**UNIVERSIDADE DE BRASÍLIA**
**INSTITUTO DE LETRAS**
**DEPARTAMENTO DE LINGUÍSTICA, PORTUGUÊS E LÍNGUAS CLÁSSICAS**
**PROGRAMA DE PÓS-GRADUAÇÃO EM LINGUÍSTICA**

# TERMINOLOGIA E TECNOLOGIA:
## UM ESTUDO DE TERMOS DE CRIMES CIBERNÉTICOS

**NARA FERNANDA JUSTINIANO**

**BRASÍLIA-DF**
**2017**

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

JJ96t

Justiniano, Nara Fernanda
Terminologia e Tecnologia: um estudo de termos de crimes cibernéticos / Nara Fernanda Justiniano; orientador Enilde Faulstich. -- Brasília, 2017.
106 p.

Dissertação (Mestrado - Mestrado em Linguistica) -- Universidade de Brasília, 2017.

1. Terminologia. 2. Crime cibernético. 3. Glossário. 4. Ciberespaço. 5. Internet. I. Faulstich, Enilde, orient. II. Título.

NARA FERNANDA JUSTINIANO

# TERMINOLOGIA E TECNOLOGIA:
# UM ESTUDO DE TERMOS DE CRIMES CIBERNÉTICOS

Dissertação apresentada à Banca Examinadora como parte dos requisitos de exigência para obtenção do grau de MESTRE EM LINGUÍSTICA pelo Programa de Pós-Graduação do Departamento de Linguística, Português e Línguas Clássicas da Universidade de Brasília.
Área de Concentração: Teoria e Análise Linguística.
Linha de Pesquisa: Léxico e Terminologia.

**Orientadora: Prof.ª Dr.ª Enilde Faulstich.**

**BRASÍLIA-DF**
**2017**

**UNIVERSIDADE DE BRASÍLIA**
**INSTITUTO DE LETRAS**
**DEPARTAMENTO DE LINGUÍSTICA, PORTUGUÊS E LÍNGUAS CLÁSSICAS**
**PROGRAMA DE PÓS-GRADUAÇÃO EM LINGUÍSTICA**

BANCA EXAMINADORA

_____
Prof.ª Dr.ª Enilde Faulstich
Presidente – UnB/LIP

_____
Prof.ª Dr.ª Rozana Reigota Naves
Membro efetivo – UnB/LIP

_____
Prof.ª Dr.ª Cleide Lemes da Silva Cruz
Membro efetivo externo – IFB

_____
Prof.ª Dr.ª Michelle Machado de Oliveira Vilarinho
Suplente – UnB/LIP

**BRASÍLIA-DF**
**2017**

Ao mestre dos mestres,
Jesus de Nazaré.

À minha mãe,
Deuselita.

## AGRADECIMENTOS

A YHWH Deus, acima de todas as coisas, na pessoa de seu filho Jesus Cristo, por seu amor, misericórdia e infinita graça; por guiar-me em cada passo e ter me feito chegar até aqui.

À minha família: Deuselita, minha mãe, uma mulher inspiradora, meu grande exemplo de amor, superação, força e fé; Natália, Renata, e Tatyana, minhas irmãs, que sempre acompanharam muito de perto minha trajetória de vida, me sustentando e motivando com seu apoio, amor e carinho.

À minha orientadora Professora Doutora Enilde Leite de Jesus Faulstich, por ter acreditado em meu potencial e investido em mim; pelo apoio, confiança, orientação, zelo no acompanhamento desta dissertação; por seu grande exemplo de excelência e dedicação ao trabalho.

Aos amigos queridos, principalmente ao casal Conceição de Paula Pinheiro da Silva e Mário Antônio Jovita Sá Brito Correia da Silva, meu reconhecimento pela dedicada parceria, rica contribuição espiritual e intelectual; por tamanha generosidade em me acolherem no seio de seu lar; pelas doações e por me incentivarem a prosseguir, me fazendo acreditar, mesmo nos momentos mais difíceis, que eu sou capaz.

A todos os amigos e colegas da pós-graduação, principalmente as queridas Renata Rezende Antunes e Paula Guedes Baron, pelas discussões teóricas, amizade, torcida solidária, companheirismo; e especialmente pelos felizes e necessários momentos de descontração e desanuviação.

Ao Grupo de Repressão a Crimes Cibernéticos da Superintendência Regional da Polícia Federal, na pessoa do senhor Delegado Chefe Stênio Santos Sousa, pela gentil colaboração no desenvolvimento deste trabalho, pela importantíssima ajuda e essencial contribuição.

À Danúzia Maria Queiroz Cruz Gama, pela amizade genuína, pela parceria solidária, pelo exímio trabalho de revisão de texto.

A Gabriel Lobo Vianna da Silveira, pela amizade, pelo companheirismo, pelo ótimo

trabalho em traduções de texto, e principalmente por ajudar a restaurar a fé em mim mesma.

Aos irmãos amados da Igreja Nacional do Senhor Jesus Cristo - INSEJEC, na pessoa da apóstola Valnice Milhomens, pelo amor fraterno, por se importarem tanto comigo, pela compreensão nas ausências, pelo zelo, carinho e cuidado, pelo alento nos momentos de angústia, fazendo-me sentir em casa e em família.

Aos professores do Departamento de Linguística, Português e Línguas Clássicas, que muito contribuíram para minha formação com seus valiosos ensinamentos, em especial à Professora Doutora Rozana Reigota Naves.

Às Professoras Doutoras Cleide Lemes da Silva Cruz e Michelle Machado de Oliveira Vilarinho, por aceitarem o convite de compor minha banca de defesa de dissertação, se disporem a ler e analisar meu trabalho, pela generosidade e disponibilidade em compartilhar conhecimentos.

Ao Centro de Estudos Lexicais e Terminológicos - Centro LexTerm, pelas ótimas condições de estudo, trabalho, pesquisa, e acervo bibliográfico fornecidos.

Aos servidores e funcionários do Departamento de Linguística, Português e Línguas Clássicas pelo apoio administrativo, que contribuem diariamente para o desenvolvimento do saber.

A todos, próximos ou distantes, que contribuíram direta ou indiretamente para que este trabalho fosse alcançado.

*“A glória de Deus está nas coisas encobertas; mas a honra dos reis está em descobri-las. ”*

*(Provérbios 25:2)*

## RESUMO

Este trabalho é um estudo linguístico desenvolvido na linha de pesquisa do Léxico e da Terminologia sobre as unidades terminológicas que compõem os crimes cibernéticos. Se, de um lado, a Internet é uma ferramenta de comunicação, inclusão e informação, por outro lado, pode ser usada como ferramenta para a prática de delitos. A hipótese de pesquisa é que existe um conjunto de delitos praticados em ambiente cibernético e que constituem um léxico específico, para o qual é necessário desenvolver um estudo terminológico próprio. A razão principal para a escolha deste tema foi a importância de se explicitar a problemática encontrada do que são e quais são os crimes de natureza cibernética. O objetivo é desenvolver um glossário que contemple a terminologia empregada em situações de crimes ocorridos em ambiente cibernético. Os objetivos específicos são: 1) identificar termos empregados para designar crimes cibernéticos; 2) verificar as relações entre termos, conceitos e definições; 3) registrar os termos em um glossário de crimes cibernéticos. A metodologia empregada foi a da pesquisa qualitativa, com coleta de dados, de acordo com os seguintes passos: 1) seleção e organização de termos; 2) registro de termos em fichas terminológicas; 3) validação dos termos com consultor; 4) registro dos termos no glossário. A presente pesquisa auxilia a compreender o atual panorama da discussão acerca da web, de sua relação com a linguagem e a conduta humana, considerando o fato de se tratar de uma terminologia recente, datada de cerca de duas décadas apenas e ainda não sistematizada, além da carência de pesquisas e publicações científicas nesta área. Apresentamos os fenômenos linguísticos encontrados após a análise de dados, como variação terminológica e estrangeirismos. Como produto final do resultado a que chegamos, apresentamos, no último capítulo, um glossário de crimes cibernéticos do português do Brasil, composto por 80 verbetes, desenvolvido no Centro Lexterm.



**Palavras-chave:** Terminologia. Crime cibernético. Glossário. Internet. Ciberespaço.

## ABSTRACT

This work is a linguistic study developed in the line of research of the Lexicon and the Terminology on the terminological units that compose the cybernetic crimes. If, on the one hand, the Internet is a tool for communication, inclusion and information, on the other hand, it can be used as a tool for the practice of crime. The research hypothesis is that there is a set of crimes practiced in a cybernetic environment and that they constitute a specific lexicon, for which it is necessary to develop a proper terminological study. The main reason for the choice of this theme was the importance of explaining the problematic found of what they are and what are the crimes of a cybernetic nature. The goal is to develop a glossary that addresses the terminology used in crime situations occurring in a cyber environment. The specific objectives are: 1) to identify terms used to designate cyber crimes; 2) to verify the relations between terms, concepts and definitions; 3) record the terms in a glossary of cyber crimes. The methodology used was qualitative research, with data collection, according to the following steps: 1) selection and organization of terms; 2) registration of terms in terminological records; 3) validation of terms with consultant; 4) registration of terms in the glossary. This research helps to understand the current panorama of the discussion about the web, its relationship with language and human conduct, considering the fact that it is a recent terminology, dating to about two decades only and not yet systematized, besides The lack of research and scientific publications in this area. We present the linguistic phenomena found after data analysis, such as terminological variation and foreignisms. As a final product of the result we have presented, in the last chapter, we present a glossary of cybercrimes in Brazilian Portuguese, composed of 80 entries, developed at the Lexterm Center.



