.

O país também possui leis específicas como a Lei de Comércio Eletrônico e a Lei de Comunicações Eletrônicas, sendo que para algumas infrações são aplicadas multas administrativas.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação de Malta:

a) Rastreamento (Scan)

   i. Art. 337C(1) (f) do Código Penal de Malta – Tomar posse ou usar de forma não autorizada quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

ii. Art. 337F(4) do Código Penal de Malta – Produzir quaisquer materiais ou cometer quaisquer atos preparatórios para acesso não autorizado. Mesma pena para a infração de acesso não autorizado;

b) Código Malicioso

i. Art. 337C(1) (d) do Código Penal de Malta – Obstruir o acesso de forma não autorizada a quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

ii. Art. 337C(1) (e) do Código Penal de Malta – Prejudicar a operação de quaisquer sistemas ou software ou integridade e confiabilidade de quaisquer dados. Pena de prisão de até 4 anos ou multa;

iii. Art. 337C(1) (g) do Código Penal de Malta – Instalar, mover, modificar, apagar ou destruir quaisquer sistemas ou software ou integridade e confiabilidade de quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

iv. Art. 337D (b) do Código Penal de Malta – Tomar posse, danificar ou destruir computadores, sistemas de computadores, redes de computadores ou suprimentos de computadores com o intuito de danificar a operação. Pena de prisão de até 4 anos ou multa;

c) Negação de Serviço

i. Art. 337C(1) (d) do Código Penal de Malta – Obstruir o acesso a quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

ii. Art. 337C(1) (e) do Código Penal de Malta – Prejudicar a operação de quaisquer sistema, softwares ou a integridade e confiabilidade de quaisquer dados. Pena de prisão de até 4 anos ou multa;

iii. Art. 337D (b) do Código Penal de Malta – Tomar posse, danificar ou destruir computadores, sistemas de computadores, redes de computadores ou suprimentos de computadores com o intuito de danificar a operação. Pena de prisão de até 4 anos ou multa;

d) Comprometimento de conta

i. Art. 337C(1) (a) do Código Penal de Malta – Usar computador ou outros dispositivos de forma não autorizada para acessar dados, softwares ou documentação de suporte contidos nesse ou em outros equipamentos ou usando, copiando ou modificando quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

ii. Art. 337C(1) (f) do Código Penal de Malta – Tomar posse ou usar de forma não autorizada quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

iii. Art. 337C(1) (i) do Código Penal de Malta – Usar códigos de acessos, senha, identificação, endereço de correio eletrônico ou quaisquer meios de acesso ou informações de acesso de forma não autorizada em um computador. Pena de prisão de até 4 anos ou multa;

e) Tentativa de Intrusão – de acordo com o art. 337F(4) do Código Penal de Malta – Produzir quaisquer materiais ou cometer quaisquer atos preparatórios para acesso não autorizado. Mesma pena para a infração de acesso não autorizado;

f) Acesso não-autorizado a informações

i. Art. 337C(1) (a) do Código Penal de Malta – Usar computador ou outros dispositivos de forma não autorizada para acessar dados, softwares ou documentação de suporte contidos nesse ou em outros equipamentos ou usando, copiando ou modificando quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

ii. Art. 337C(1) (f) do Código Penal de Malta – Tomar posse ou usar de forma não autorizada quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

iii. Art. 337C(1) (i) do Código Penal de Malta – Usar códigos de acessos, senha, identificação, endereço de correio eletrônico ou quaisquer meios de acesso ou informações de acesso de forma não autorizada em um computador. Pena de prisão de até 4 anos ou multa;

iv. Art. 15 (1) da Lei de Serviços de Segurança – Interceptação de comunicação sem mandado judicial. Pena de prisão de até 2 anos e/ou multa;

v. Art. 23 (1) da Lei de Comércio Eletrônico – Acessar, copiar, se apropriar ou recriar dispositivo de assinatura de terceiros com a intenção de criar ou permitir que alguém crie assinatura não autorizada através de tal dispositivo. Pena de prisão de até 4 anos ou multa;

g) Acesso não-autorizado a transmissões

i. Art. 15 (1) da Lei de Serviços de Segurança – Interceptação de comunicação sem mandado judicial. Pena de prisão de até 2 anos e/ou multa;

