UNIVERSIDADE FEDERAL DE SANTA CATARINA

ESPECIALIZAÇÃO EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO APLICADAS À SEGURANÇA PÚBLICA E DIREITOS HUMANOS

DEIVIS NOAL FERREIRA

PLANEJAMENTO DE AÇÕES PARA APLICAÇÃO DA LEGISLAÇÃO ATUAL SOBRE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO CORRELACIONADA AS NORMAS EXISTENTE DENTRO DA INSTITUIÇÃO BRIGADA MILITAR

Araranguá, 12 de dezembro de 2016

DEIVIS NOAL FERREIRA

PLANEJAMENTO DE AÇÕES PARA APLICAÇÃO DA LEGISLAÇÃO ATUAL SO-BRE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO CORRELACIONADA AS NOR-MAS EXISTENTE DENTRO DA INSTITUIÇÃO BRIGADA

Trabalho de Curso submetido à Universidade Federal de Santa Catarina – UFSC, como parte dos requisitos necessários para a obtenção do Grau de Especialista em Tecnologia da Informação e Comunicação Aplicada à Segurança Pública e Direitos Humanos. Sob a orientação da Professora Dra. Solange Maria da Silva.

Araranguá, 2016

Deivis Noal Ferreira

Planejamento de ações para aplicação da legislação atual sobre tecnologia da informação e comunicação correlacionada as normas existente dentro da instituição Brigada Militar

Trabalho de Curso submetido à Universidade Federal de Santa Catarina – UFSC, como parte dos requisitos necessários para a obtenção do Grau de Especialista em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos.

_____
Professora Solange Maria da Silva
Doutora/UFSC

_____
Examinador
Título/Instituição

_____
Examinador
Título/Instituição

Araranguá, 12 de dezembro de 2016

“Dedico esta conquista em especial a minha filha Bethina, que nasceu em meio a realização do curso e a minha esposa Fernanda, que com amor e compreensão colaborou para o resultado deste trabalho, por incentivar e escutar quando mais precisava durante esta caminhada.

AGRADECIMENTOS

Agradeço a Deus por esta oportunidade de aprendizagem que foi concedida, pela força, fé e coragem para encarar as adversidades, nunca permitindo que desistisse de alcançar o meu objetivo. Agradeço o apoio da família e aos meus colegas dos diversos Órgãos que atuam na Segurança Pública que diuturnamente dedicam suas vidas para a manutenção da ordem. Ao coordenador do Curso de Especialização em Tecnologias da Informação e Comunicação Aplicadas à Segurança Pública e Direitos Humanos, Professor Giovani, Coordenador do Pós TIC SENASP, sempre disponível a auxiliar em qualquer adversidade encontrada ao longo do caminho. A Natana muito competente no assessoramento para o bom andamento do Curso. Ao meu chefe Major Alex Sandre Pinheiro Severo, Chefe da Divisão de Redes do Departamento de Informática da Brigada Militar, grande incentivador para a realização deste estudo. A todos os professores que me acompanharam durante a especialização, em especial a minha orientadora, Professora Dra. Solange Maria da Silva, responsável pela realização deste trabalho. À Universidade Federal de Santa Catarina – UFSC e a Brigada Militar do Estado do Rio Grande do Sul.

"O homem não teria alcançado o possível se, repetidas vezes, não tivesse tentado o impossível".

Max Weber

RESUMO

Este trabalho propõe que sejam observados a legislação vigente aplicando a realidade, viabilizando a possibilidade de desenvolver atividades possuindo um amparo legal nas mais diversas áreas de atuação. Ainda, pretende uma análise de correlação entre as leis aprovadas recentemente e o que existe na Corporação, com o objetivo de apontar as lacunas existentes. No meio Institucional é importante que exista previsão escrita regulamentando o uso dos serviços de tecnologia da informação e comunicações. Estes documentos devem possuir a definição de alguns conceitos para levar a conhecimento do usuário, principalmente aquele que não possui formação técnica no assunto, cabe salientar que é a maioria. Será abordado o fenômeno informacional não apenas como uma construção social, mas o usuário da informação dentro da Instituição, limitado por um contexto político-histórico-cultural, deve obedecer ao conteúdo das normas regulatórias vigentes. Para analisar estas questões, tomou-se como referência teórico-metodológica a análise dos casos práticos observados na atividade fim, compreendendo a legislação e a análise doutrinária desses fenômenos, bem como uma breve explanação da tipificação dos delitos informáticos com o intuito de exemplificar as consequências para o uso indevido dos serviços. A pesquisa descreve alguns princípios que podem ser utilizados como referência, apontando as delimitações do objeto das Notas de Instrução da Instituição, indicando alternativas para as situações em que ocorram cometimento de falta grave por usuários ao descumprir o previsto em norma. Também analisa princípios constitucionais que podem ser observados como referência para orientar a utilização das TIC pelos usuários. Salientando a importância da normatização interna da Instituição quanto ao auxílio aos gestores no controle do uso correto do acesso a informação.

Palavras-chave: Segurança Pública, Tecnologia da Informação e Comunicação, Policia Militar, Legislação, Notas de Instrução

ABSTRACT

This study proposes that are observed at current legislation applying realida, enabling the possibility of developing activities having a legal support in various areas of practice. Still, you want an analysis of correlation between the laws approved and filed recently and what exists in the enterprise, with the objective of pointing out the shortcomings there and try. In the middle building it is important to have written estimates by regulating the use of information technology services and communications. Will be addressed the phenomenon of information not only as a social construction, but the user of information within the institution, limited by a political and cultural-historical, must comply with the content of the regulatory norms in force. To analyze these issues, it was taken as th20eoretical-methodological reference analysis of practical cases observed in the activity end, understanding the Law and the analysis of these doctrinal phenomena, as well as a brief explanation of the typification of the offenses with a view to illustrate the consequences for inappropriate use of services. The research describes some principles that can be used as a reference, pointing out the boundaries of the object of the notes of instruction of the Institution, indicating alternatives for situations in which occur committing of serious misconduct by users to circumvent the prescribed in the standard. It also analyzes the constitutional principles that can be observed as a reference to guide the use of ICT by users. Stressing the importance of standardization within the institution with regard to aid managers in control of the correct use of the access to information.

Keywords: Public Security, Information and Communication Technology, Military Police, Legislation, Instruction Notes.

LISTA DE ILUSTRAÇÕES

Figura 1.....26

Figura 2.....34

Figura 3: Políticas (Estratégico), Normas (Tático) e Procedimentos (Operacional).....36

LISTA DE ABREVIATURAS E SIGLAS

APF - Administração Pública Federal
CNJ - Conselho Nacional de Justiça
DSIC - Departamento de Segurança da Informação e Comunicações
GGI - Gabinete de Gestão Integrada
GSIC - Gestão da Segurança da Informação Comunicações.
ITIL - Information Technology Infrastructure Library
MJ - Ministério da Justiça
NI – Nota de Instrução
PMERS – Policia Militar do Estado do Rio Grande do Sul
POSIC - Política de Segurança da Informação e Comunicações
SENASP - Secretaria Nacional de Segurança Pública
SINESP - Sistema Nacional de Informações de Segurança Pública, Prisional e sobre Drogas
SINESPJC - Sistema Nacional de Estatística de Segurança Pública e Justiça Criminal
SSP/RS - Secretaria de Segurança Pública do Estado do Rio Grande do Sul
TI - Tecnologia da Informação
TIC - Tecnologia da Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO 12
1.1 Problematização 14
1.2 Justificativa 15
1.3 Questão de pesquisa 15
1.4 Objetivos 15
1.4.1 Objetivo Geral 15
1.4.2 Objetivos Específicos 15
2 LEIS E NORMAS DE REGULADORAS RELACIONADAS A TECNOLOGIA DA INFORMAÇÃO 16
2.1 NORMAS INTERNAS DA INSTITUIÇÃO 16
2.1.1 Diretrizes Gerais 16
2.1.2 Notas de Instrução (NI) 16
2.1.3 Notas de Instrução Temáticas 17
2.2 LEGISLAÇÃO APLICADA A TECNOLOGIA DA INFORMAÇÃO 17
2.2.1 Legislação Relacionada à Lei de Acesso à Informação 17
2.2.2 Portaria nº. 119/2015-SSP/RS 18
2.3 DEFINIÇÃO DE DELITOS INFORMÁTICOS 19
2.3.1 Delitos Informáticos Impróprios 20
2.3.2 Delitos Informáticos Próprios 20
2.3.3 Delitos Informáticos Mistos 29
3 PROCEDIMENTOS METODOLÓGICOS 31
3.1 Métodos de Abordagem 31
3.2 Métodos de Interpretação 31
3.3 Métodos de Procedimento 31
3.4 Modelo de Pesquisa 31
3.5 Procedimento de Pesquisa 32
3.6 Técnicas de Pesquisa 32
4 PLANEJAMENTO DE AÇÕES NA AREA DE TI PARA CORPORAÇÃO 33
4.1 A Política de Segurança da Informação e Comunicações (POSIC) 33
4.2 Recomendações para Institucionalização da POSIC 33
4.3 Gerenciamento de serviços de TIC 34
4.4 Orientações Derivadas do Departamento de Segurança da Informação e Comunicações (DSIC) 35
4.5 Fatores para Elaboração de um Plano de Gerenciamento 37
CONSIDERAÇÕES FINAIS 39
REFERÊNCIAS 42

1 INTRODUÇÃO

O tema do presente trabalho tem como fulcro auxiliar na criação de uma política de uso da tecnologia da informação e da comunicação dentro da Instituição. Para que não seja ferido normas do ordenamento jurídico brasileiro. Esta regulamentação visa melhorar o desempenho dos processos rotineiros e gerenciais da organização, apresentado maior velocidade na obtenção de informações de qualidade para a tomada de decisão.