**Keywords**: Terminology. Cyber crime. Glossary. Internet. Cyberspace.

## RÉSUMÉ

Ce travail est une étude linguistique menée dans la ligne de Lexicon et terminologie des unités terminologiques qui constituent des crimes de cyber-recherche. D'une part, l'Internet est un outil de communication, d'inclusion et de l'information, d'autre part, il peut être utilisé comme un outil pour commettre des irrégularités. L'hypothèse de recherche est qu'il ya un certain nombre de crimes commis dans l'environnement cybernétique et constituent un lexique spécifique, pour lequel il est nécessaire de développer une étude terminologique lui-même. La principale raison du choix de ce thème est l'importance d'expliquer les problèmes trouvés quels sont et quels sont la nature des crimes cybernétiques. L'objectif est de développer un glossaire qui comprend la terminologie utilisée dans les situations de crimes dans l'environnement cybernétique. Les objectifs spécifiques sont: 1) identifier les termes utilisés pour désigner la cybercriminalité; 2) de vérifier la relation entre les termes, les concepts et les définitions; 3) enregistrer les termes dans un glossaire de la cybercriminalité. La méthodologie a été la recherche qualitative avec la collecte de données, selon les étapes suivantes: 1) la sélection et l'organisation des termes; 2) les conditions d'inscription dans les registres de terminologie; 3) la validation des termes consultant; 4) l'enregistrement des termes du glossaire. Cette recherche permet de comprendre la situation actuelle de la discussion sur le web, sa relation avec la langue et le comportement humain, compte tenu du fait qu'il est une terminologie récente, datée près de deux décennies seulement et pas encore systématisée, en plus le manque de recherche et de publications scientifiques dans ce domaine. Ici, les phénomènes linguistiques trouvés après l'analyse des données, comme la variation et loanwords terminological. Comme résultat final du produit que nous avons, nous avons présenté dans le dernier chapitre, un glossaire de la cybercriminalité les Portugais du Brésil, composé de 80 entrées, développées dans Lexterm Center.



**Mots-clés**: Terminologie. Cybercriminalité. Glossaire. Internet. Cyberspace.

## RESUMEN

Este trabajo es un estudio lingüístico realizado en la línea de investigación del léxico y la terminología de las unidades terminológicas que comprenden los delitos cibernéticos. Por un lado, la Internet es una herramienta de comunicación, la inclusión y la información, por otra parte, se puede utilizar como una herramienta para cometer irregularidades. La hipótesis de la investigación es que hay una serie de crímenes cometidos en el entorno cibernético y constituyen un léxico específico, para lo cual es necesario desarrollar un estudio terminológico en sí. La razón principal para elegir este tema fue la importancia de explicar los problemas que encontró lo que son y lo que son la naturaleza de los delitos cibernéticos. El objetivo es desarrollar un glosario que incluye la terminología utilizada en situaciones de crímenes en el entorno cibernético. Los objetivos específicos son: 1) la identificación de los términos utilizados para designar a los delitos informáticos; 2) para verificar la relación entre los términos, conceptos y definiciones; 3) registrar los términos en un glosario de los delitos informáticos. La metodología utilizada fue la investigación cualitativa con la recopilación de datos, de acuerdo con los siguientes pasos: 1) la selección y organización de los términos; 2) los términos de inscripción en los registros de terminología; 3) la validación del consultor términos; 4) el registro de los términos en el glosario. Esta investigación ayuda a comprender la situación actual de la discusión en la web, su relación con el lenguaje y el comportamiento humano, teniendo en cuenta el hecho de que es una terminología reciente, de fecha casi dos décadas solamente y no ha sistematizado, además la falta de investigación y publicaciones científicas en esta área. Aquí los fenómenos lingüísticos que se encuentran después del análisis de los datos, como la variación terminológica y préstamos. Como resultado final del producto que tenemos, hemos presentado en el capítulo anterior, un glosario de la ciberdelincuencia el portugués de Brasil, compuesto por 80 entradas, desarrolladas en Lexterm Center.



**Palabras clave**: Terminología. Ciberdelincuencia. Glosario. Internet. Ciberespacio.

## LISTA DE ABREVIATURAS

PL: Projeto de Lei

UT: Unidade Terminológica.

UTC: Unidade Terminológica Complexa.

WWW: Word Wide Web.

## LISTA DE GRÁFICOS

## LISTA DE ILUSTRAÇÕES

## LISTA DE QUADROS

**SUMÁRIO**

# INTRODUÇÃO

O advento da Internet revolucionou o modo como as pessoas vivem e se comunicam. As inovações tecnológicas advindas da Internet afetaram as esferas da vida pública e privada da humanidade. A Internet trouxe consigo benefícios e malefícios. De um lado, é notável sua contribuição para a sociedade, operando como importante fator de comunicação, informação e inclusão. Já por outro lado, pode ser usada como um instrumento que favorece o cometimento de delitos, trazendo novas formas de prática para crimes já conhecidos, e também o surgimento de delitos inéditos que o Poder Judiciário ainda não determina como julgar.

Esta dissertação, inserida no âmbito da linha de pesquisa do Léxico e da Terminologia, é uma proposta de estudo linguístico de itens lexicais selecionados a partir de crimes que ocorrem na Internet sob enfoque sincrônico. O objetivo deste estudo é verificar as relações entre os conceitos e as definições nas unidades terminológicas que compõem a comunicação para designar crimes que ocorrem no meio virtual. O resultado foi a elaboração de um glossário de termos sobre os crimes cibernéticos.

Ao observarmos os itens lexicais que designam especificamente crimes praticados em ambiente virtual, buscamos pesquisas sistemáticas de caráter linguístico que contemplassem a análise dessa natureza de conteúdo. Notamos que há uma lacuna nos estudos lexicais e terminológicos, o que motivou nosso senso de investigação e o desenvolvimento deste estudo.

A hipótese de pesquisa é que existe um conjunto de delitos praticados em ambiente cibernético, que constituem um léxico específico, para o qual é necessário desenvolver um estudo terminológico próprio. Os questionamentos de nossa investigação são: classificar a formação dos termos de crimes cibernéticos e verificar se ocorre variação na designação de crimes cibernéticos. A base teórica para o desenvolvimento desta dissertação são os constructos teóricos formulados por Faulstich (1995, 2001, 2004, e 2014).

Esta dissertação é de natureza qualitativa, para compreender e interpretar determinado levantamento de dados de maneira exploratória. Este estudo foi compreendido do ponto de vista da abordagem funcionalista da linguagem, que procura compreender os termos em seu uso funcional, como estão empregados na interação, e como é usualmente interpretada a linguagem que ocorre em situações de crimes ocorridos em interfaces tecnológicas.

O estudo de palavras e expressões empregadas para designar crimes que ocorrem na Internet possibilita a ampliação do diálogo acadêmico entre áreas que, a priori, aparentariam ser antes não tão afins, como é o caso do Direito, da Tecnologia, da Informática, e da Linguística. A construção de um ciberespaço seguro abrange diversas atividades que se

integram e relacionam pela terminologia, tecnologia, comunicação social, e legislação, levando campos distintos a interagir harmonicamente.

O presente trabalho constitui uma dissertação cuja proposta pode ser útil para profissionais, professores e estudantes interessados no tema abordado. O glossário oferece conhecimentos e informação especializada. A investigação nos possibilitou organizar uma interseção de estudos linguísticos com interfaces tecnológicas, para apresentar um trabalho inédito, original, atual, inovador, e de relevância para o estudo científico da área.

Desse modo, o trabalho apresenta primeiramente Introdução, na qual apresentamos o tema e reflexões iniciais. Após este momento, estruturamos o trabalho em cinco capítulos.

No Capítulo 1, o assunto é crimes cibernéticos e legislação, em que abordamos uma retrospectiva histórica sobre a Internet, o surgimento e as funções, e de que maneira ela constitui o patrimônio virtual. O levantamento de tais informações fez-se necessário para contextualizar o assunto e compreender como se dão, o que são, e quais são os crimes cibernéticos. Além disso, abordamos a legislação vigente no Brasil, a relação entre crimes cibernéticos, o princípio da legalidade e a problemática da ausência de definições a respeito do tema.

No Capítulo 2, descrevemos os procedimentos metodológicos utilizados para a recolha, a seleção e a organização de dados de análise. Os procedimentos possuem caráter qualitativo e descritivo que buscam compreender o estabelecimento do método adequado, as fontes que originaram o corpus analisado, e os procedimentos de análise de dados.

No Capítulo 3, expomos à análise de dados os fenômenos linguísticos encontrados na constituição dos termos, detalhando minuciosamente as unidades terminológicas complexas, as modalidades de variação terminológica encontradas, além de discorrermos sobre o fenômeno do estrangeirismo, presente na terminologia empregada nos crimes cibernéticos. Nesse capítulo, apresentamos, junto às análises, os fundamentos teóricos dos fatos mais significativos do ponto de vista terminológico, que fundamentam esta dissertação. Nosso propósito foi oferecer um consistente arcabouço teórico para a sustentação do trabalho. Todo esse trabalho foi realizado pela análise e interpretação de dados, com a finalidade de verificar quais são os recursos disponíveis para formação de termos e quais são os processos de formação pertinentes a cada termo.