ii. Art. 16 (1) (a) da Lei de Serviços de Segurança – Divulgação intencional da transmissão ou de seu conteúdo por funcionário de serviços de telecomunicações. Pena de prisão de até 1 ano e/ou multa;

iii. Art. 35 (3) da Lei de Comércio Eletrônico – Infrações cometidas em transmissões ou mensagens por funcionários de prestadoras de serviço de redes ou serviços de comunicações eletrônicas ou instalações associadas. Pena de prisão de até 6 meses ou multa;

iv. Regulamento 5(1) dos Regulamentos de Processamento de Dados Pessoais – Ouvir, colocar escutas, manter ou conduzir

quaisquer outros tipos de interceptação ou vigilância de comunicações ou tráfego de dados. Suscetível a multa;

h) Modificação não-autorizada de Informação

i. Art. 337C(1) (a) do Código Penal de Malta – Usar computador ou outros dispositivos de forma não autorizada para acessar dados, softwares ou documentação de suporte contidos nesse ou em outros equipamentos ou usando, copiando ou modificando quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

ii. Art. 337C(1) (b) do Código Penal de Malta – Extrair de forma não autorizada quaisquer dados, softwares ou documentações de suporte. Seja através de exibição em tela ou quaisquer outros meios. Pena de prisão de até 4 anos ou multa;

iii. Art. 337C(1) (c) do Código Penal de Malta – Copiar forma não autorizada quaisquer dados, softwares ou documentações de suporte para quaisquer mídias de armazenamento Pena de prisão de até 4 anos ou multa;

iv. Art. 337C(1) (f) do Código Penal de Malta – Tomar posse ou usar de forma não autorizada quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

v. Art. 337C(1) (g) do Código Penal de Malta – Instalar, mover, modificar, apagar ou destruir quaisquer sistemas ou software ou integridade e confiabilidade de quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 4 anos ou multa;

vi. Art. 23 (2) da Lei de Comércio Eletrônico – Alterar, divulgar ou usar dispositivo de assinatura de terceiros sem autorização ou em excesso a ordem judicial, criar ou permitir intencionalmente que alguém crie assinatura não autorizada através de tal dispositivo. Pena de prisão de até 4 anos ou multa;

vii. Art. 23 (3) da Lei de Comércio Eletrônico – Criar, publicar ou alterar quaisquer outras atividades utilizando certificado ou assinatura eletrônica para fraudes ou quaisquer outras finalidades ilícitas.. Pena de prisão de até 4 anos ou multa;

viii. Art. 23 (5) da Lei de Comércio Eletrônico – Acessar, copiar, se apropriar ou recriar dispositivo de criação de assinatura de provedores de serviços de certificação sem autorização com a intenção de criar ou permitir que alguém crie assinatura não autorizada através de tal dispositivo ou em excesso a ordem judicial, criar ou permitir intencionalmente que alguém crie assinatura não autorizada através de tal dispositivo. Pena de prisão de até 4 anos ou multa;

i) Acesso não-autorizado a sistemas de comunicações

i. Art. 5 (1) (d) da Lei de Comércio Eletrônico – Usar redes ou dispositivos de comunicações eletrônicas com propósito distinto para o qual foi fornecido ou para uso impróprio.. Suscetível a multa;

ii. Art. 337D (a) do Código Penal de Malta – Modificar sem autorização computadores, sistemas de computadores, redes de computadores ou suprimentos de computadores. Pena de prisão de até 4 anos ou multa;

iii. Art. 337C(1) (i) do Código Penal de Malta – Usar códigos de acessos, senha, identificação, endereço de correio eletrônico ou quaisquer meios de acesso ou informações de acesso de forma não autorizada em um computador. Pena de prisão de até 4 anos ou multa;

j) Spam – Regulamento 10 dos Regulamentos de Processamento de Dados Pessoais – Se utilizar de quaisquer serviços de comunicações eletrônicas para encaminhar comunicações não solicitadas com intuito comercial sem consentimento prévio explícito. Suscetível a multa.

21. Polônia

O Código Penal da Polônia, assim como o Código de Processo Penal vêm sendo atualizados para a inclusão de dispositivos relacionados a informática.

Em 2004 foi aprovada uma emenda com o propósito de tornar aderente a legislação polonesa à Convenção em Crimes Cibernéticos do Conselho da Europa.