Diante das garantias previstas na Constituição Federal, como o princípio da legalidade, quando alguém só poderá ser punido, se anteriormente ao fato praticado existir lei que o considere como crime, ainda que o fato seja imoral, antissocial ou danoso não existirá a possibilidade de punir o autor.

Cabe ressaltar que a Constituição Federal estabelece que:

> "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> XXXIX – Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". ...

A observância do princípio da legalidade leva ao questionamento da tipicidade do crime, onde um fato somente será típico se a lei descrever, previamente e todos os elementos da conduta humana tida como ilícita.

Diante dos institutos da legalidade e tipicidade, buscou-se impor limites ao poder punitivo do Estado, onde um indivíduo somente pratica uma conduta prevista como crime, se a conduta assim se encontrar descrita dentro do nosso ordenamento vigente.

Segundo PEDROSO (2008), penalista brasileiro, explica que:

> "Não basta, consequentemente, que o fato concreto, na sua aparência, denote estar definido na lei penal como crime. Há mister corresponda à definição legal. Nessa conjectura, imprescindível é que sejam postas em confronto e cotejo as características abstratas enunciativas do crime com as características ocorrentes no plano concreto, comparando-se uma a uma. Se o episódio a todas contiver, reproduzindo uma exatidão e fidelidade a sua imagem abstrata, alcançará a adequação típica. Isso porque ocorrerá a subsunção do fato ao tipo, ou seja, o seu encarte ou enquadramento à definição legal. Por via de consequência, realizada estará a tipicidade, primeiro elemento da composição jurídica do crime. " (PEDROSO, 2008, p.45).

Ante o exposto, para a sua caracterização do crime necessita de alguns fatores indispensáveis, como a tipificação expressa como crime por lei; uma conduta comissiva ou omissiva e sendo expressa como tal, seja também vigente para surtir efeitos perante todos.

O princípio da tipicidade tem o objetivo de classificar as condutas humanas em normas penais proibitivas, ou em normas negativas, incriminando todos os fatos que possam estar desviados de uma conduta aceita socialmente. Assim, e somente através dela, é que se pode verificar uma transgressão à norma penal, e devido a tal agressão é que poderá cominar uma aplicação de uma pena.

Nos crimes informáticos, devido a uma falta ou ausência de normas legais que o tipifiquem, socorrem-se à analogia para tentar ajustar as condutas atípicas à norma penal e à realidade social, mesmo sendo proibitiva a aplicação desta dentro da esfera penal.

Vale observar que a analogia jurídica aplicada na norma penal incriminadora não pode ser considerada válida, nos casos prejudiciais ao réu, como bem explica Fernando Capez:

> "A aplicação da analogia em norma penal incriminadora fere o princípio da reserva legal, uma vez que um fato definido em lei como crime, estaria sendo considerado como tal. Imagine considerar típico o furto de uso (subtração de coisa alheia móvel para o uso), por força da aplicação da analogia do artigo 155 do Código Penal (subtrair coisa alheia móvel com ânimo de assenhoramento definitivo). Neste caso, um fato não considerado criminoso pela lei passaria a sê-lo, em evidente afronta ao princípio constitucional do art. 5º, XXXIX (reserva legal)." (CAPEZ, 2010, p.59).

Com a evolução do tema, obrigou-se a elaboração de uma lei com alcance para regular exclusivamente crimes digitais, os casos existentes eram decididos com adaptações de artigos que já constavam no Código Penal brasileiro. Com a nova legislação, que criminaliza a invasão de dispositivos informáticos, subsidiou-se a Justiça com instrumentos próprios para esse tipo de situação, tornando-se assim mais ágil.

Importante referir que para definição do bem jurídico a ser alcançado deve ser respeitado os elementos que definem o conceito de crime. São eles a conduta, o resultado, nexo causal e a tipicidade. No transcorrer do trabalho figurarão algumas definições aplicadas ao tema, Através da Lei 12.737, também conhecida como Lei Carolina Dieckmann, que tipifica crimes cometidos na internet, entrou em vigor em 2 de abril de 2013. A Lei ganhou este apelido de Carolina Dieckmann após roubo de 36 fotos íntimas da atriz, que estavam no computador dela e acabaram veiculadas na internet. A polícia identificou quatro suspeitos de terem roubado as fotos do computador da atriz. Como ainda não havia definição no Código Penal para este tipo de crime, os acusados foram indiciados por furto, extorsão qualificada e difamação.

Considerando que a tecnologia da informação e da comunicação está cada vez mais presente no dia-a-dia das pessoas de modo geral, quem obtém a informação, possui a capacidade realizar uma ação de forma rápida, permite que se resolva determinado problema e de forma preventiva procurar sua solução, pode também ser utilizada para adquirir conhecimento e consequentemente transformar não só vidas de forma individual, mas a realidade de uma sociedade. Podemos dizer que o acesso e uso da Informação dita as regras em todas as áreas, assim, como ocorreu na Revolução Industrial, onde prevaleceram as regras das máquinas na capacidade de produzir bens materiais. Hoje, podemos considerar o maior bem é a informação, na forma do conhecimento, e não basta somente tê-la em mãos, faz-se necessário planejar e executar de forma organizada.

Trazendo para o nível Institucional, para que ela possa ser utilizada para proporcionar resultados produtivos. O progresso da informática, através da TIC's em todas as áreas proporciona maior acessibilidade às tecnologias acesso à rede mundial em qualquer lugar (tablet, smartphones, notebooks etc.).

Diante dessas colocações iniciais, e seus desdobramento, o presente estudo irá percorrer diversos fatores relevantes no tocante a previsão legal e os princípios norteadores correlacionados a realidade de outras Instituições.

1.1 Problematização

Diagnosticar os possíveis problemas enfrentados diante da inexistência de normas regulatórias atualizadas na Instituição, que possibilitem uma segurança jurídica na realização das tarefas.

A importância de planejar da estruturação em normas regulatórias para estabelecimento de um padrão relativo ao gerenciamento do Sistema de acesso as Informações e as Comunicações na Brigada Militar, desde a aquisição de material até a utilização de serviços na área de TIC.

Evidenciar os impactos resultantes do uso indevido dos meios disponíveis, evitando a interrupção de serviços que possam afetar a atividade policial militar em sua principal missão que é a manutenção da ordem pública.

1.2 Justificativa

O tema do presente trabalho pretende criar uma dinâmica que propicie aos usuários a criação de Normas de Instrução que regulem as atividades desenvolvidas na área de TIC na Instituição como por exemplo a utilização da rede e-mail, rede de dados, utilização de equipamentos de informática, e principalmente a utilização de dados/informações.

1.3 Questão de pesquisa

Como viabilizar a aplicação das normas existentes na legislação Brasileira que ainda não são aplicadas na Instituição?

Diagnosticar os possíveis problemas enfrentados diante da inexistência um planejamento diante da escassez de normas regulatórias atualizadas na Instituição, que possibilitem uma segurança jurídica na realização das tarefas, bem como o bom andamento das atividades do dia-a-dia.

1.4 Objetivos

1.4.1 Objetivo Geral

Identificar as lacunas existentes entre a legislação existente e a normatização existente na Instituição utilizando o planejamento estratégico visando estruturar uma linha de ações para proporcionar uma maior segurança e uma funcionalidade objetiva nas atividades pertinentes a área.

1.4.2 Objetivos Específicos

- Ações para criar/aprimorar, diante da legislação vigente as NI’s reguladoras aplicáveis a Instituição.

- Criar uma proposta para implementação das oportunidades de melhoria identificadas.

- Analisar a transposição de limites jurisdicionais na relação das sanções disciplinares através de procedimento administrativos com a previsão dos delitos.

2 LEIS E NORMAS DE REGULADORAS RELACIONADAS A TECNOLOGIA DA INFORMAÇÃO

2.1 NORMAS INTERNAS DA INSTITUIÇÃO

2.1.1 Diretrizes Gerais

A finalidade da estruturação em normas regulatórias deve ser estabelecer um padrão relativo ao gerenciamento do Sistema de Comunicações na Brigada Militar, no desde a aquisição, recebimento, distribuição, recolhimento, desativação, identificação, manutenção de material e serviços na área de TIC. Segue o princípio da eficácia do Sistema de Comunicações é garantida pela presteza, clareza, informalidade e uso correto da informação.