No Capítulo 4, apresentamos o glossário das unidades terminológicas estudadas que compõem o cenário de crimes cibernéticos, com informações técnicas, instruções de como consultar a obra e informações sobre a macro e microestrutura dos verbetes.

No Capítulo 5, expomos como considerações finais as reflexões e conclusões resultantes de todo o estudo realizado nesta pesquisa.

Por fim, relacionamos as Referências da dissertação e do glossário. Nos Anexos, acrescentamos o questionário aplicado na entrevista com o Grupo de Repressão a Crimes Cibernéticos, e a legislação específica existente no Brasil a respeito do tema.

Esclarecemos, ainda, que os gráficos, figuras e quadros cuja referência é Justiniano (2015, 2016) foram criados para os fins desta dissertação.

**JUSTIFICATIVA**

A ideia da pesquisa nasceu a partir da minha experiência profissional trabalhando com revisão e produção de textos. Primeiramente me interessei pela linguagem da Internet ao ser convidada a participar de Projetos Especiais de um dos maiores grupos de comunicação do Brasil e o maior da região centro-oeste, o Grupo Diários Associados. Envolvi-me com planejamento, elaboração, produção e revisão de textos e conteúdo, integrando, junto a outros profissionais, uma equipe incumbida da criação e desenvolvimento de um site institucional.

Outro momento importante para que eu me interessasse pelo tema foi, no decorrer da profissão, minha participação em um Grupo de Trabalho em que auxiliei a aprimorar uma categorização desenvolvida para classificar entradas no banco de dados do site da empresa. O objetivo era melhorar a qualidade, eficácia e eficiência das ferramentas de busca no site e facilitar mecanismos de buscas on-line. A classificação de domínios distintos e necessidade de categorização e criação de campos semânticos mostrou-me que uma variedade de questões linguísticas precisava ser considerada.

Ao compor uma equipe multidisciplinar e trabalhar lado a lado com programadores, comunicólogos, administradores, historiadores, *web* designers, entre outros, pude notar que havia uma grande distância entre o mundo acadêmico e o mundo comercial da internet. Certo dia, necessitei consultar um glossário da Internet, e notei que não havia. Passei a fazer pesquisas e, lendo vasta literatura a respeito da Terminologia e Política do Idioma produzida pela Prof.ª Dr.ª Enilde Faulstich, me deparei com a obra "Lexicologia: a linguagem do noticiário policial", livro resultante de sua dissertação de mestrado.

Inicialmente, já foi possível verificar que os termos que designam o que ocorre no ciberespaço não possuem definições claras e muitos nem sequer encontram-se formalmente registrados ou dicionarizados. Tal fato ampliou meu interesse para a linguagem utilizada no caso de crimes cibernéticos. A falta de termos de especialidade nessa área dificulta o trabalho profissional e fragiliza a utilização do ciberespaço.

Itens lexicais são capazes de demonstrar a relação reflexiva entre a língua e a sociedade. Desenvolvemos, então, partindo dessa ótica, uma proposta de estudos capaz de analisar itens lexicais selecionados, considerando a ênfase na relação atualmente estabelecida entre a linguagem, as interfaces tecnológicas do ciberespaço e os crimes nele praticados.

A motivação inicial, fazendo convergir áreas que englobam diferentes dimensões, foi refinada, saindo de algo amplo como itens lexicais em contexto de *web* para tomar forma e resultar no tema de pesquisa "Terminologia e tecnologia: um estudo de termos de crimes cibernéticos".

Entendendo a importância e a carência de uma possível solução para este problema, me dediquei à elaboração de material com conteúdo que esteja em consonância com o uso adequado da Internet e que subsidie o direito a um ciberespaço seguro. Isso só foi possível com o desenvolvimento do glossário, que tem como objetivo principal promover um léxico especializado, que esteja disponível para ser consultado e que sirva de apoio para profissionais e usuários da web, além de ser matéria que promove conhecimento, acesso à informação e proporciona sermos mais cidadãos no ambiente digital.

## DELIMITAÇÃO DO PROBLEMA

A hipótese de pesquisa desta dissertação é que existe um conjunto de delitos praticados em ambiente cibernético e que constituem uma linguagem de especialidade, para a qual é necessário desenvolver um estudo terminológico próprio.

## OBJETIVOS

Esta dissertação tem como objetivo geral desenvolver um glossário que contemple a terminologia empregada em situações de crimes ocorridos em ambiente cibernético.

Para atingir o objetivo geral apresentado, relacionamos abaixo os seguintes objetivos específicos:

1) Identificar termos empregados para designar crimes cibernéticos;
2) Verificar as relações entre termos, conceitos e definições;
3) Registrar os termos em um glossário de crimes cibernéticos.

# CAPÍTULO 1 - CRIMES CIBERNÉTICOS E LEGISLAÇÃO

## 1.1 A Internet

Este capítulo é importante para situar o leitor quanto ao assunto da dissertação e ao nosso objeto de estudo. Para entender o que são, quais são e como se dão os crimes cibernéticos, precisamos fundamentalmente pesquisar e compreender primeiro a própria Internet.

Pouco mais de duas décadas desde sua criação, a Internet deixou de ser um ambiente restrito a poucos computadores universitários conectados, tornando-se um fenômeno mundial. Sobre o advento da Internet, Crystal (2005) relata que:

> Embora a Internet como tecnologia tenha estado presente desde a década de 1960 para e-mails e bate-papo, as pessoas só começaram a explorá-la 30 anos mais tarde. A Rede Mundial só passou a existir propriamente em 1991. (p. 75)

Crystal (2005) propõe que, para usufruir da inovação deste século, faz-se necessário levar em consideração as funções que ela seria capaz de realizar. Somente em última análise, a definição para Internet seria meramente uma associação de redes de computadores compartilhando padrões comuns, permitindo que mensagens fossem enviadas de qualquer computador em uma rede para outra. Dessa forma, podemos compreender a Internet como o agente de uma verdadeira revolução. O mesmo autor sustenta essa característica revolucionária considerando que acontecimentos da magnitude como o que a Internet promoveu são, na verdade, eventos raros na história da humanidade.

> Não creio que 'revolução' seja uma palavra muito forte para o que vem acontecendo. Revolução é qualquer combinação de acontecimentos que produza mudanças radicais de consciência ou comportamento em um período de tempo relativamente curto, e foi isso que ocorreu. Há sempre continuidades com o passado, mas estas são compensadas pelo surgimento de uma perspectiva genuinamente nova. (CRYSTAL, 2005, p.15)

A Internet é a maior rede mundial, capaz de fornecer uma variedade crescente de serviços e informações, tornando possível um número sem precedentes de pessoas se comunicarem e interagirem umas com as outras, através de diversificados recursos e múltiplas técnicas. Considerando tais fatores, parece-nos adequado falar em revolução quando consideramos o popular www, como é conhecida a Word Wide Web.

Ao falarmos de Internet, é preciso levar também em consideração o computador, seu principal e primeiro veículo de propagação. Atualmente, é possível utilizar a Internet nos mais

variados tipos de dispositivos, como *tablets, notebooks*, e até mesmo em aparelhos de telefone móvel, os celulares. Porém, houve uma época em que a Internet dependia exclusivamente do computador para seu uso. Lévy (1999, p.31)) discorre sobre o surgimento do computador e como o uso dessa tecnologia se desenvolveu e afetou a sociedade:

> Os primeiros computadores (calculadoras programáveis capazes de armazenar os programas) surgiram na Inglaterra e nos Estados Unidos em 1945. Por muito tempo reservados aos militares, seu uso civil disseminou-se durante os anos 60. [...] que haveria um movimento geral de virtualização da informação e da comunicação, afetando profundamente os dados elementares da vida social, ninguém com a exceção de alguns visionários, poderia prever naquele momento.

Muitos crimes cibernéticos são praticados através do uso de um computador. A virada fundamental dessa tecnologia, segundo Lévy (1999), data dos anos 1970, com a introdução do computador pessoal na vida da população. É importante considerarmos esses marcos para entendermos em que contexto surgem posteriormente os crimes cibernéticos.

> Um verdadeiro movimento social nascido na Califórnia na efervescência da "contracultura" apossou-se das novas possibilidades técnicas e inventou o computador pessoal. Desde então, o computador iria escapar progressivamente dos serviços de processamento de dados das grandes empresas e dos programas profissionais para tornar-se um instrumento de criação (de textos, de imagens, de músicas), de organização (banco de dados, planilhas), de simulação e de diversão (jogos), nas mãos de uma porção crescente da população dos países desenvolvidos. (LÉVY, 1999, p. 32)

Outro momento importante no crescente da tecnologia foi o surgimento do chamado ciberespaço. Trata-se de um local virtual, interativo e comunitário, fruto da inteligência coletiva, em que tempos depois ocorreriam os primeiros crimes cibernéticos. A esse respeito, Levy (1990, p.32) relata que:

> No final dos anos 80 e início dos anos 90, um novo movimento sociocultural originado pelos jovens profissionais das grandes metrópoles e dos campi americanos tomou rapidamente uma dimensão mundial. Como no caso do computador pessoal, uma corrente cultural espontânea e imprevisível impôs um novo curso ao desenvolvimento tecno-econômico. (...) as tecnologias digitais surgiram, então como a infraestrutura do ciberespaço, novo espaço de comunicação, de sociabilidade, de organização e de transação, mas também novo mercado da informação e do conhecimento.