A Polônia conta também com lei específica em informática, como a Lei de 18 de julho de 2002 sobre serviços eletrônicos e define dispositivos sobre spam.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação polonesa:

a) Rastreamento (Scan) – Não é penalizado na maioria dos casos, mas pode ser aplicado o art. 267 §1 do Código Penal polonês – Obter informação sem autorização através da conexão à transmissão ou da quebra de mecanismos de proteção. Pena de prisão de até 2 anos, restrição da liberdade de até 12 meses e multa;

b) Código Malicioso

    i. Art.269a do Código Penal Polonês – Obstruir ilegalmente o funcionamento de sistema computacional através de transmissões, dano, exclusão ou modificação de dados de computador. o acesso de forma não autorizada a quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 5 anos;

    ii. Art.268a §1 do Código Penal Polonês – Destruir, danificar, excluir ou alterar registro de informação essencial em transmissão eletrônica de informações, obstruindo ou tornando o acesso mais difícil aos usuários autorizados. Pena de prisão de até 2 anos e multa;

iii. Art.268a §2 do Código Penal Polonês – Infração do art. 268a §1 com danos materiais significantes (40.000 euros ou mais. Pena de prisão de até 5 anos;

c) Negação de Serviço – de acordo com o art. 269a do Código Penal Polonês, obstruir ilegalmente o funcionamento de sistema computacional através de transmissões, dano, exclusão ou modificação de dados de computador. o acesso de forma não autorizada a quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 5 anos;

d) Comprometimento de conta– de acordo com o art. 269b §1 do Código Penal Polonês, acessar informações ilegalmente através de ferramentas hacker ou do uso de senhas, códigos de acesso ou similares de forma ilegal. Pena de prisão de até 3 anos;

e) Tentativa de Intrusão

   i. Art. 269b §1 e 14 §1 do Código Penal Polonês – Tentativa de acesso ilegal a sistema de informação através de ferramentas hacker ou do uso de senhas, códigos de acesso ou similares de forma ilegal. Pena de prisão de até 3 anos;

   ii. Art. 267 §1 e 14 §1 do Código Penal polonês – Tentativa de obter informação sem autorização através da conexão à transmissão ou da quebra de mecanismos de proteção. Pena de prisão de até 2 anos, restrição da liberdade de até 12 meses e multa;

f) Acesso não-autorizado a informações

   i. Art. 269b §1 do Código Penal Polonês – Acesso ilegal a sistema de informação através de ferramentas hacker ou do uso de senhas, códigos de acesso ou similares de forma ilegal. Pena de prisão de até 3 anos;

   ii. Art. 267 §1 do Código Penal polonês – Obter informação sem autorização através da conexão à transmissão ou da quebra de mecanismos de proteção. Pena de prisão de até 2 anos, restrição da liberdade de até 12 meses e multa;

g) Acesso não-autorizado a transmissões

   i. Art. 267 §1 do Código Penal polonês – Obter informação sem autorização através da conexão à transmissão ou da quebra de mecanismos de proteção. Pena de prisão de até 2 anos, restrição da liberdade de até 12 meses e multa;

   ii. Art. 269a do Código Penal Polonês - Obstruir ilegalmente o funcionamento de sistema computacional através de transmissões, dano, exclusão ou modificação de dados de computador. o acesso de forma não autorizada a quaisquer dados, softwares ou documentação de suporte. Pena de prisão de até 5 ano;

h) Modificação não-autorizada de Informação

   i. Art. 269b §1 do Código Penal Polonês – Acesso ilegal a sistema de informação através de ferramentas hacker ou do uso de senhas, códigos de acesso ou similares de forma ilegal. Pena de prisão de até 3 anos;

   ii. Art. 267 §1 do Código Penal polonês – Obter informação sem autorização através da conexão à transmissão ou da quebra de mecanismos de proteção. Pena de prisão de até 2 anos, restrição da liberdade de até 12 meses e multa;

i) Acesso não-autorizado a sistemas de comunicações, de acordo com o art. 269b §1 do Código Penal Polonês, acesso ilegal a sistema de informação através de ferramentas hacker ou do uso de senhas, códigos de acesso ou similares de forma ilegal. Pena de prisão de até 3 anos

j) Spam – de acordo com o art. 24 da Lei de 18 de Julho de 2002 sobre Serviços Disponibilizados Eletronicamente, distribuição de informação comercial não solicitada é contravenção suscetível a prisão de 30 dias, restrição da liberdade ou multa.