2.1.2 Notas de Instrução (NI)

Conforme previsto nota de instrução Administrativa nº 001, de 30 de julho de 2004, a NI tem como objetivo uniformizar conceitos e fixar doutrina policial militar; padronizar a execução de atividades peculiares; unificar a interpretação da legislação em vigor, aplicada à Brigada Militar; definir processos corporativos. A elaboração das Notas de Instrução cabe aos Órgãos integrantes do Comando-Geral e aos que compõem o nível departamental de apoio (Departamentos).

O órgão normatizador elabora a NI e encaminha em base virtual na forma de Minuta ao Estado Maior da Brigada Militar/PM3, que a examina quanto a técnica redacional e conteúdo, submetendo-a, se necessário, a demais órgãos a que esteja afeta a matéria; A proposição de norma sob a forma de NI obedecerá os princípios da Necessidade e Oportunidade, da Objetividade e Clareza e da Concisão, devendo primar pelo esgotamento da matéria regulada; Sempre deverão ser obedecidos, na confecção das Notas de Instrução itens: como *finalidade*, a ementa da NI, sendo de extrema relevância a clareza e concisão em sua redação; *base legal*, indicará a legislação que suporta a normatização disposta para a matéria; *execução*, consistirá na parte dispositiva, em que a norma será explicitada e *prescrições diversas* , apresentará aspectos relevantes ao entendimento da parte dispositiva, em compreensão e extensão.

Na hipótese de alteração da matéria normatizada, a identificação da NI será mantida, com o acréscimo, após o número original, de um ponto, seguido de numeração sequencial.

No caso de revogação total da NI, sua numeração não será reutilizada para outra matéria, assinalando-se, nos instrumentos de controle, a expressão “REVOGADA”, sob numeração acrescida numeração sequencial após o número originário.

2.1.3 Notas de Instrução Temáticas

Ao observarmos especificamente as Notas de Instruções Temáticas vigentes, relacionadas a área de TIC, cabe destacar a nota de instrução tecnológica nº 001.1, de 25 de novembro de 2014, que prevê os procedimentos na Brigada Militar quanto à administração, responsabilidades e utilização do serviço de correio eletrônico adotado como canal oficial de comunicação na Corporação.

O serviço de correio eletrônico utilizado pela Brigada Militar, ainda que fornecido por terceiros, possui caráter institucional, e as contas são direcionadas para atenderem necessidades de comunicação entre seus órgãos, para assuntos oficiais ou funcionais, admitindo o tráfego de mensagens pessoais que contribuam para a integração de seus servidores, dentro dos limites da ética e das demais normas que regem a Corporação, e que não estejam previstos nesta Nota de Instrução como de conteúdo restringido

Existem outras Notas de Instrução regulando o uso das telecomunicações através de rádio e telefonia, tratando de forma muito superficial temas como a utilização da rede de dados, utilização de equipamentos de informática, e principalmente a utilização de dados/informações.

2.2 LEGISLAÇÃO APLICADA A TECNOLOGIA DA INFORMAÇÃO

2.2.1 Legislação Relacionada à Lei de Acesso à Informação

A Lei Nº 12.527, de 18 de novembro de 2011, dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no§ 2º do art. 216 da Constituição Federal.

Nesta Lei cabe salientar as responsabilidades de agentes públicos, quanto ao acesso as informações, inclusive se militares.

> Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:
> I - recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

> II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
> III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;
> IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;
> V - impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;
> VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e
> VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.
> § 1o Atendido o princípio do contraditório, da ampla defesa e do devido processo legal, as condutas descritas no caput serão consideradas:

2.2.2 Portaria nº. 119/2015-SSP/RS

No âmbito do Estadual, com objetivo de consolidar as normas de gestão, utilização, coordenação e supervisão dos sistemas de informação e dos bancos de dados criminais e administrativos utilizados âmbito da Secretaria de Segurança Pública do Estado do Rio Grande do Sul e das instituições vinculadas: Brigada Militar, Instituto Geral de Perícias, Polícia Civil e Superintendência dos Serviços Penitenciários ou que sejam objeto de compartilhamento por meio de convênio ou instrumento.

Para melhor entendimento cabe salientar algumas definições sobre as normas de utilização dos sistemas de tecnologia da informação nesta portaria:

> "Art. 1º. Para os fins desta portaria, adotam-se as seguintes definições:
> ...
> X - Equipamento de tecnologia da informação: todo e qualquer dispositivo de processamento (estações de trabalho, notebooks, palmtops, etc.) e seus periféricos (impressoras, multifuncionais, copiadoras, scanners, teclado, mouse, dispositivos de áudio e de vídeo, etc.); ...
> ...
> XIV - segurança da informação: proteção da informação de vários tipos de ameaças para garantir a continuidade da atividade de segurança pública, minimizar o risco a atividade, maximizar o retorno sobre os investimentos e as oportunidades de seus processos, preservando a confidencialidade, a integridade e a disponibilidade da informação.

Também conceitua TI e define usuário:

> ...
> XVIII - tecnologia da informação – TI: conjunto de hardware e software que desempenha uma ou mais tarefas de processamento de informações fazendo parte do sistema de informação das organizações, que inclui a coleta, transmissão, armazenar, recuperar, manipular e exibir dados;
> XIX – usuário: todo indivíduo devidamente identificado por um nome ou código (login) e uma senha de uso exclusivo para acesso à infraestrutura de tecnologia da

> informação, sendo considerado usuário ativo aquele que está no pleno exercício de suas funções e inativo aquele que estiver afastado do cargo em razão de licenças, afastamentos cautelares por decisão judicial ou administrativa, além dos aposentados;

Nesta Portaria prevê o responsável pela instituição de Normas e Diretrizes sobre o tema, bem como as consequências para casos que infrinjam o regramento vigente.

> ...
> Art. 46. Cabe ao Comandante-Geral da Brigada Militar, ao Chefe de Polícia Civil, ao Superintendente dos Serviços Penitenciários, ao Diretor-Geral do Instituto-Geral de Perícias e ao Comandante Geral dos Bombeiros adotarem as necessárias providências para que a Instituição sob sua responsabilidade adote os princípios e diretrizes de utilização dos sistemas de TI.
> § 1º. A inobservância destas normas pelo usuário deverá ensejar a instauração de procedimento administrativo e apuração de suas circunstâncias, respondendo o agente civil, penal e administrativamente.
> § 2.º Os chefes dos setores de tecnologia da informação das Instituições Vinculadas e Conveniadas que agirem com dolo ou culpa na inobservância dos preceitos dispostos nesta portaria ficam sujeitos às responsabilidades civil, administrativa e criminal.
> ...

2.3 DEFINIÇÃO DE DELITOS INFORMÁTICOS

Para melhor entendimento quando se trata de delito ou crime, cabe um abreve descrição de conceitos dos elementos necessários para configuração do fato típico, que é o primeiro substrato do crime, ou seja, o primeiro requisito ou elemento do crime. São elementos do fato típico a conduta, o resultado, o nexo causal entre a conduta e o resultado e a tipicidade. Na falta de qualquer destes elementos, o fato passa a ser atípico e, por conseguinte, não há crime.

> Conduta é a ação ou omissão humana, voluntaria e consciente, dolosa ou culposa, dirigida a determinada finalidade. O resultado é a transformação que a conduta criminosa provoca, é a lesão ou ameaça a um bem jurídico penalmente tutelado. Nexo Causal é o vínculo estabelecido entre a conduta do agente e o resultado. E a tipicidade é a ligação entre o fato e o tipo penal, é o enquadramento da conduta praticada à definição típica legal. (CLAUDIO, 2017, p. 01)

Ainda no campo do entendimento, importante salientar a previsão de delito de acesso não autorizado a sistemas computacionais. Em rigor, para que um delito seja considerado informático é necessário que o bem jurídico por ele protegido seja a inviolabilidade de dados.

A pura utilização do computador para a execução de um delito, não caracterizaria o crime informático, se o bem jurídico afetado não seja a informação automatizada. Aos delitos em que o computador foi o instrumento para a execução do crime, mas não houve ofensa ao bem jurídico inviolabilidade dos dados, definem-se os delitos informáticos impróprios e àqueles em que o bem jurídico afetado foi a inviolabilidade dos dados, denomina-se delitos informáticos próprios.

Segundo Viana (2001, p. 37), Os crimes informáticos impróprios, nos quais o computador é mero instrumento de realização do crime, não havendo violação de dados, como nos casos de difamação, calúnia e injúria; crimes informáticos próprios, nos quais o bem jurídico violado são os dados computacionais; crimes informáticos mistos, nos quais há a violação de dados computacionais e de outros bens jurídicos distintos; crimes informáticos mediatos ou indiretos, os quais servem de instrumento para a consumação de outro delito não-informático, como no caso de furto de dinheiro de contas bancárias pelo computador.