A Internet, criada em 1990, como um meio de possibilitar que físicos em diferentes instituições compartilhassem informações, pesquisas e documentos sobre seus estudos, se difundiu com tamanha rapidez e se expandiu para outras áreas de uma maneira impensável, e

de forma paradoxal, já que é abrangente e concomitantemente específica nos mais diversos assuntos. Muito provavelmente, em seus primórdios de criação, nem os mais visionários poderiam prever os desdobramentos e até o lado negativo impresumível que viria a surgir com os crimes cibernéticos.

Segundo Crystal Crystal(2005, p.77), "o termo ciberespaço foi cunhado para capturar a ideia de um mundo de informação presente ou possível, em forma digital, chamado anteriormente de *information superhighway"*, ou como o técnico de computadores Timothy Berners-Lee, o criador da Word Wide Web (ou web, como comumente conhecemos) a definiu: "um universo de informação acessível por rede, um conjunto do conhecimento humano" (BERNERS-LEE, 1999, p. 132 apud CRYSTAL, 2005).

O primeiro *website* da história da Internet, projetado por Berners-Lee, estava centrado em informações sobre o projeto Word Wide Web Consortium, ou também W3. Não há imagens da tela original dessa página, porém ainda hoje é possível acessar uma cópia, conforme a Figura 1 que disponibilizamos a seguir:

Fonte: Página da Word Wide Web[1]

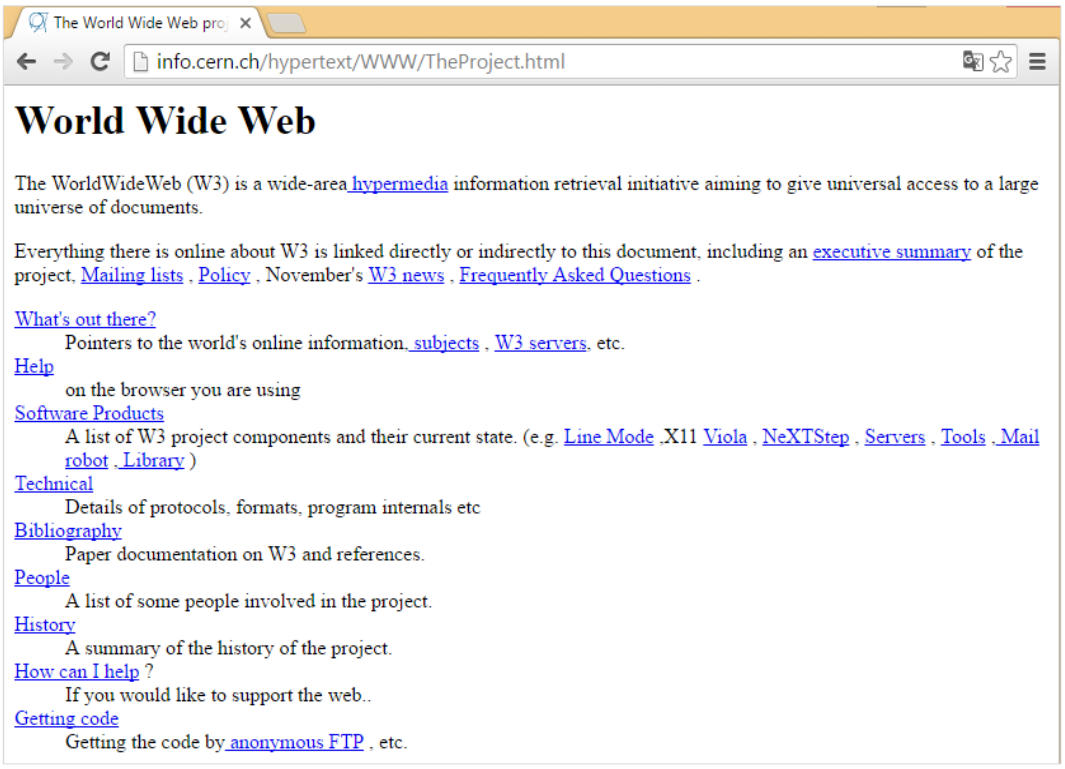



**Figura 1** - Primeira página da Word Wide Web

Podemos observar pelas informações disponíveis na página, que o *site* oferece uma explicação sobre em que se constitui a www. Informações de como criar um navegador, como instalar e configurar um servidor web estão acessíveis. Visitantes podem aprender mais sobre

[1] Disponível em: <http://info.cern.ch/hypertext/WWW/TheProject.html> Acesso em 23 ago. 2015.

hipertexto, detalhes técnicos para criação de sua própria página *web*, e podem ter até mesmo uma explicação sobre como pesquisar na web para obter informações. Dessa análise, podemos notar que o primeiro *website* foi, justamente, uma página cujo objetivo do conteúdo era o de orientar como criar um *website*.

Diante do conteúdo da página apresentada, podemos observar que o Word Wide Web se apresenta como uma iniciativa de recuperação de informação de área ampla, com o objetivo de dar acesso universal a um grande universo de documentos, a partir de um sistema de identificação global. Podemos notar que o primeiro *website* da história apresenta como conteúdo uma linguagem de *website*, que serve para descrever e falar a respeito da construção do próprio website, referindo-se à sua própria linguagem. Curiosamente, foi elaborado de maneira altamente metalinguística, exprimindo uma elevada noção de reflexão sobre o próprio objeto.

Avaliando a página, é possível perceber que Berners-Lee deixou sua ideia disponível livremente, sem registro de patente e sem a cobrança de royalties devidos. O World Wide Web apresenta suas normas baseadas em tecnologia livre, de modo que possam ser facilmente adotadas por qualquer pessoa. Sem a cobrança de direitos exclusivos para o produtor, possibilita a criação de outros sistemas e extensões sem a preocupação de licenciamento, tornando-se aberto para todos, e sem custos.

É pertinente para esta pesquisa que se evidencie o processo de construção do ciberespaço, a fim de termos uma melhor compreensão de como a Internet se desenvolveu até chegar ao ponto que vivenciamos hoje, visto que é nesse cenário que ocorrem os crimes cibernéticos.

A Internet foi, portanto, planejada para interação multimídia entre usuários de computador em qualquer lugar do mundo. Suas múltiplas funcionalidades incluem hoje referências enciclopédicas, dados arquivísticos, anúncios, notícias, autopublicações, jogos, transações comerciais de todos os tipos, filmes, músicas, áudios, fotos, textos, imagens, além das mais variadas formas de trabalho, jogos e diversão. Tudo isso cada vez mais disponível e acessível.

O mundo da Internet é extremamente fluido, com usuários explorando possibilidades de expressão, introduzindo novas combinações de elementos, interagindo e reagindo ao desenvolvimento e às inovações tecnológicas. A Internet é um canal eletrônico, globalizado e interativo. Esse breve percurso histórico que aqui apresentamos acerca da Internet nos ajudará a entender melhor como cada uma dessas características implica consequências para o tipo de linguagem empregada, inclusive no que tange à designação de crimes de natureza cibernética.

## 1.2 O papel da Internet

Certamente, a tecnologia vem modificando, ao longo dos anos, algumas dimensões de nossas relações sociais, temporais, espaciais e pessoais. A Internet, como uma das mais recentes formas de tecnologia, está inserida em nossas vidas, e também nas relações que estabelecemos com a construção de conhecimentos, inclusive linguísticos. A Internet pode ser tomada como sendo um recurso favorável, parte inerente da vida cotidiana do ser humano. Muitas sociedades têm se estruturado de tal forma que praticamente não são mais capazes de existir sem a Internet, constituindo uma relação de dependência, e até mesmo colocando-se no lugar de reféns da tecnologia.

O ambiente virtual, parte do crescente tecnológico, pode ser também um grande vilão se tomado com más intenções de uso. Na Era Digital, tanto a construção da linguagem quanto a relação do homem com ela estão mudando rapidamente. O século XXI precisa agora aprender a lidar com as consequências de verdadeiras revoluções tecnológicas.

Ao desenvolver um trabalho em um panorama contemporâneo, propomo-nos a dialogar com o novo, o que está sendo experienciado por pesquisadores, linguistas, estudiosos, professores, profissionais e estudantes que vivenciam a hipermídia em plena Web 2.0, também conhecida como Web participativa, ou colaborativa.

A facilidade de comunicação, inclusão, informação, superação de distâncias, transações comerciais, velocidade de trocas, dentre outros, são claros sinais de pontos positivos que a Internet promoveu e promove. Os pontos negativos também vão surgindo concomitantemente, tais como prática de crimes, informações inconsistentes, fontes inseguras, conteúdos ilegais, distanciamento nas relações pessoais, entre outros.