22. Portugal

Portugal possui tradição em regulamentos específicos relacionados à informática. Em 1991, promulgou a Lei da Criminalidade Informática que estabeleceu uma estrutura legal a ser aplicada em crimes por computador, aderente à Recomendação 89(9) do Conselho Europeu.

O Código Penal português sofreu uma atualização para a inclusão de fraudes por computador.em 1998.

Além dessa atualização, Portugal conta com outras leis específicas como a Lei 67/98 de 1998 que dispõe sobre acesso a dados pessoais e a diretiva do Parlamento Europeu e Conselho de 2002, aplicado através da Lei do Comércio Eletrônico e da Lei 41/2004 que dispõem sobre retenção de dados em provedoras e operadoras de comunicação eletrônica e sobre spam.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação portuguesa:

a) Rastreamento (Scan) – de acordo com o art. 8 da lei 109/91 portuguesa, a interceptação da comunicação em sistema sem autorização e usando dispositivos técnicos é infração passível de pena de prisão de até 3 anos ou multa;
b) Código Malicioso
    i. Art. 5 da lei 109/91 portuguesa – Causar dano intencionalmente ao suprimir ou excluir total ou parcialmente um programa de computador para obter benefício ilegítimo para o agente ou para terceiros. A aplicação desse dispositivo depende do alvo da ação e da intenção do perpetrador. Pena de prisão de até 10 anos ou multa, depende do dano ocasionado;
    ii. Art. 6 da lei 109/91 portuguesa – Introduzir, modificar, apagar ou suprimir dados ou programas de computador através da intervenção num sistema com a intenção de impedir ou perturbar o funcionamento de um sistema de computador ou comunicação. Pena de prisão de até 10 anos ou multa, depende do dano ocasionado;

c) Negação de Serviço – de acordo com o art. 6 da lei 109/91 portuguesa, introduzir, modificar, apagar ou suprimir dados ou programas de computador através da intervenção num sistema com a intenção de impedir ou perturbar o funcionamento de um sistema de computador ou comunicação. Pena de prisão de até 10 anos ou multa, depende do dano ocasionado;

d) Comprometimento de conta – o art. 7 da lei 109/91 portuguesa, acessar sem autorização um sistema com a intenção de obter um benefício ou vantagem ilegítima para o próprio agente ou para terceiros. A mera invasão não é punível, depende da intenção da ação. Pena de prisão de até 5 anos ou multa;

e) Tentativa de Intrusão – o art. 7 da lei 109/91 portuguesa, tentar acessar sem autorização um sistema com a intenção de obter um benefício ou vantagem ilegítima para o próprio agente ou para terceiros. A mera invasão não é punível, depende da intenção da ação. Pena de prisão de até 1 ano ou multa;

f) Acesso não-autorizado a informações

   i. Art. 7 da lei 109/91 portuguesa - acessar sem autorização um sistema com a intenção de obter um benefício ou vantagem ilegítima para o próprio agente ou para terceiros. A mera invasão não é punível, depende da intenção da ação. Pena de prisão de até 5 anos ou multa;

   ii. Art. 8 da lei 109/91 portuguesa - interceptação da comunicação em sistema sem autorização e usando dispositivos técnicos. Pena de prisão de até 3 anos ou multa;

   iii. Art. 44 da lei 67/98 portuguesa – obter acesso ilegal a dados pessoais. Pena de prisão de até 1 ano ou multa que podem ser aumentados dependendo do dano, do meio utilizado e benefício ilegítimo obtido;

g) Acesso não-autorizado a transmissões – de acordo com o art. 8 da lei 109/91 portuguesa, a interceptação da comunicação em sistema sem

autorização e usando dispositivos técnicos é infração passível de pena de prisão de até 3 anos ou multa;

h) Modificação não-autorizada de Informação

   i. Art. 6 da lei 109/91 portuguesa – Introduzir, modificar, apagar ou suprimir dados ou programas de computador através da intervenção num sistema com a intenção de impedir ou perturbar o funcionamento de um sistema de computador ou comunicação. Pena de prisão de até 10 anos ou multa, depende do dano ocasionado;