Existem várias nomenclaturas que possam dirigir-se a esses delitos (virtuais, informáticos, cibernéticos, de informática, dentre outros), deve-se subdividir os crimes informáticos em dois grandes grupos, ficando o primeiro com os crimes violadores do computador e seus componentes; e o segundo com os crimes violadores de bens jurídicos já protegidos pelo ordenamento há tempos, sendo o computador o instrumento para sua realização.

Os delitos mais complexos em que tanto a norma que visar tutelar o bem jurídico, quanto a proteção da inviolabilidade dos dados, sejam afetados são denominados como delitos fundamentos de direito penal informático Mistos. Nos casos em que um delito informático próprio é praticado como crime-meio para a realização de um crime-fim não informático, este acaba por receber daquele a característica de informático, será o delito informático mediante ou indireto

2.3.1 Delitos Informáticos Impróprios

Delitos informáticos impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico reconhecido na inviolabilidade da informação automatizada (dados). Hipóteses clássicas de crimes informáticos impróprios são os crimes contra a honra - calúnia (art. 138 CP), difamação (art. 139 CP), injúria (art. 140 CP). O envio de um e-mail, por exemplo. Muito conhecido, para seu cometimento não há necessidade que o agente detenha grandes conhecimentos técnicos do uso de computadores.

2.3.2 Delitos Informáticos Próprios

Os delitos informáticos Próprios são aqueles que a inviolabilidade é protegida pela norma penal no acesso informações automatizadas. Além do delito de acesso não autorizado a sistemas computacionais há ainda outras modalidades de crimes como a interferência em dados informatizados é uma modalidade de crime informático próprio abrangida pelo acesso não autorizado a sistemas computacionais. A hipótese procura prevenir a alteração ou destruição de

dados armazenados em sistemas computacionais e sua execução implica necessariamente em um acesso não autorizado.

No ano 2000, a lei 9.983 criou mais dois tipos penais ao Código Penal Brasileiro prevendo a hipótese da interferência em dados informatizados unicamente quando praticada por funcionário público no exercício de suas funções. Em ambas as condutas previstas, não se pune a simples leitura dos dados, mas de crime especial em relação a não se tratar de acesso não autorizado a sistemas computacionais.

> "O princípio da especialidade decorre de antiga e conhecida regra, segundo a qual a lei especial derroga a geral. De acordo com este princípio, um tipo que possui, além dos caracteres do outro, alguns mais - como acontece com os tipos qualificados em relação aos tipos básicos (homicídio criminis causa e homicídio simples, por exemplo) - ou tipos alterados em relação aos tipos não alterados (roubo e furto, por exemplo)."(ZAFFARONI et PIERANGELl, 1999. p. 734)

A interferência em sistemas computacionais é diversa de proteger a integridade dos dados especificamente, mas seu processamento. A inviolabilidade dos dados, assim, é protegida indiretamente, uma vez que perder a capacidade de processar os dados pode equivaler a perder os próprios dados.

Não há nesta hipótese um acesso aos dados armazenados no sistema. A ação do agente é no sentido de impossibilitar o funcionamento do sistema, fazendo com que as máquinas entrem em pane e parem de funcionar. A integridade dos dados permanece inviolada, porém não há mais como acessá-los, pois, o sistema torna-se inoperante.

Até a criação da lei 12.737 de 30 de novembro de 2012 a interferência em sistemas computacionais não estava tipificada no ordenamento jurídico brasileiro. A interceptação ilegal é um crime informático próprio no qual os dados são capturados durante sua transferência de um sistema computacional para outro. O agente não obtém acesso direto ao computador da vítima, limitando-se a interceptar os dados em trânsito entre duas máquinas. Assemelha-se a uma escuta telefônica (grampo), pois os dados são lidos durante sua transmissão.

A conduta estava tipificada no ordenamento jurídico pátrio na Lei n° 9.296 de 24 de julho de 1996, que em seu art. 10° prevê:

> "Art. 10º - "Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de 2 (dois) a 4 (quatro) anos, e multa."

Na legislação brasileira não havia um tipo penal específico visando à repressão dos vírus informáticos, mas é era possível a punição utilizando como referência o crime de dano (art. 163 do CP) quando a conduta destruir, inutilizar ou deteriorar os dados armazenados no sistema computacional.

O crime de dano é uma das matérias mais divergentes dentro do âmbito dos crimes de informática julgados por analogia, aplicando o artigo 163 do Código Penal, para os casos mais corriqueiros da internet que é a destruição ou a inutilização de arquivos de dados, aplicava-se analogamente aos crimes em que vírus destroem ou danificam substancialmente dados de terceiros. O artigo 163 do código penal diz que:

> "Art. 163- Destruir, inutilizar ou deteriorar coisa alheia.
> I Com violência à pessoa e grave ameaça.
> II Com emprego de substancia inflamável ou explosiva, se o fato não constitui crime
> III Contra o patrimônio da União, Estado, Município empresa concessionária de serviços públicos ou sociedade de economia mista.
> IV - Por motivo egoístico ou com prejuízo considerável para a vítima. "

Para Mirabetti (2010) para que seja configurado o crime de dano é necessário que haja pelo menos uma das três condutas descritas no tipo penal que são:

> "Destruir inutilizar ou deteriorar. Destruir é eliminar, desfazer, desmanchar, demolir (quebrar um vidro, matar um animal, derrubar um muro etc). Inutilizar significa tornar inútil, imprestável, inservível a coisa (quebrar peças de uma máquina tirar ponteiros de um relógio etc). Deteriorar, estragar, arruinar, adulterar (mutilar um animal, misturar um liquido no vinho etc) " (MIRABETTI, 2010. p. 240)

Ademais nota-se a impossibilidade do enquadramento da conduta do crime informático no crime de dano, tornando clara a necessidade da criação de um fato típico, para proteger o usuário da internet.

Conhecida como Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos 12.737 de 30 de novembro de 2012, alterando o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, que dispõe sobre a tipificação criminal de delitos informáticos, crimes relacionados ao meio eletrônico, como violar dados de usuários, invadir computadores ou tirar sites do "ar". O projeto que deu origem à lei foi elaborado na época em que fotos íntimas da atriz Carolina Dieckmann foram copiadas de seu computador e espalhadas pela rede mundial de computadores.

Com o objetivo de adequar o direito às mudanças tecnológicas que transformam rotineiramente a sociedade, visando suprir o vácuo legislativo que anteriormente havia sobre o tema, lembrando que o crime constitui fato típico, devendo todas as suas nuances estarem previstas especificamente na norma, sob pena de atipicidade da conduta.

Antes do ano de 2012, a falta de previsão legal específica tornava muito difícil a apuração dos crimes virtuais, uma vez que a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. Nesse sentido, podemos citar, dentre outros, o Código Penal (CP), a Lei de Segurança Nacional (Lei nº 7.170/83), o Estatuto da Criança e do Adolescente (Lei n. 8.069/90) e a Lei dos crimes de software (ou lei antipirataria, Lei n. 9.609/98).

Diante da falta de previsão específica da legislação, era muito difícil a identificação dos sujeitos e a obtenção de provas para a condenação criminal quanto aos crimes virtuais, que exige certeza.

A edição da Lei n. 12.737, introduzindo os arts. 154-A, 154-B, e alterando os arts. 266 e 298, do Código Penal:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. "

Sobre o art. 154-A do Código Penal, cabe ressaltar que ele trouxe para o ordenamento jurídico o crime novo de “Invasão de Dispositivo Informático”, baseia-se na conduta de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. A pena prevista para o crime simples é de detenção de 3 meses a um ano e multa, havendo, entretanto, a previsão das formas qualificada e causas de aumento de pena.

A redação do art. 154-A do CP, tende a proteger o bem jurídico tutelado representado pela liberdade individual, a privacidade e a intimidade das pessoas como de modo geral. É um crime comum e o sujeito ativo do crime cibernético pode ser qualquer pessoa (física ou jurídica, de direito público ou de direito privado) e sujeito passivo, pode ser qualquer pessoa passível de sofrer dano moral ou material decorrente da violação do seu sistema de informática. Crime de ação múltipla, apresentando os núcleos “instalar” e “invadir”, podendo o agente praticar ambas as condutas e responder por crime único no mesmo contexto.

Quanto à culpabilidade, a conduta criminosa do crime cibernético caracteriza-se somente pelo dolo, não havendo a previsão legal da conduta na forma culposa. O crime do caput do art. 154-A se consuma com a mera invasão ou instalação de vulnerabilidade, não sendo importante para a consumação a obtenção ou não da vantagem ilícita pelo agente. Na forma qualificada (art. 154, § 3º, do CP), referida abaixo, o crime é material, pois exige para a consumação a obtenção efetiva de conteúdo ou o controle remoto não autorizado do dispositivo.

O art. 154-A, § 1º, do CP, prevê a forma equiparada do crime cibernético, incriminando com a mesma pena do “caput” a conduta de quem “produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput”, sendo esse, também, um crime de ação múltipla que exige dolo específico, tal qual o caput do art. 154-A do CP.