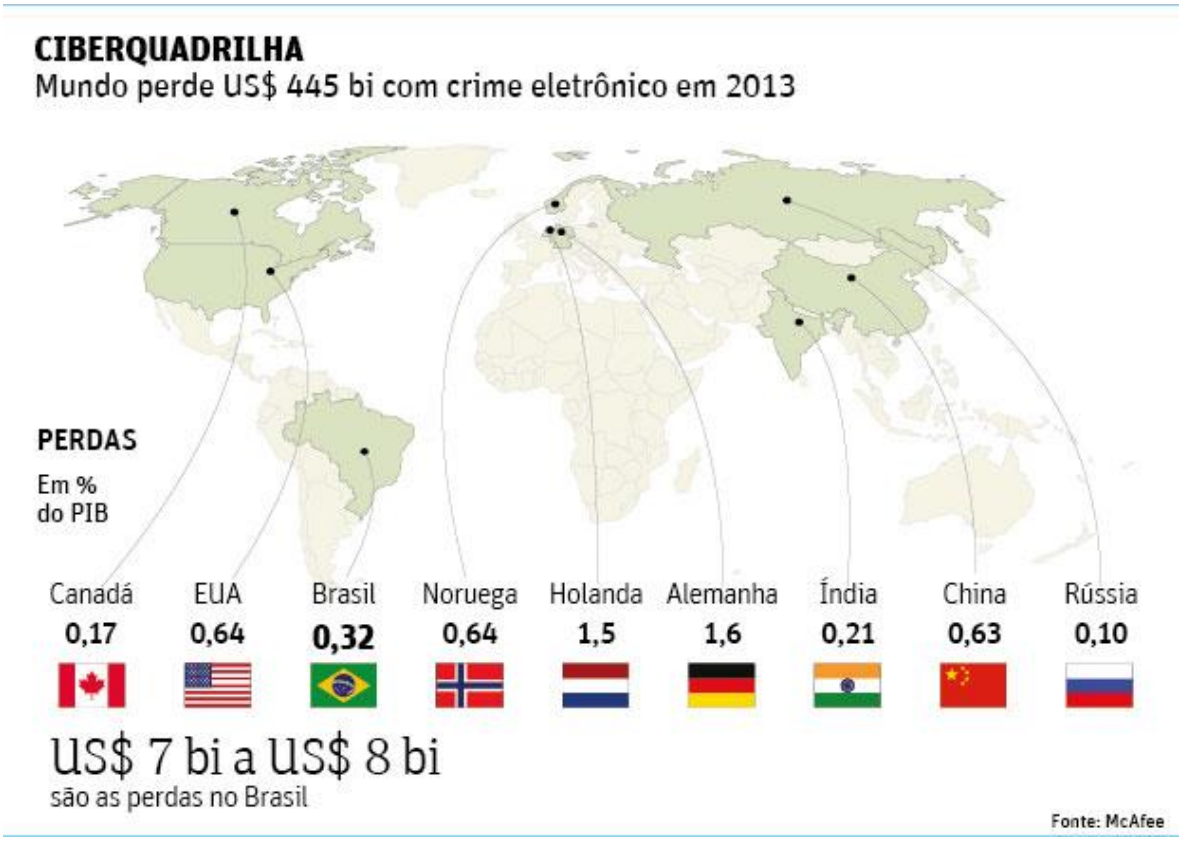
À medida que a Internet tem facilitado a vida das pessoas, em contrapartida, devido à dificuldade de investigação gerada pelo anonimato que ela oferece, é grande a sensação de impunidade. Dessarte, a Internet trouxe consigo tanto benefícios quanto malefícios para a vida em sociedade.

Como vimos, a Internet, desde seu projeto de criação não está originalmente ligada a nenhum tipo de crime. Todavia, apesar das boas intenções de invenção do recurso, de acordo com Folha (2014), o Brasil perdeu entre 7 e 8 bilhões de dólares em 2013 entre ataques de hackers, roubos de senhas, clonagens de cartões, pirataria virtual, além de espionagem industrial e governamental, entre outros crimes cibernéticos. Essas informações são muito relevantes para compreendermos a dimensão que os crimes cibernéticos podem atingir.

São crimes arquitetados muitas vezes por quadrilhas internacionais, que contam com hackers e engenheiros para atacar áreas vulneráveis do comércio internacional, transferência de valores, e produção de tecnologia. Podemos perceber o alto grau de importância do assunto, pois trata-se de novas modalidades de crime.

De acordo com Folha (2014), pesquisa mundial feita pela McAfee, empresa de segurança eletrônica do Grupo Intel, divulga que pelo menos 5% das empresas brasileiras já sofreram algum tipo de ataque cibernético. Podemos ver outras estimativas que fazem parte da pesquisa no Gráfico 1, seguinte.

**Gráfico 1** – Perdas financeiras com crimes eletrônicos no mundo em 2013




Fonte: Editoria de Arte/FolhaPress[2]

Ao analisarmos o gráfico, podemos notar que o Brasil, em 2013, perdeu o equivalente a 0,32% do PIB brasileiro devido ao cometimento de crimes cibernéticos, o que equivale entre 7 e 8 bilhões de dólares. Isso deixa o Brasil em quinto lugar no mundo dentre os países mais

[2] Disponível em <http://www1.folha.uol.com.br/mercado/2014/06/1467110-brasil-perde-ate-us-8-bilhoes-com-crime-cibernetico.shtml> Acesso em 15 ago. 2015

prejudicados com essa modalidade de crime. Em primeiro lugar, está a Alemanha, com uma perda de 1,6 de seu PIB, seguida da Holanda com 1,5 % de seu PIB, e em terceiro lugar estão Estados Unidos e Noruega, com 0,64%.

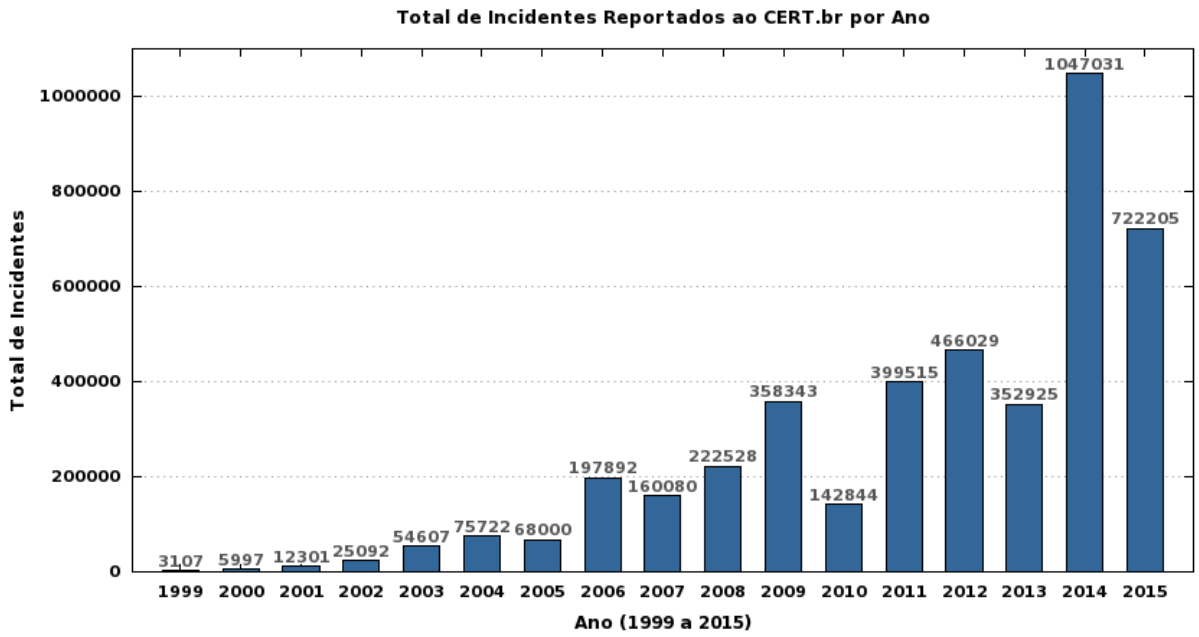
No mundo, esses prejuízos atingiram em 2013 entre 375 bilhões e 575 bilhões de dólares aproximadamente, incluindo tanto as perdas quanto os gastos para recuperação de ataques. Podemos notar que os crimes cibernéticos causam graves perdas financeiras com proporções reais para diversos países no mundo.

Ainda segundo a pesquisa, o crime cibernético (também chamado crime eletrônico dentre outras variantes, conforme veremos no Capítulo 3), já é o terceiro que mais causa prejuízos no mundo, precedido do narcotráfico, da falsificação de marcas, e de propriedade intelectual. Mesmo com essa constatação, as  Mesmo com esta constatação, os limites e intolerâncias aos crimes cibernéticos aainda não estão muito bem estabelecido em muitos países, assim como no Brasil.

Para isso, o governo, as empresas, e a sociedade precisam adotar ações estratégicas e enérgicas para controlá-los e combatê-los. Precisamos então, primeiramente, compreender e definir as situações que configuram os crimes cibernéticos, para, após esse momento, especificá-los e descrevê-los. Empenhamo-nos numa pesquisa a fim de gerar um material com conteúdo que pode ajudar na construção de uma legislação eficaz para ser aplicada no Brasil, de forma que seja fomentado o combate aos crimes cibernéticos.

No Brasil, segundo dados estatísticos divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, o CERT.br, setor vinculado ao Comitê Gestor da Internet no Brasil – CGI.br, houve o aumento significativo no número de incidentes. Podemos ver outras estimativas que fazem parte da pesquisa, conforme pode ser observado no gráfico seguinte.

**Gráfico 2** – Total de incidentes reportados ao CERT.br por ano




Fonte: Página do CERT.br[3]

Na análise dos dados apresentados, os últimos dezesseis anos mostram que a quantidade de ações danosas informadas no meio cibernético passaram de pouco mais de três mil em 1999, para mais de um milhão no ano de 2014. O quadro é extremamente preocupante e acentua a percepção aqui apresentada, da necessidade de um estudo terminológico dos crimes cibernéticos que venha a fomentar pesquisas que possam subsidiar o trabalho de combate aos crimes, com vistas a retirar o país da atual situação de vulnerabilidade.