   ii. Art. 5 da lei 109/91 portuguesa – Causar dano intencionalmente ao suprimir ou excluir total ou parcialmente um programa de computador para obter benefício ilegítimo para o agente ou para terceiros. A aplicação desse dispositivo depende do alvo da ação e da intenção do perpetrador. Pena de prisão de até 10 anos ou multa, depende do dano ocasionado;

i) Acesso não-autorizado a sistemas de comunicações - de acordo com o art. 6 da lei 109/91 portuguesa, introduzir, modificar, apagar ou suprimir dados ou programas de computador através da intervenção num sistema com a intenção de impedir ou perturbar o funcionamento de um sistema de computador ou comunicação. Pena de prisão de até 10 anos ou multa, depende do dano ocasionado;

j) Spam – de acordo com o art. 22 do Decreto de Lei 7/2004, o uso de correio eletrônicos para finalidade comercial sem consentimento prévio do destinatário (pessoa física). No caso de pessoa jurídica é permitido desde que seja incluída a opção de remoção da lista (opt-out). A negligência também é punível. Suscetível a multa.

23. Reino Unido

No Reino Unido, os crimes por computador são punidos através das leis já existentes que sofreram reformas através da atualização e ampliação das leis existentes de forma abranger novas situações em vez de introduzir leis completamente novas, segundo o European Comission (2006).

A Lei de Mau Uso de Computador, em vigor em 1990, foi criada para prevenir acesso não autorizado ou modificações de sistemas de computadores e evitar o uso do computador como instrumento para cometer infrações.

De 2004 a 2005 a lei passou por revisões que incluíram dispositivos conectados em rede, atualização de termos e ataques DoS.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação do Reino Unido:

a) Rastreamento (Scan)

    i. Seção 1 da Lei de Regulação dos Poderes Investigativos de 2000 – Interceptação intencional e não autorizada da transmissão de quaisquer comunicações através de serviços postais ou de sistema de comunicação público. Pena de até 2 anos de prisão ou multa;

    ii. Seção 2 da Lei de Mau Uso de Computador – Facilitar o cometimento dos crimes descritos na seção 1 da Lei de Mau Uso de Computador. Pena de até 6 meses e/ou multa;

b) Código Malicioso – de acordo com a Seção 3 da Lei de Mau Uso de Computador, ter conhecimento e causar a modificação intencional e não autorizada do conteúdo de quaisquer computadores é infração com pena de até 5 anos ou multa;

c) Negação de Serviço – de acordo com a Seção 3 da Lei de Mau Uso de Computador, ter conhecimento e causar a modificação intencional e não autorizada do conteúdo de quaisquer computadores, (a) para ocasionar danos a operação; (b) impedir ou obstruir o acesso a quaisquer programa ou dados em qualquer computador; ou (c) para ocasionar danos a operação de um programa ou da confiabilidade dos dados é infração com pena de até 5 anos ou multa;

d) Comprometimento de conta Serviço – de acordo com a Seção 1 da Lei de Mau Uso de Computador, fazer com que um computador execute quaisquer funções com a intenção de manter acesso não autorizado a

quaisquer programas ou dados de um computador é infração com pena de até 6 meses ou multa. A promotoria pode conduzir o caso como fraude e não como crime de computador;

e) Tentativa de Intrusão – de acordo com a Seção 1 da Lei de Mau Uso de Computador, fazer com que um computador execute quaisquer funções com a intenção de manter acesso não autorizado a quaisquer programas ou dados de um computador é infração com pena de até 6 meses ou multa. A promotoria pode conduzir o caso como fraude e não como crime de computador;

f) Acesso não-autorizado a informações - não há dispositivos específicos, a acusação se baseia no modus operandi;

g) Acesso não-autorizado a transmissões – de acordo com a Seção 1 da Lei de Regulação dos Poderes Investigativos de 2000, a interceptação intencional e não autorizada da transmissão de quaisquer comunicações através de serviços postais ou de sistema de comunicação público é infração com pena de até 2 anos de prisão ou multa;

h) Modificação não-autorizada de Informação – de acordo com a Seção 3 da Lei de Mau Uso de Computador, ter conhecimento e causar a modificação intencional e não autorizada do conteúdo de quaisquer computadores é infração com pena de até 5 anos ou multa;