O art. 154-A, § 2º, do CP presumi causa de aumento de pena de um sexto a um terço, no caso da ocorrência de prejuízo de caráter econômico/financeiro para a vítima, sendo tal causa de aumento aplicável somente para a forma simples do delito, e não para a forma qualificada, prevista no parágrafo seguinte, em razão da topografia do dispositivo em comento.

O art. 154-A, § 3º, do CP cita pena e regime prisional diferenciado (seis meses a dois anos de reclusão e multa) para as seguintes hipóteses: 1) quando a invasão possibilitar a obtenção de conteúdo de comunicações eletrônicas privadas; 2) quando possibilitar a obtenção do conteúdo de segredos comerciais ou industriais; 3) quando possibilitar a obtenção do conteúdo de informações sigilosas, assim definidas em lei; e 4) quando possibilitar o controle remoto não autorizado do dispositivo invadido. Ressalte-se que as figuras qualificadas acima descritas configuram crime subsidiário, de subsidiariedade expressa, pois que em seu preceito secundário prevê a norma que ela somente será aplicada "se a conduta não constitui crime mais grave".

Por sua vez, os parágrafos 4º e 5º, I a IV, do CP, ocorrem nas causas de aumento de pena, aplicáveis somente para a forma qualificada do delito (§ 3º, do art. 154-A, do CP).

O artigo Art. 154-B destaca o procedimento previsto na ação penal:

> "Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. "

Neste sentido, como se refere a crime condicionado à representação da vítima, muitos casos serão omitidos por falta de exercício do direito subjetivo, se o agente passivo for a União, Estados, DF ou Municípios ou contra empresas concessionárias de serviços públicos, a ação é incondicionada.

Art. 3o Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

> "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
> Art. 266. .....
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. "
> "Falsificação de documento particular
> Art. 298. .....
> Falsificação de cartão
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. "

O artigo 266 tipifica o crime de perturbação ou interrupção de serviços ligados à comunicação, estabelecendo a pena de 1 (um) a 3 (anos), e multa, para quem cometer o crime. Ao incluir os parágrafos, o ordenamento amplia o alcance da norma para os serviços telemáticos

ou de utilidade pública, incluindo, assim, os ilícitos cometidos não só contra o interesse público, mas, também, contra dados informáticos, norte principal da inovação legislativa analisada.

O parágrafo incluído no artigo 298, que tipifica o crime de falsificação de documento particular, estende os efeitos da norma aos cartões de crédito e de débito, os quais receberam do legislador a qualidade de documento particular devidamente reconhecido, e protegido, pelo ordenamento.

A figura a seguir ilustra um mapa explicativo logo após a aprovação da Lei de Crimes que tipificam as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares:

Figura 1

Fonte: Revista IstoÉ – Edição2475.2013

A análise do posicionamento jurisprudencial acerca do tema é importante na compreensão de determinado assunto jurídico. No caso dos crimes informáticos, esta tarefa se torna um pouco difícil, pois, como se observou no tópico anterior, a legislação específica foi aprovada

no final de 2012, havendo poucos julgados dedicados à legislação. No entanto, ao realizar a pesquisa, verificou-se a existência de julgados interessantes que merecem destaque nesta obra.

A Lei n.º 12.735 de 30 novembro de 2012, aparece como suporte para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu artigo 4º a determinação de que os órgãos da polícia judiciária devem estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado, tudo de acordo como determinar o regulamento específico, conforme segue:

> "Art. 1º - Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. ...
> ...
> Art. 4º - Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. "

Com esta determinação legal, todos os setores da polícia judiciária brasileira deverão organizar setores especializados nos crimes cometidos na esfera virtual, criando no sistema jurídico brasileiro o suporte necessário para a edição de legislações dedicadas ao assunto

Exemplo de julgados sobre o tema antes e após vigorar a lei que trata sobre crimes informáticos:

> "Ementa - CRIME CIBERNÉTICO - FUNCIONÁRIO PÚBLICO - DELITO SEM COMPLEXIDADE - ESSÊNCIA DOS CRIMES DE ALTERAÇÃO DE SISTEMA INFORMATIZADO - CIRCUNSTÂNCIAS JUDICIAIS FAVORÁVEIS - PENA BASE FIXADA NO MÍNIMO. Funcionário da CEEE que transfere no sistema, débito de fornecimento de energia para pessoa fictícia. Crime cibernético tipificado no art. 313-A do Código Penal. Sendo favoráveis todas as circunstâncias judiciais, a pena base deve situar-se no mínimo. Não se pode entender como complexa, conduta de agente nessas condições, já que a alteração de dados em sistema informatizado é da própria..."

Neste caso o réu promoveu a alteração de dados no sistema informatizado da Companhia de Energia Elétrica, visando beneficiar duas pessoas, amigos seus, um por puro altruísmo e o outro, por ter o remunerado generosamente. Resultou no parcial provimento a apelação, para reduzir a pena base para dois anos de reclusão e declarar extinta a punibilidade pela prescrição, eis que a continuação deve ser desconsiderada nessa hipótese.

> “Ementa: RECURSO EM SENTIDO ESTRITO. CRIMES CONTRA A HONRA. CIVIL EM FACE DE MILITAR DA ATIVA. CRIME DE INFORMÁTICA COMUM. DECLINAÇÃO DA COMPETÊNCIA. JUSTIÇA FEDERAL. NÃO OCORRÊNCIA JUSTIÇA MILITAR DA UNIÃO. COMPETÊNCIA PARA JULGAR OS CRIMES MILITARES DEFINIDOSEM LEI. PREVISÃO CONSTITUCIONAL. A Magna Carta, em seu art. 124, apesar de não especificar a matéria a ser julgada pela Justiça Castrense, prescreve que a ela compete processar e julgar os crimes militares definidos em lei, utilizando o critério ratione legis. Nesses termos, deixou ao alvedrio da legislação infraconstitucional a delimitação de sua jurisdição. A esta especializada Justiça não cabe julgar os integrantes das Forças Armadas, mas sim os agentes que tenham sido denunciados pela prática dos crimes militares definidos na legislação penal castrense, incluindo os civis. Trata-se de crime de informática impróprio ou comum, uma vez que os crimes de calúnia, difamação ou injúria podem ser praticados por qualquer meio, seja ele eletrônico ou não. In casu, a consumação do crime configurou-se no momento em que o Comandante da Base Aérea de Fortaleza e os demais militares tomaram conhecimento do conteúdo da mensagem postada eletronicamente, fato ocorrido no interior do aquartelamento. ” RECURSO PROVIDO. DECISÃO UNÂNIME. STM - RECURSO EM SENTIDO ESTRITO RSE 478920117100010 CE 0000047-89.2011.7.10.0010 (STM)
> Data de publicação: 06/02/2013

Na ação a seguir constata-se a importância de previsão normativa dentro da Instituição para delimitar as atribuições funcionais dos usuários:

> “Ementa: APELAÇÃO. PEDOFILIA. - Das Preliminares. DA NULIDADE DA REALIZAÇÃO DO EXAME - In casu, não há que se falar em nulidade da apreensão das imagens e fotos encontradas no computador do réu, sob o fundamento de que não foi observado o disposto no artigo 159 do Código de Processo Penal. E isso, porque, no caso dos autos, verifica-se que eventual designação de perito para acompanhar a diligência era, apenas, para verificar a necessidade de quais materiais deveriam ser apreendidos e, não para a confecção de laudo, sendo certo que sequer seria imprescindível tal agir, ou seja, não há determinação legal para que o cumprimento de mandado de busca e apreensão seja acompanhado por perito. Ademais, como bem observado pelo Magistrado de piso, nos dias de hoje qualquer pessoa com médio entendimento em informática consegue extrair arquivos de um computador, mormente um policial lotado numa unidade especializada em crimes de informática sendo que, a apreciação sobre fotografias ou vídeos apresentando crianças e adolescentes nus ou em situação pornográfica tampouco é matéria difícil de distinguir para um cidadão mediano, e a nomeação do policial mencionado como perito "ad hoc" pela autoridade policial é perfeitamente regular. Outrossim, diante dos diversos arquivos encontrados no qual possuem a imagem do acusado, dúvidas não restam de que o computador periciado, realmente, pertencia a ele. O fato dos computadores não terem sido, devidamente, lacrados, em nada desnatura a obtenção das provas telemáticas, uma vez que elas seriam obtidas independentemente do lacre anterior, pois de acordo com as explicações dos peritos, o procedimento realizado por eles atinge não apenas os arquivos diretamente acessíveis, mas também aqueles previamente apagados que possam ser recuperados. Em relação às demais irregularidades aventadas pela defesa (ausência de 02 testemunhas na lavratura do auto de apreensão; descrição minuciosa dos bens apreendidos), tratam-se de meras irregularidades formais...” TJ-RJ - APELAÇÃO APL 00794471220128190002 RJ 0079447-12.2012.8.19.0002 (TJ-RJ)
> Data de publicação: 03/12/2014

2.3.3 Delitos Informáticos Mistos

Definidos como delitos derivados do acesso não autorizado a sistemas computacionais que ganharam status de delitos sui generis dada à importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos.