## 1.3 Patrimônio virtual

A Internet vem funcionando como um verdadeiro repositório do conhecimento mundial. Toda a sorte de informações, dados públicos ou privados são inseridos diariamente no ciberespaço, onde são armazenados para divulgação, pesquisa, consulta ou até mesmo arquivamento. Assim sendo, toda essa gama de conteúdos que se encontra disponível na Internet pode ser vista como um amplo patrimônio que está sendo construído coletivamente pela humanidade. A Internet, quando considerada como uma grande riqueza de informações que vêm sendo acumulada dia após dia, acaba também vulnerável a alguns tipos de crimes, da mesma forma que qualquer outra fonte de bens.

[3] Disponível em: <http://www.cert.br/stats/incidentes/> Acesso em 07 de março de 2016

Dodebei (2008) apresenta a ideia de patrimônio desvinculado apenas do sentido de simples acumulação. Isso favorece considerar a existência de verdadeiros patrimônios no ciberespaço. É possível aos itens componentes do léxico especificar particularidades que qualificam conceitos. Dessa forma, o conceito de patrimônio pode sofrer uma ampliação de definição, ou reconfiguração. É plausível que a circulação dos bens patrimoniais digitais ou digitalizados na *web* possibilite que o conceito de acumulação também faça parte da constituição da memória virtual do mundo no ciberespaço.

Para falar de crimes cibernéticos, é preciso, primeiramente, situar-nos em conceitos primordiais. Dodebei (2008) explicita que o nome Internet vem de *Internetworking* que significa "ligação entre redes". Embora geralmente pensada como rede, a Internet na verdade é o conjunto de todas as redes que usam protocolos de conexão. A mesma autora estabelece a diferenciação existente entre a Internet e a *web,* visto que as duas palavras muitas vezes são empregadas como equivalentes, porém não tem o mesmo significado. A Internet é o conjunto de meios físicos (linhas digitais, computadores, roteadores etc.), programas, e protocolos de conexão usados para o transporte da informação, e a *web* é um dos serviços disponíveis através da Internet.

Em uma comparação simplificada, a Internet seria considerada análoga à rede telefônica, com seus cabos, sistemas de discagem e encaminhamento de chamadas, enquanto que a *web* seria similar a utilizar um telefone para comunicações de voz, embora o mesmo sistema possa ser usado para transmissões de fax ou dados, por exemplo. A Internet não é a World Wide Web, uma vez que, devido ao seu desenvolvimento e amplidão, ela melhor significaria o veículo pelo qual o correio eletrônico, os servidores, a www e outros serviços trafegam. Nesse ambiente complexo, interessa-nos discutir crimes cibernéticos como um dos fenômenos que ali se propaga silenciosamente.

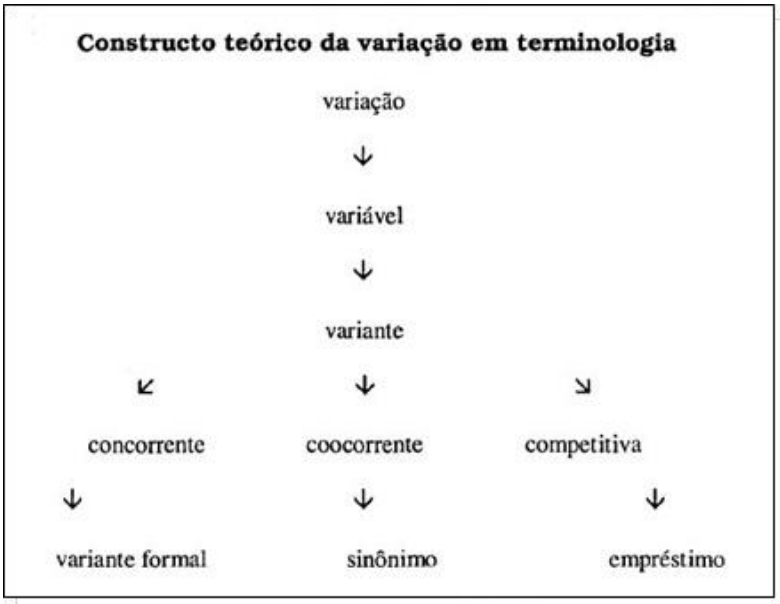
Como constatação desta pesquisa, podemos dizer que a Internet foi disponibilizada para pessoas comuns através da *web*. A www ficou conhecida por proporcionar uma interface da internet acessível e interessante, principal responsável pela popularização da Internet. Juntamente com navegadores, ou *browsers*, propôs aos usuários o acesso à informação.

Na literatura que discorre sobre virtualidade e digitalidade, os conceitos são obscuros e não há muita clareza em suas definições. Daí que se torna difícil compreender crime nesse ambiente. Porém, é possível compreender que digitalizar compreende o processo de representar um objeto concreto ou analógico em bits. A imagem digitalizada se transforma em conjuntos de pixels que podem ser compreendidos visualmente pelo olho humano e também

tais pressupostos teóricos. Seus postulados apresentam a ideia de abandono do isomorfismo categórico entre termo-conceito-significado associado à aceitação de que, sendo a terminologia um fato de língua, acomoda elementos variáveis.

Na figura que segue, apresentamos o esquema gráfico do Constructo teórico da variação em terminologia, proposto por Faulstich (2001), no qual podemos visualizar a distribuição das categorias em concorrentes, coocorrentes e competitivas:

**Figura 7** – Constructo teórico da variação em terminologia




Fonte: Faulstich (2001, p. 26)

As definições e explanações acima são importantes, pois, em nossa pesquisa, identificamos diferentes fenômenos de variação dentre as unidades terminológicas selecionadas do contexto da linguagem empregada para designar crimes cibernéticos. No processo de investigação nos dados de pesquisa, constatamos a ocorrência de variantes coocorrentes na maioria dos termos, e alguns termos foram classificados como variantes competitivas.

A observação direta do uso dos termos de crimes cibernéticos ocorreu sob a perspectiva da teoria da variação em terminologia proposta por Faulstich (2001), que aplica-se ao nosso trabalho, pois privilegia o estudo do termo e do conceito com base na observação do uso e no registro social. Importa-nos, portanto, averiguar como ocorre a variação dos termos de crimes cibernéticos.

Faulstich (2001, p.26) apresenta, as categorias de variantes dos termos, a saber:

por programas de computação. De fato, o mundo virtual é habitado apenas por objetos digitais, ou que passaram pelo processo de digitalização.

Para tratarmos de crimes cibernéticos, é preciso retomar conceito de ciberespaço, que é o cenário em que ocorrem os crimes dessa natureza. A esse respeito, Lévy (2001) relata que:

> O ciberespaço (que também chamarei de 'rede') é o novo meio de comunicação que surge da interconexão mundial de computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ele abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo 'cibercultura', especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço. (p.71)

No espaço virtual, o conceito de patrimônio sofre transformações produzidas pelas novas dimensões de tempo e de espaço do mundo organizado por redes interligadas de computadores, notadamente em relação aos atributos de acumulação, permanência e integridade. Podemos, portanto, inferir que existe verdadeiro patrimônio ilimitado de espécie virtual, em um território digital, que a *web* nos proporciona.

Com relação a crimes cibernéticos, a Cartilha de segurança para a Internet, elaborada pelo comitê Gestor da Internet no Brasil (2012), reconhece que muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio. Podem ser inclusive tipificados como estelionato, que, de acordo com o Código Penal Brasileiro, Título II, Capítulo VI, artigo 171, é definido como "obter para si ou para outro, vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento". Dessa forma, o indivíduo que comete um crime cibernético pode ser considerado estelionatário.

Há complexidades para a construção do sentido e do significado de itens lexicais que denominam os crimes de cunho cibernético. A primeira delas diz respeito à compreensão de uma extensão conceitual ao que tradicionalmente se nomeia. Os adjetivos virtual e digital, por exemplo, modificam o conceito de patrimônio, especificando-o com propriedades criadas no âmbito da filosofia (virtual) ou no âmbito da cibernética (digital). Ao lado das noções de digitalidade e de virtualidade, identificamos a possibilidade do conceito de acumulação fazer parte da constituição da memória no ciberespaço.

O argumento principal que sustentamos é que a internet é um patrimônio integralmente artificial, herdado de um processo evolutivo no qual o homem tem um papel maiúsculo. A Internet é um patrimônio criado pelo homem, mas que não é de propriedade

exclusiva de nenhum grupo humano nem do passado nem do presente. Tem sua origem em tipos de ações humanas por ser obra construída, mantida, ou modificada, intencionalmente, pelo trabalho e engenho humanos, com propósitos bem definidos.

Por sua vez, o ciberespaço contribui para um patrimônio difuso e coletivo, intangível em algumas de suas dimensões. Um dos principais pontos é que são justamente essas características que dificultam a proteção de quem se expõe nesse ambiente virtual.

Não obstante, entendemos que o ciberespaço, inevitavelmente utilizado pela sociedade, assim como outros bens públicos ou coletivos, precisa que empenhemos esforços no sentido de protegê-lo, tornando-o um local seguro contra crimes cibernéticos, mesmo que a ideia de o resguardar pareça algo difícil, complexo e até pretensioso.

A definição apropriada do que são e quais são os crimes cibernéticos é o começo de um ciberespaço mais seguro e preservado, não somente porque é útil aos seres humanos, mas principalmente porque tem um valor inestimável em si mesmo, enquanto manifestação complexa do fenômeno da vida.