i) Acesso não-autorizado a sistemas de comunicações – de acordo com a Seção 1 da Lei de Regulação dos Poderes Investigativos de 2000, a interceptação intencional e não autorizada da transmissão de quaisquer comunicações através de serviços postais ou de sistema de comunicação público é infração com pena de até 2 anos de prisão ou multa

j) Spam – de acordo com os dispositivos sobre Comunicações Eletrônicas e Privacidade:

    i. Material de marketing não solicitado não deve ser enviado via e-mail sem consentimento prévio do destinatário;

ii. Material de marketing não solicitado não deve ser enviado via e-mail se o endereço do remetente for mascarado, ocultado ou inválido.

24. República Checa

O Código Penal da República Tcheca sofreu atualizações em 1991 que incluiu a Seção 257a que trata dos danos e mau uso de dados.

Os tchecos contam com algumas leis específicas como a Lei 480 de 2004 que possui dispositivos sobre spam, considerada um ilícito civil indenizável e lei de proteção de dados pessoais.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação do Reino Unido:

a) Rastreamento (Scan) - não há dispositivos específicos e só poderá ser punível se for tentado ou cometido crime subsequentemente;

b) Código Malicioso

   i. Seção 257a do Código Penal – Obter acesso não autorizado a dados e modificar, alterar ou excluir dados ou modificar sistema de computador com a intenção de ocasionado danos. Pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

   ii. Seção 249 do Código Penal – Uso de propriedade de terceiros sem autorização. Pena de prisão de até 3 anos, proibição de ações específicas ou multa;

   iii. Art. 182(1)(a) do Código Penal – Prejudicar e colocar em perigo a operação de instalações de telecomunicações públicas. Pena de prisão de até 6 anos ou multa;

c) Negação de Serviço

   i. Seção 257a do Código Penal – Uso não autorizado, destruir ou tornar os dados de provedora de telecomunicações inutilizáveis com a intenção de ocasionar dano. Pena de prisão de até 5 anos,

restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

ii. Art. 182(1)(a) do Código Penal – Prejudicar e colocar em perigo a operação de instalações de telecomunicações públicas. Pena de prisão de até 6 anos ou multa;

d) Comprometimento de conta

i. Seção 257a do Código Penal – Ganhar acesso intencionalmente a provedora de telecomunicações, seguido de uso, alteração, exclusão ou modificação não autorizada de dados. Pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

ii. Seção 249 do Código Penal – Uso de propriedade de terceiros sem autorização. Pena de prisão de até 3 anos, proibição de ações específicas ou multa;

e) Tentativa de Intrusão

i. Seção 257a em conjunto com a Seção 8 do Código Penal – Medidas preparatórias com o objetivo de ganhar acesso intencionalmente a provedora de telecomunicações, seguido de uso, alteração, exclusão ou modificação não autorizada de dados. Pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

ii. Seção 249 do Código Penal – Medidas preparatórias com o objetivo de usar propriedade de terceiros sem autorização. Pena de prisão de até 3 anos, proibição de ações específicas ou multa;

f) Acesso não-autorizado a informações

i. Seção 257a do Código Penal – Ganhar acesso intencionalmente a provedora de telecomunicações, seguido de uso, alteração, exclusão ou modificação não autorizada de dados. Pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos

específicos ou multa, que podem variar de acordo com os danos ocasionados;

ii. Art. 239 do Código Penal – Interceptação de comunicação ou de comunicação de dados privada. Pena de prisão de até 6 meses. Quando cometido pelo provedor de comunicação, a pena pode ser aumentada para 1 ano ou perda da licença de operação;

g) Acesso não-autorizado a transmissões

i. Seção 257a do Código Penal – Ganhar acesso intencionalmente a provedora de telecomunicações, seguido de uso, alteração, exclusão ou modificação não autorizada de dados. Pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

ii. Art. 239 do Código Penal – Interceptação de comunicação ou de comunicação de dados privada. Pena de prisão de até 6 meses. Quando cometido pelo provedor de comunicação, a pena pode ser aumentada para 1 ano ou perda da licença de operação;

iii. Art. 240 do Código Penal – Divulgação do conteúdo de informações confidenciais ou o abuso de tais mensagens. Pena de prisão de até 2anos ou proibição de atividades específicas;