Trata-se do acesso não autorizado a sistemas computacionais do sistema eleitoral que surgiu como tipo penal no ordenamento jurídico nacional com a Lei 9.100/95 assim o tipificou:

> "Art. 67, VII - "Obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos."

Podemos citar o exemplo de um envio de e-mail é um acesso remoto de escrita no qual o remetente grava o conteúdo do e-mail no computador do destinatário. A permissão e autorização do destinatário é somente de escrita e é presumida no momento em que alguém de qualquer forma disponibiliza seu endereço eletrônico.

Na Internet a prática é bastante comum o envio de e-mails publicitários para pessoas que nunca ofereceram seus endereços eletrônicos para este fim. Os remetentes destes e-mails indesejados têm permissão de escrita no computador da vítima, mesmo que esta não tenha autorizado o envio de tais mensagens.

Existe um comércio catálogos de e-mails, endereços eletrônicos são adquiridos pelas mais diversas formas e não é difícil encontrar quem venda. Obviamente que os destinatários destes e-mails não cederam seus endereços para quem enviou tais mensagens publicitárias, não há sequer uma autorização tácita que justifique a escrita destes dados em seu computador, em tese, tipificaria o acesso não autorizado a sistemas computacionais.

Mesmo que profundamente condenável, tal prática, não parece ofender com o grau de gravidade necessária a inviolabilidade dos dados, razão pela qual a conduta será considerada atípica pela aplicação do princípio da insignificância.

Na interpretação das normas penais não podemos omitir que os tipos penais, para serem materialmente válidos, devem fundamentar-se na proteção de um bem jurídico socialmente relevante. O Direito Penal deve ser o remédio extremo que a sociedade admite que tenha consequências colaterais extremamente gravosas não só para o condenado, mas também para ela própria.

O reconhecimento desta subsidiariedade do Direito Penal remete ao Direito Romano no qual já se afirmava a necessidade de haver uma proporção entre o delito praticado e a pena aplicada foi ressaltada por BECCARIA no século XVIII;

> "Não somente é interesse de todos que não se cometam delitos, como também que estes sejam mais raros proporcionalmente ao mal que causam à sociedade. Portanto, mais fortes devem ser os obstáculos que afastam os homens dos crimes, quando são contrários ao bem público e na medida dos impulsos que os levam a delinquir. Deve haver, pois, proporção entre os delitos e as penas." (BECCARIA, 1999. p. 37)

3 PROCEDIMENTOS METODOLÓGICOS

O método de abordagem servirá para ordenação e organização dos dados e saberes coletados, consiste em retirar conclusão genérica a partir de fatos particulares analisados através de pesquisa de campo junto aos usuários.

A metodologia de elaboração dessa pesquisa de trabalho de conclusão leva em conta as ideias deste autor, de forma imparcial, sem descuidar do rigor acadêmico e científico, como forma de evitar que o mesmo se torne uma produção dogmática e desprovida de rigor técnico.

3.1 Métodos de Abordagem

O método de abordagem utilizado na presente pesquisa, e que servirá para ordenação e organização dos dados e saberes coletados, é o método indutivo, ou seja, o raciocínio parte de uma proposição concreta para construir a proposição discursiva abstrata.

Tal método consiste em retirar conclusão genérica a partir de fatos particulares, em processo inverso ao método dedutivo.

3.2 Métodos de Interpretação

O método de interpretação a ser utilizado está focado na análise dos fenômenos encontrados na atividade fim, compreendendo a legislação e a análise doutrinária desses fenômenos. Ainda será observada a influência de tais fatores na instituição, sempre tendo como balizador o tema da pesquisa efetuada.

3.3 Métodos de Procedimento

O método de procedimento escolhido para dar prosseguimento ao trabalho é o método comparativo, no qual, partindo da pesquisa efetuada, serão comparados os institutos e procedimentos utilizados na aplicabilidade do tema. Então, espera-se que seja possível verificar as semelhanças e diferenças entre estes, de forma a ampliar o conhecimento na realidade atual da Instituição e seus efeitos.

3.4 Modelo de Pesquisa

O modelo de pesquisa a ser utilizado será a revisão bibliográfica e documental pertinente ao objeto de estudo, bem como a pesquisa na legislação vigente, normas de instrução referentes ao tema.

3.5 Procedimento de Pesquisa

Será utilizado o procedimento monográfico, no qual se partirá de acontecimentos particular para, a partir daí, alcançar generalizações.

3.6 Técnicas de Pesquisa

A pesquisa é de cunho teórico e, para que seja efetivada, serão utilizadas bibliografias de doutrinadores nacionais, artigos e textos de autores nacionais, consultas a sites da internet previamente observados e com conferência da veracidade de suas informações, para fins de complementação da monografia.

A pesquisa documental se dará em arquivos de ordem pública, principalmente no que tange à questão normativas das Instituições. Já a pesquisa bibliográfica terá por centro a produção doutrinária nacional, a partir de um primeiro filtro de obras a serem consultadas, sempre tendo em vista a qualidade da fonte de consulta.

4 PLANEJAMENTO DE AÇÕES NA AREA DE TI PARA CORPORAÇÃO

4.1 A Política de Segurança da Informação e Comunicações (POSIC)

Observando o guia de Orientações ao Gestor em Segurança da Informação e Comunicações (SIC), aprovado pelo Gabinete de Segurança Institucional, órgão essencial da Presidência da República, com o intuito de coordenar a atividade de Segurança da Informação e Comunicações, mantendo o compromisso do Estado de promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Direcionada ao âmbito da Administração Pública Federal (APF), mas com conceitos perfeitamente utilizáveis no âmbito da Policias Militares. A POSIC é um documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SIC. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação de uma organização. Assim, deve ser entendida como uma declaração formal dos órgãos e entidades da APF acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os agentes públicos e colaboradores. Na elaboração de uma POSIC, a organização deve se preocupar não somente com aspectos técnicos, mas, também, considerar questões comportamentais e práticas do cotidiano. Afinal, as organizações enfrentam problemas de segurança que não estão necessariamente relacionados somente aos aspectos tecnológicos. Neste contexto, uma POSIC declara o comprometimento da alta direção organizacional com a finalidade de prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão da Segurança da Informação Comunicações (GSIC). Além disso, o estabelecimento de suas diretrizes objetiva viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação no âmbito da APF, direta e indireta.

4.2 Recomendações para Institucionalização da POSIC

No Quadro 1 algumas recomendações que devem ser observadas pelo Gestor de SIC durante o desenvolvimento, implantação e manutenção de uma POSIC.

Recomendações ao Gestor de SIC
1. Realizar planejamento, pautado nas características do órgão ou entidade da APF. Considerando o contexto da organização, mapear e avaliar o que deve ser protegido.
2. Promover a aprovação da POSIC pela alta direção. O patrocínio da alta direção é fundamental para o sucesso na adoção da POSIC.
3. Efetuar análise dos ativos de informação que devem ser protegidos. Analisar o que efetivamente deve ser protegido. Caso a organização já possua políticas e programas de segurança, avaliar deficiências e fatores de risco, visando seu refinamento.
4. Elaborar normas estabelecendo regras e proibições. Devem ser elaboradas normas referentes ao uso dos ativos de informação, tais como: utilização da internet, uso de dispositivos móveis, gerenciamento de acessos físicos e lógicos, utilização do e-mail, entre outros.
5. Obter aprovação e apoio institucional. No tocante à legislação vigente (leis trabalhistas, por exemplo) e à cultura organizacional, as normas e procedimentos relacionados à POSIC devem ser lidos e aprovados pelos departamentos Jurídico e de Recursos Humanos, respectivamente. 23 Recomendações ao Gestor de SIC Além disso, a POSIC deve ter o apoio e patrocínio da alta administração.
6. Investir na educação e capacitação. A POSIC deve ser de conhecimento de todos na organização, além de estar sempre disponível. Para isso, é fundamental iniciativas relacionadas à educação e capacitação dos envolvidos.
7. Fazer avaliação periodicamente. A fim de que não fique ultrapassada ou desatualizada, a POSIC, bem como os instrumentos normativos gerados a partir dela, devem ser revistos de acordo com a periodicidade estabelecida ou tempestivamente, quando se fizer necessário.