O que pretendemos com essa seção foi salientar que o ciberespaço, como parte integrante da Internet, deve ser considerado como patrimônio, como um bem ou conjunto de bens trafegando em uma realidade não analógica, descentralizada e de âmbito mundial, de valor reconhecido para a humanidade, a partir do qual pode-se conectar qualquer tipo de usuário e possibilita o acesso a toda espécie de informação, e que está suscetível às mais variadas formas de crimes e, portanto, precisa ser protegido, e deve ser preservado para o usufruto da sociedade, como uma verdadeira herança deixada a nós pelo que nos antecederam.

Levando em conta esse raciocínio, podemos considerar as violações e delitos que ofendem a este bem um ato condenável de consequências negativas que suscitaria uma reação organizada da sociedade. Estamos falando dos crimes cibernéticos, que lesam o patrimônio virtual, que faz parte do patrimônio cultural, do patrimônio público, e do patrimônio individual.

### 1.4 Crimes cibernéticos: o que são?

Em entrevista realizada com do Grupo de Repressão aos Crimes Cibernéticos da Polícia Federal, segundo Sousa (2015, p.1), a definição mais adequada a adotar para o termo “crime cibernético” é:

> Utilizo o conceito de crime cibernético como a ação humana que utiliza o sistema informático como meio para a prática de condutas ilícito-típicas ou como o fim último daquelas. No primeiro caso, diz-se crime cibernético impróprio; no segundo, próprio.

Nesse sentido, é preciso esclarecer que os crimes cibernéticos impróprios são aqueles que utilizam o sistema informático como meio para a prática de condutas ilícito-típicas já existentes, que já estão previstos na legislação penal tradicional brasileira. A alteração que ocorre é apenas instrumental, não havendo, portanto, a necessidade de legislação específica.

Um furto, por exemplo, pode ser praticado de forma pessoal ou de forma cibernética, mas será tratado da mesma forma pelo Código Penal, no Artigo 155. Outro exemplo é o crime de pedofilia, ou estelionato, que é a utilização do sistema informático como meio, como veículo para a prática de um delito que já se encontra devidamente definido e previsto na legislação penal vigente. Os infratores cometem delitos já previstos na legislação nacional, porém valendo-se da Internet como um meio. Nestes casos, portanto, não há o que se falar em novos tipos penais, já que as condutas ou bens que porventura forem violados já estão tutelados pelo Código Penal e por leis específicas.

São considerados crimes cibernéticos próprios aqueles que têm o sistema computacional como fim da conduta ilícito-típica. Estes, sim, exigem legislação especial, pois se configuram como novos tipos penais. A Internet, os computadores e o ciberespaço, conforme discorremos nas seções anteriores são tecnologias extremamente recentes na história da humanidade, datadas de cerca de apenas duas décadas. E no caso do Brasil, no que remete a leis que regulam, tipificam e esclarecem quais são esses crimes e determine suas penas, notamos uma extrema carência.

Outrora, para tratar, por exemplo, da invasão de um computador, não havia legislação, visto que o nosso Código Penal é de 1940, quando os computadores ainda não existiam. Portanto, não poderiam ser considerados como bens jurídicos demandantes de proteção jurídica. A Lei nº 12.737, de 30 de novembro de 2012, veio suprir essa lacuna e previu o crime de "invasão de dispositivo informático", quando inseriu o Artigo 154-A, no Código Penal.

Além disso, a mesma lei alterou a redação do Art. 266 do Código Penal para prever a conduta de "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", que se refere ao ataque distribuído de negação de serviço ou ataque de negação de serviço. Isso ocorre quando uma máquina é exigida para além de sua capacidade de transmissão de pacotes na rede, o que ocasiona a

interrupção desse serviço.

Para crimes cibernéticos diversas infrações ainda não estão previstas em lei, tendo como consequência a impunidade, por ausência de regulamentação específica na área de Direito Penal, dando vazão à atuação de agentes criminosos.

A Internet, uma inovação tecnológica, acabou por acrescentar um novo *modus operandi* para cometimento de delitos. Porém, seja como for, por mais que um crime já esteja previsto em lei, tal previsão não cita o emprego da Internet como uma nova possibilidade para atingir o objetivo, que é o resultado final de um crime. Muitas vezes, a interpretação se dá por analogia.

Corrêa (2002, p.10) afirma que, sem que haja uma legislação específica para tratar os crimes cibernéticos, não é possível dar o mesmo tratamento a um crime cometido na "vida real", por assim dizer, e a um cometido no ciberespaço. Caracterizar como um tipo de qualidade a infração previamente descrita no Código Penal Brasileiro, que leve em consideração o agravante do indivíduo ter cometido determinado crime por meio da Internet, seria uma possível solução a ser considerada.

Essa pode ser uma alternativa para se equilibrar as diferentes condutas, já que não pareceria equitativo julgar e condenar um indivíduo que cometeu o crime de peculato, ou estelionato no mundo material da mesma forma que uma pessoa que o cometeu no mundo digital, tendo em vista a gravidade de consequências, geração de efeitos, e maiores possibilidades de opções de atuação.

### 1.5 Crimes cibernéticos e o Princípio da Legalidade

Partindo do que estabelece o Artigo 5º, inciso II, da Constituição Federal, *"*ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*",* o Direito Penal estabelece um comando geral e abstrato, o Princípio da Legalidade, como uma consequência direta e necessária da própria noção do Estado Democrático de Direito, afinal o Brasil é regido por leis que asseguram a participação democrática.

Segundo o Princípio da Legalidade, há dois outros princípios: o Princípio da Anterioridade da Lei Penal e o Princípio da Reserva Legal. O primeiro institui que não é possível atribuir uma pena a um ato praticado antes da edição de uma lei penal específica, exceto em benefício do réu. O segundo estabelece que não existe delito fora da definição da norma, ou seja, não é possível punir um indivíduo sem que antes haja uma lei prévia, escrita, estrita e certa.

Podemos entender, segundo tais dispositivos, que com relação aos crimes, somente mediante a lei é possível criar direitos, deveres e proibições, ficando os indivíduos vinculados aos comandos legais disciplinadores de suas atividades. Mediante a jurisprudência atual, não há o que falar em crime sem primeiro existir lei anterior que o defina, e não há como imputar pena sem prévia cominação legal. É preciso ordenamento jurídico para práticas que não tinham consagração legal, como no caso de delitos cibernéticos.

### 1.6 Crimes cibernéticos e a legislação vigente no Brasil

A chegada da Era Digital trouxe consigo algumas implicações, dentre elas a necessidade urgente de uma legislação específica e adequada para o novo cenário que surge. A problemática da ausência de legislação acerca do tema no Brasil se intensificou, visto que a identificação dos crimes muitas vezes não é possível. A virtualização das relações sociais, que englobam tanto as de ordem pessoal, como comercial e governamental, originou a discussão sobre a necessidade controversa de se regulamentar ou não o uso da Internet.

Leis que caracterizam crimes cibernéticos e garantem uma punição foram sancionadas e entraram em vigor. Essas novas regras modificaram o Código Penal, que agora tipificam os crimes cibernéticos e instituem punições. Foram publicadas três leis que alteram o Código Penal, a fim de tratar a questão de crimes cibernéticos. São elas: a Lei nº 12.735, de 30 de novembro de 2012; a Lei nº 12.737, de 30 de novembro de 2012; e a Lei nº 12.965, de 23 de abril de 2014, ou Marco Civil da Internet.

Note-se o quão recente é essa regulamentação, já que ocorreu apenas em 2012. Porém, a popularização do uso da Internet no Brasil intensificou-se nos últimos vinte anos e a jurisprudência, que não acompanhou o ritmo da tecnologia, começa a ser instituída já retardatária. Essas três leis são tudo o que temos no Brasil como legislação vigente acerca de crimes cibernéticos, e ainda não abarcam todos os tipos e variedades de crimes ocorridos em ambiente virtual, conforme veremos na análise que segue.

#### 1.6.1 Lei nº 12.735, de 30 de novembro de 2012

A Lei nº 12.735/12 tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares. O projeto original dessa Lei, o PL 84/99, já tramitava no Congresso desde 1999. Cabe aqui considerar a lentidão da tramitação no Poder Legislativo de 13 anos entre a criação do projeto e a promulgação da lei.

Ao analisarmos o texto, a Lei também dá outra providência, no Artigo 4º, que estabelece 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.

Apresentamos o texto da Lei nº 12.735, de 30 de novembro de 2012 ao final da dissertação, em Anexos.

### 1.6.2 Lei nº 12.737, de 30 de novembro de 2012

A Lei nº 12.737/12 dispõe sobre a tipificação criminal de delitos informáticos e más condutas cometidas através da Internet. Essa Lei tipifica crimes como: a invasão de computadores, o roubo de senhas e de conteúdos de e-mail, a derrubada proposital de sites e o uso de dados de cartões de débito e crédito sem autorização do titular. A disseminação de vírus de computador ou códigos maliciosos para roubo de senhas é agora considerado crime cibernético e poderá ser punida com prisão de três meses a um ano, além de multa.

A Lei nº 12.737/12, apelidada de Lei Carolina Dieckmann, é fruto do Projeto de Lei PL 35/12, elaborado em razão do vazamento na Internet de fotos íntimas que expunham conteúdo com caráter de nudez da atriz. É importante considerar que, por se tratar de uma figura pública e influente, o caso foi tratado com urgência, o que apressou a promulgação da Lei.

A prática do uso de dados de cartões de débito e crédito sem autorização do dono, por exemplo, passou a ser equiparada à falsificação de documento, com penas de um a cinco anos de prisão e multa.