iv. Art. 182(1)(a) do Código Penal – Prejudicar e colocar em perigo a operação de instalações de telecomunicações públicas. Pena de prisão de até 6 anos ou multa;

h) Modificação não-autorizada de Informação – de acordo com o art. 257a do Código Penal, ganhar acesso intencionalmente a provedora de telecomunicações, seguido de uso, alteração, exclusão ou modificação não autorizada de dados é infração com previsão de pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

i) Acesso não-autorizado a sistemas de comunicações

i. Seção 257a do Código Penal – Ganhar acesso intencionalmente a provedora de telecomunicações, seguido de uso, alteração, exclusão ou modificação não autorizada de dados. Pena de prisão de até 5 anos, restrição de liberdade ou de acesso a objetos específicos ou multa, que podem variar de acordo com os danos ocasionados;

ii. Art. 182(1)(a) do Código Penal – Prejudicar e colocar em perigo a operação de instalações de telecomunicações públicas. Pena de prisão de até 6 anos ou multa;

j) Spam

i. Seção 11(1) da Lei de Serviços da Sociedade da Informação – Uso de mensagens comerciais sem o consentimento prévio do destinatário é infração passível de multa;

ii. Art. 178 da do Código Penal – Processamento não autorizado de dados pessoais, mesmo por negligência é infração passível de multa.

25. Suécia

A Suécia conta com vários dispositivos específicos em seu Código Penal e está em processo de harmonização com a Convenção em Crimes Cibernéticos do Conselho da Europa e com a Decisão sobre a Estrutura em Ataques contra Sistemas de Informação do Conselho Europeu.

Dentre os dispositivos específicos sobre informática, o Código Penal sueco trata da violação do sigilo de telecomunicações e correio, da intrusão em depositório seguro, da escuta, da violação de sigilo de dados, da destruição ou dano de propriedade, de dano, destruição ou obstrução de propriedade pública e da sabotagem.

No que se refere à tabela de incidentes da European Comission (2006), pode-se identificar na legislação da Suécia:

a) Rastreamento (Scan)

i. Cap. 4, Seção 9c do Código Penal – Violação do sigilo de dados. Pena de até 2 anos de prisão ou multa;

ii. Cap. 4, Seção 10 do Código Penal – Tentativa de violação do sigilo de dados. Pena de até 2 anos de prisão ou multa;

b) Código Malicioso – de acordo com o Cap. 4, Seção 9c do Código Penal, a violação do sigilo de dados é infração passível de pena de até 2 anos de prisão ou multa;

c) Negação de Serviço – de acordo com o Cap. 4, Seção 9c do Código Penal, a privação ilegal é infração passível de pena de até 2 anos de prisão ou multa;

d) Comprometimento de conta Serviço – de acordo com o Cap. 4, Seção 9c do Código Penal, a violação do sigilo de dados é infração passível de pena de até 2 anos de prisão ou multa;

e) Tentativa de Intrusão

i. Cap. 4, Seção 9c do Código Penal – Violação do sigilo de dados. Pena de até 2 anos de prisão ou multa;

ii. Cap. 4, Seção 10 do Código Penal – Tentativa de violação do sigilo de dados. Pena de até 2 anos de prisão ou multa;

f) Acesso não-autorizado a informações

i. Cap. 4, Seção 9c do Código Penal – Violação do sigilo de dados. Pena de até 2 anos de prisão ou multa;

ii. Cap. 4, Seção 10 do Código Penal – Tentativa de violação do sigilo de dados. Pena de até 2 anos de prisão ou multa;

g) Acesso não-autorizado a transmissões – de acordo com o Cap. 4, Seção 9c do Código Penal, a privação ilegal é infração passível de pena de até 2 anos de prisão ou multa;

h) Modificação não-autorizada de Informação – de acordo com o Cap. 4, Seção 9c do Código Penal, a privação ilegal é infração passível de pena de até 2 anos de prisão ou multa;

i) Acesso não-autorizado a sistemas de comunicações – de acordo com o Cap. 4, Seção 9c do Código Penal, a privação ilegal é infração passível de pena de até 2 anos de prisão ou multa;

iii. Spam – de acordo com a Seção 13b da Lei de Práticas de Marketing – Não há sanção, no entanto, pode ser aplicada multa se a ação não for interrompida após a ordem de encerrar a atividade.