Figura 2 - Recomendações ao Gestor de SIC

Fonte: Guia básico de orientações ao gestor em segurança da informação e comunicações

4.3 Gerenciamento de serviços de TIC

A Polícia Militar do Estado de São Paulo optou pela implantação de processos de gerenciamento serviços de TIC baseado no ITIL. Segundo Capitão Aercio Dornelas Santos - A partir de meados de 2005. A opção para a implementação de gerenciamento de serviços de TIC originou-se da política do governo do estado de São Paulo para a área de segurança pública ao iniciar ações para o combate ao crime organizado, para o aumento da sensação de segurança e

para integrar, racionalizar e otimizar as atividades policiais, disponibilizando ferramentas de inteligência para melhorar a gestão dos serviços de segurança pública no Estado. A Polícia Militar do Estado de São Paulo (PMESP) tem entre seus objetivos organizacionais a modernização do aparelho policial e a expansão de sistemas inteligentes, estando a implantação de projetos focados na inovação e em suporte tecnológicos alinhados a esses objetivos organizacionais e de governo. Todas essas ações articuladas estão centradas na aplicação intensiva da tecnologia como instrumento para a transformação dos organismos policiais do estado, aumentando a eficácia e a eficiência das operações e intervenções preventivas, reativas e investigativas. Ao mesmo tempo em que fizeram expandir a disponibilidade de recursos tecnológicos - principalmente os projetos de implantação e expansão de radiocomunicação digital (sistema que tem como prioridade a segurança das comunicações e a integração das comunicações e operações de todos os organismos policiais do estado) - essas ações elevaram ainda mais o grau de dependência das polícias militar, civil e técnico-científica da base tecnológica instalada. Pela arquitetura e configuração implantada, coube à Polícia Militar a responsabilidade pelo gerenciamento e pela manutenção de toda a sua infraestrutura tecnológica. A área de Tecnologia da Informação e Comunicação (TIC) tornou-se, então, um fator crítico de sucesso para a organização. E passou a ter os seguintes desafios: gerar valor para os projetos de TIC; melhorar os custos e diminuir os riscos; administrar o crescimento da complexidade dos ambientes de TIC; lidar com o aumento da pressão para alavancar a tecnologia nas estratégias de negócio; adequar-se em conformidade com as normas regulatórias; e manter a segurança sobre as informações.

4.4 Orientações Derivadas do Departamento de Segurança da Informação e Comunicações (DSIC)

O trabalho desenvolvido pelo Grupo de Trabalho (GT) – “Elaboração de Guia de Orientações ao Gestor de SIC”, instituído no âmbito do Comitê Gestor da Segurança da Informação (CGSI), por meio da Portaria Nº 26 do Conselho de Defesa Nacional (CDN), de 15 de julho de 2014. Na qual reúne métodos e instrumentos, visando orientar os gestores, com importantes aspectos inerentes à relevância do tema nos dias atuais. O Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações foi elaborado com o propósito de oferecer ao leitor orientações e dicas referentes à implementação das ações de segurança da informação nas organizações públicas federais, mas podem ser adotadas pelos demais Órgãos Públicos.

As políticas de Segurança da Informação específicas da Instituição devem ser de fácil leitura e entendimento, podem seguir a estruturação em níveis estratégico, tático e operacional conforme sugerido na Figura 1.

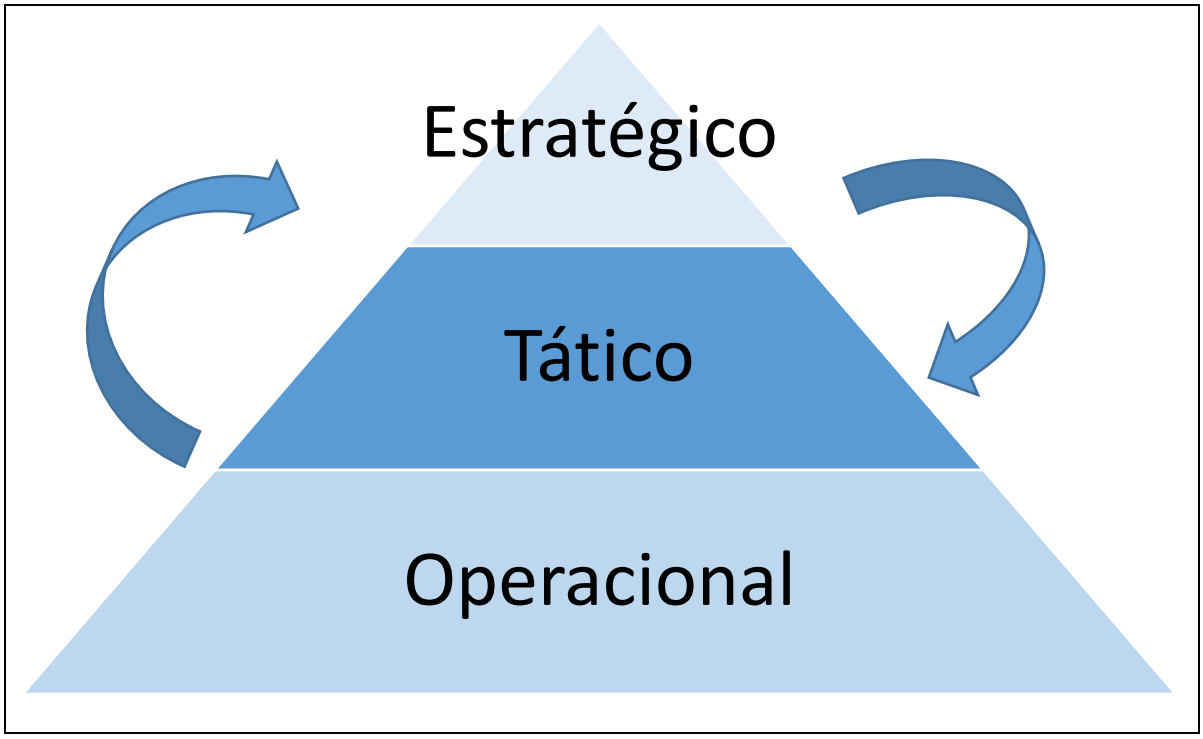

Figura 3: Políticas (Estratégico), Normas (Tático) e Procedimentos (Operacional)

Fonte: Guia básico de orientações ao gestor em segurança da informação e comunicações

Ainda observando o Guia Básico de Orientações ao Gestor em Segurança da Informação e Comunicações publicado em 2015 pelo Governo Federal, recomenda-se a normatização dos respectivos assuntos, envolvendo as áreas de tecnologia, pessoas, ambiente e processos. Além disso, sugere-se que temas ainda não normatizados no governo federal, mas já amparados por outras normas, também sejam analisados a luz das necessidades específicas de cada órgão, vale citar alguns destes temas:

1) Planejamento e Gestão de SIC;

2) Tratamento da Informação;

3) Formação de Equipes de Tratamento de Incidentes de Segurança em Redes Computacionais;

4) Gerenciamento de Incidentes de Segurança em Redes Computacionais;

5) Inventário e mapeamento de ativos de informação;

6) Gestão de Riscos nos aspectos de SIC;

7) Gestão de mudanças nos aspectos relativos à SIC;

8) Gestão de Continuidade de Negócios nos aspectos de SIC;

9) Avaliação e Conformidade de SIC;

10) Controles de Acesso relativos à SIC;

11) Uso seguro de Dispositivos móveis;

12) Uso seguro de Computação em nuvem;

13) Uso seguro de Redes Sociais;

14) Desenvolvimento e obtenção de software seguro;

15) Atuação e adequações para profissionais da área de SIC;

16) Atividades de ensino em SIC;

17) SIC em Sistemas Estruturantes;

18) Uso de recursos criptográficos;

19) Registro de eventos, coleta e preservação de evidências de incidentes de segurança;

20) Uso seguro de e-mail;

21) Backup; e

22) Uso seguro da Internet.

4.5 Fatores para Elaboração de um Plano de Gerenciamento

Diante da resistência natural das mudanças, principalmente as culturais, muito presente dentro de uma Instituição Militar. A elevação do foco na tecnologia para o foco no usuário; a avaliação da TIC sob a perspectiva da prestação dos serviços.

Atividades a serem realizadas devem buscar reduzir os impactos resultantes de um uso indevido dos meios disponíveis, evitando a interrupção de serviços que possam afetar o desempenho da atividade fim, ou seja, interfira no policiamento ostensivo vindo a prejudicar, por exemplo a suspensão do uso de um serviço que traria mobilidade para o policial que está na rua antendendo ao público.

Assim o plano de ação deve ser claramente definido e documentado, para ser usado quando ocorrer um incidente que atinja pessoas, recursos, serviços e outras ações ligadas a execução do serviço de ponta.

Alguns passos para desenvolver a estrutura das normas a serem aplicadas:

(A) Revisar conceitos e definições.

(B) Definir forma de coleta de informações.

(C) Relacionar áreas inseridas na abrangência do trabalho.

(D) Reunir com patrocinador do projeto.

(E) Reunir individualmente com as áreas para analisar as informações coletadas.

O treinamento minimiza as dificuldades para o desenvolvimento da estrutura por parte de quem gerencia. A fase de percepção de foco em serviços e processos, da expansão dos limites funcionais.

CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo possibilitou uma análise de como a previsão legal das TIC é de grande importância no ambiente dos Órgãos de TIC da Polícia Militar. Além disso, também permitiu uma pesquisa para obter dados mais consistentes sobre as etapas do processo, identificou que o grau de conhecimento em informática dos profissionais, possui importantes implicações práticas, visto que, além de identificar a falta de previsão de obrigações do usuário, através de normas, para utilização da rede de dados, utilização da rede e-mail, até mesmo a utilização indevida de equipamentos de informática da Instituição e principalmente a utilização de dados/informações de uso exclusivo na atividade policial. Vale ressaltar que os resultados foram obtidos com base na análise dos processos disponíveis pela Instituição ao usuário final das TIC na PMERS, podendo este ser divergente no momento da implantação do plano de ação que por ventura venha ser executado. Estudos futuros podem analisar os efeitos dos resultados obtidos após implantação de um plano de ação nortear o uso das informações disponíveis.

Nesse sentido, falhas estratégicas e brechas jurídicas prejudicam o alinhamento entre as Unidades de planejamento e a área executiva. A manutenção da atual infraestrutura de TIC da Polícia Militar não requer um elevado ônus na alocação de recursos de custeio e de investimentos da Corporação, por isso a atenção no gerenciamento e no monitoramento do desempenho é de grande relevância, sob o prisma da Unidade que gerencia as TIC, conclui-se que os processos de Gestão da TIC vigentes na Polícia Militar não apresentam um nível que tenha acompanhado a legislação sobre o tema e talvez seja adequado definir etapas para alcançar as metas e os objetivos estratégicos da Instituição.

Ao ser acionado, o gestor de cada Órgão Estatal que possui a missão de conduzir a política de uso da dos meios disponíveis, não pode se ausentar de tal dever. Como observado até então que há inegavelmente a ausência de previsão normativa específica para conduzir os desdobramentos em âmbito Institucional no que tratam dos crimes informáticos, as decisões nos Tribunais, através de seus juízes vem tentando conte-los através da aplicação de uma solução que achem justa. Tudo isto em função de referida omissão, deixando por consequência a missão de legisladores àqueles que não possuem poder para tal, devido a um caso concreto que a eles foram apresentados.

Visto que não se admite o uso de analogia para prejudicar o réu no Direito Penal, espera-se que a conduta esteja claramente definida no texto da lei, dando por respeitados a

legalidade e tipicidade dos crimes conforme dito anteriormente. Assim, algumas condutas criminosas mediante o uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, devem estar claramente definidas na lei.

Entretanto, isto é o que não podemos notar nos dias atuais, onde a inexistência de uma regulamentação harmônica que trate dos crimes informáticos, e também normas específicas dentro das Instituições sobre o referido tema.

Por isso, existe a necessidade de se elaborar uma política na qual determine previsão legal de procedimentos para as condutas praticadas nos crimes informáticos, inibindo a ocorrência destes delitos, tal ausência de regimento encoraja o surgimento de novos delitos neste meio tecnológico. Seus agentes sempre serão agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena, ou impor uma sanção a uma conduta que o ordenamento penal não considere expressamente como criminosa, mesmo que tal conduta produza prejuízos financeiros ou atente contra a integridade humana, bens resguardados pelo direito penal

Embora atualmente estejamos presenciando o surgimento de novos tipos legais, que dado a suas singularidades, subsidiam os operadores do direito em geral, em todos os ramos legais e não só em relação à matéria penal.

Desta forma, considerando que estamos passando por um processo de mudança e evolução mundial que deve ser acompanhado pelo estudioso da área jurídica, que de maneira alguma poderá ficar alheio aos desafios que a sociedade informatizada impõe, não devemos, portanto, medir esforços para desenvolver respostas coerentes, gerar modelos de conhecimento, métodos de análises inovadores que alcancem fórmulas que permitam um correto e justo desenvolvimento para auxiliar a Justiça Penal.

Alguns integrantes da corporação consideram que as normas específicas institucionais representam apenas perda de tempo e de gastos desnecessários e, portanto, tendem a não colaborarem. Estas pessoas tendem a não utilizar as Notas de Instrução vigentes, podendo dificultar o entendimento do comando da instituição sobre a real necessidade de investimento no tema.

A solução então, passa necessariamente pela criação de normas específicas que venham trazer tipicidade a essas condutas perpetradas pelo uso das novas tecnologias acompanhadas de sansões penais específicas que coíbam a prática dos crimes informáticos que como dito anteriormente, podem causar graves danos aos bens resguardados pelo direito penal.

Por fim, vale ressaltar que a existência este tipo de delito não faz mais parte de nossa imaginação ou de um suposto futuro e sim da realidade atual que assola a todos, portanto, deve ser levada a sério pelas autoridades competentes no sentido de realizar de forma efetiva as mudanças necessárias para tentar acabar como o território sem lei instalado no universo virtual.

.

REFERÊNCIAS

BARBOSA JUNIOR, Sergio Jose. Crimes informáticos: delitos virtuais no direito brasileiro. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 19, n. 4008, 22 jun. 2014. Disponível em: <https://jus.com.br/artigos/29634>. Acesso em: 23 março 2017

BARUFFI, Helder; CIMADON, Aristides. A metodologia científica e a ciência do Direito. 2. Ed. Dourados: Evangraf, 1997.

_____. A sociedade brasileira. São Paulo: Timétis, 1997.

BECCARIA. Dos Delitos e Das Penas, São Paulo: José Bushatsky, 1978

BRASIL. Constituição da República Federativa do Brasil; 1998.

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. Estabelece as Diretrizes da Educação Nacional. Diário Oficial [da República Federativa do Brasil], Brasília, v. 134, nº 248, 23 dez. 1996.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal. Diário Oficial [da República Federativa do Brasil], Brasília, seção 1, nº 01, 18 nov. 2011.

BRASIL. Presidência da República. Casa Militar. Departamento de Segurança da Informação e Comunicações. Guia básico de orientações ao gestor em segurança da informação e comunicações: versão 2.0 /Casa Militar, Departamento de Segurança da Informação e Comunicações; organizadores Danielle Rocha da Costa, José Ney de Oliveira Lima. – Brasília: Presidência da República, 2016.

BRASIL. Tribunal de Justiça-RS. ACR: 70043570068 RS, Relator: Gaspar Marques Batista, Data de Julgamento: 06/10/2011, Quarta Câmara Criminal, Data de Publicação: Diário da Justiça do dia 13/10/2011.

BRASIL. Tribunal de Justiça-RJ. ACR: 70043570068 RS, 0794471220128190002 RJ 0079447-12.2012.8.19.0002 - Data de publicação: 03/12/2014

CAPEZ, Fernando. Curso de Direito Penal, volume 1, parte geral. São Paulo; Saraiva, 2010.

CLAUDIO, Olivia. Crimes Cibernéticos: teoria do crime. *Jusbrasil.* https://oliviaclaudio7.jusbrasil.com.br/artigos/446342507/delitos-informaticos. Acesso em maio 2017.

DE FARIA, Matheus Afonso. O Problema da tipificação dos crimes informáticos. *Âmbito Jurídico.* http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11275. Acesso em maio 2017.

FAULSTICH, Enilde L. de J. Como ler, entender e redigir um texto. 6. Ed. Petrópolis: Vozes, 1996.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos da metodologia científica. 5. ed. São Paulo: Atlas S.A., 2003. 310 p

MEDEIROS, João Bosco. Redação Científica: a prática de fichamentos, resumos, resenhas. 10ª ed. São Paulo: Atlas 2008.

MIRABETTI. Julio Fabrinni, manual do direito penal, volume 2 parte especial, São Paulo. Atlas 27 de 2010.

PEDROSO, Fernando de Almeida. Direito Penal, Parte Geral: Estrutura do Crime. LEVD: São Paulo. 1993.

RELATÓRIO de análise da maturidade dos processos de governança de TIC na Polícia Militar do Estado de São Paulo. São Paulo, 30 jan. 2008

ROCHA, Dinamar Cristina Pereira. Dissertações de mestrado Título: Criação e gestão do conhecimento na área de segurança pública Data da defesa: 17 de abril de 2013. 117 páginas. Fundação Pedro Leopoldo.

Link: http://www.fpl.edu.br/2013/media/pdfs/mestrado/dissertacoes_2013/dissertacao_dinamar_cristina_pereira_rocha_2013.pdf

SÁ, Elizabeth Schneider de et al. Manual de normalização de trabalhos técnicos científicos e culturais. 2. Ed. Petrópolis: Vozes, 1996.

SILVEIRA, Artur Barbosa da. Os crimes cibernéticos e a Lei nº 12.737/2012. Conteúdo Jurídico, Brasília-DF: 22 jan. 2015.
Disponível em: <http://www.conteudojuridico.com.br/?artigos&ver=2.52253&seo=1>.
Acesso em: 23 fevereiro 2017.

VIANA, Túlio Lima. Do acesso não autorizado a sistemas computacionais: fundamentos do direito penal informático. Belo Horizonte: UFMG, 2001. Disponível em: <http://www.bibliotecadigital.ufmg.br>. Acesso em: 24 mar. 2017

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. Manual de direito penal brasileiro: parte geral. 11.ed. São Paulo: Revista dos Tribunais, 2015.