Os crimes como "invasão de dispositivo informático" podem ser punidos com prisão de três meses a um ano, além de multa. Condutas danosas, como obter, pela invasão, conteúdo de "comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas" podem ter pena de seis meses a dois anos de prisão, além de multa. O mesmo ocorre se o delito envolver a divulgação, comercialização ou transmissão a terceiros, por meio de venda ou repasse gratuito, do material obtido com a invasão.

A lei prevê ainda o aumento das penas de um sexto a um terço se a invasão causar prejuízo econômico e de um a dois terços "se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos". As penas também poderão ser aumentadas de um terço à metade se o crime for praticado contra o presidente da República, presidentes do Supremo Tribunal Federal, da Câmara, do Senado, de

assembleias e câmaras legislativas, de câmaras municipais ou dirigentes máximos "da administração direta e indireta federal, estadual, municipal ou do Distrito Federal".

A Lei nº 12.737/12 é resultado de uma interação especial existente entre o Direito e a Tecnologia, que afeta diretamente os cidadãos, tipificando a prática de crimes cibernéticos perante a economia e a sociedade brasileira, contribuindo na construção de uma sociedade mais livre e justa. Porém, uma das críticas em relação às punições previstas nessa Lei é que são muito brandas, pois no Brasil pena de até quatro anos de reclusão para crime sem violência pode ser convertido em restrição de direitos. Ou seja, na prática dificilmente alguém sofrerá perda de liberdade, porque a nova lei prevê no máximo um ano de detenção.

Cabe aos pesquisadores do léxico, a desafiadora tarefa de investigar relações conceituais novas, facilitar respostas claras, capazes de suprir as necessidades advindas de novas eras, para promover conhecimentos seguros e coexistência pacífica entre os indivíduos. Esse novo mundo que surge, a Era Digital, exige um estudo de investigação que identifique novos termos e compile as informações em um glossário, visto que as condutas delituosas promovem o aumento da potencialidade lesiva de um ato antissocial quando se utilizam também da Internet.

A Internet possui grande potencialidade, concentra a atenção de pessoas, de governos, e de empresas. O ciberespaço movimenta um enorme contingente de empresas de tecnologia e de telecomunicações, responsáveis por fazer a rede funcionar. Empresas de conteúdo, comunicação, publicidade e propaganda criam sítios sobre assuntos e negócios dos mais variados. Pela Internet são realizadas diversas formas de transações financeiras e bancárias, ofertados vários recursos e serviços, com resultado no aumento do valor econômico associado ao mundo virtual. Assim sendo, o controle das ações precisa receber ordenamento jurídico do Estado.

Para fins de consulta, o texto da Lei nº 12.737/12 é apresentado ao final da dissertação, em Anexos.

### 1.6.3 Lei nº 12.965, de 23 de abril de 2014, ou Marco Civil da Internet

A Lei nº 12.965/14, ou o Marco Civil da Internet, é a lei que regulamenta o uso da Internet no Brasil mediante a previsão de princípios, garantias, direitos e deveres para os usuários da rede, da mesma forma que estabelece determinações para a atuação do Estado, com vistas à normatização e ao desenvolvimento de responsabilidades com caráter histórico e político.

Após ser desenvolvido colaborativamente um debate aberto com a sociedade por meio do blog <http://culturadigital.br/marcocivil>, surge o Marco Civil, apresentado como um Projeto de Lei do Poder Executivo à Câmara dos Deputados, sob o número PL 2.126/2011.

Ao analisarmos o texto da norma, destacamos o propósito de tratar de temas antes negligenciados e a intenção de promover avanços, como a busca de instituir direitos e deveres para usuários, provedores de serviço e de conteúdo e demais agentes envolvidos com o uso da Internet, e também garante a liberdade de manifestação do pensamento, a escolha do usuário sobre o conteúdo que deseja acessar, a livre concorrência na rede e a possibilidade de inovação.

O Art. 3º, no inciso IV, traz como um dos princípios da disciplina do uso da internet no Brasil, a preservação e a garantia da neutralidade da rede. Isso significa dizer que os provedores de acesso devem manter-se neutros de maneira a tratar todos os dados que circulam na Internet da mesma forma, sem distinção do fluxo de informação por conteúdo, origem e destino. Com a neutralidade, as empresas de telecomunicações não podem beneficiar o fluxo de tráfego de um site ou um serviço em detrimento de outro. Ou seja, por serem as provedoras, não poderão filtrar ou bloquear a comunicação.

Outro benefício que o Marco Civil da Internet oferece é a garantia da privacidade das comunicações. A atuação das empresas a partir de então precisa ser mais clara. A proteção dos dados pessoais e a privacidade dos usuários são garantias estabelecidas pela nova Lei. Isso significa, por exemplo, que as empresas de Internet que trabalham com os dados dos usuários para fins de publicidade (como os anúncios dirigidos) não poderão mais repassar suas informações para terceiros sem o seu consentimento expresso e livre.

A proteção aos dados dos internautas é garantida e só pode ser violada mediante ordem judicial, o que significa que, se alguém encerrar sua conta em uma rede social ou serviço na Internet, pode requerer que suas informações pessoais sejam eliminadas de maneira definitiva. O Marco Civil da Internet institui que os dados pertencem aos titulares, não a terceiros. Quanto a essa questão, é necessário ficar atento também à atualização dos termos de uso dos serviços e aplicativos.

A afirmação em Lei de que o sigilo e a proteção de privacidade garantidos aos meios de comunicação tradicionais, como cartas e telefonemas, tem a mesma validade para o conteúdo das comunicações privadas em meios eletrônicos, como *e-mails*, é um avanço importante.

Analisando o texto do Marco Civil, podemos também observar que a maior proteção da liberdade de expressão na Internet é outro progresso. A Lei assegura a liberdade de expressão, como preconizado na Constituição de 1988, fazendo do ciberespaço um ambiente democrático, aberto e livre, sem violar o direito à intimidade, à liberdade individual e à vida privada.

Uma mudança bastante significativa que essa Lei promove é com relação à retirada de conteúdo do ar, pois não havia uma regra clara sobre esse processo. Agora, indivíduos vítimas de violações da intimidade podem solicitar mediante ordem judicial a retirada de conteúdos da Internet, de forma direta, aos sites ou serviços que estejam hospedando esse conteúdo. Nesses casos, os provedores de acesso devem informar "os motivos e informações relativos à não disponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo", como atesta o Artigo 20 da Lei.

Ainda segundo o Marco Civil, os Juizados Especiais serão os responsáveis pela decisão sobre a ilegalidade ou não dos conteúdos, antes que eles sejam retirados do ar. Isso se aplica aos casos de ofensa à honra ou injúria, que serão tratados da mesma forma como ocorre fora de Internet. Essas violações são analisadas pelo Judiciário, garantindo que todos tenham pedidos avaliados por um juiz e não pelo provedor de Internet, que pode ser pressionado a retirar ou censurar conteúdos por diversas razões, como motivos financeiros, políticos, religiosos, entre outros.

A regulamentação do Marco Civil da Internet é muito importante para assegurar a segurança jurídica de suas normas e reforçar os direitos e garantias certificados. Apresentamos o texto na íntegra da Lei nº 12.965/12 ao final da dissertação, em Anexos.

A pesquisa da legislação existente no Brasil a respeito de crimes cibernéticos foi muito importante para o desenvolvimento de nosso trabalho, já que pudemos nos aprofundar no tema e destacar itens lexicais pertinentes. Na sequência deste estudo, discutiremos os princípios teóricos que amparam a descrição dos dados, composto por um léxico terminológico, e a metodologia empregada para coleta e análise de dados.

# CAPÍTULO 2 - PROCEDIMENTOS METODOLÓGICOS PARA COLETA A ANÁLISE DOS DADOS

## 2.1 Léxico Terminológico

Estamos em um período da história que se diferencia, de forma dialética, pela crescente integração mundial e compartilhamento de informações de um lado, concomitante à intensa especialização e particularização das áreas de conhecimento de outro. As diversas áreas do conhecimento trafegam em seu próprio universo linguístico, o que faz da terminologia uma área de atuação e um campo de estudos promissor para profissionais e pesquisadores. Tal cenário favorece o surgimento de léxicos terminológicos cada vez mais precisos e específicos, como é o caso de crimes cibernéticos.

Entendemos léxico terminológico como o conjunto de termos de uma determinada área de especialidade, pois, de acordo com Faulstich (2011, p.1), "reconhecemos que o léxico tem por objeto a unidade lexical, designada termo, em terminologia, lexema, em lexicologia, e lema em lexicografia". Ainda segundo a autora, o léxico é o espaço no qual se interpretam fenômenos linguísticos, considerando a dimensão do escopo conceitual, no qual o que caracteriza o termo é a atribuição de certos conceitos a uma forma lexical, de tal maneira que o termo se insere numa ontologia e num universo de discurso específico.

Logo, podemos entender que o léxico terminológico, diferentemente do léxico lexical, ou do léxico lexicográfico, apesar de se sobreporem, trata de uma unidade de características linguísticas comuns às das palavras da língua comum, utilizada em um domínio temático. É o termo especializado e utilizado em áreas técnicas, um conjunto de palavras técnicas referentes a uma ciência, atividade profissional, ou grupo social. Diante dessa perspectiva, importa-nos nesta dissertação enfatizar o estudo do léxico terminológico focado nos termos de crimes cibernéticos.

Segundo Faulstich (2012, p. 1), termo é uma "palavra simples, palavra composta, símbolo ou fórmula que designam os conceitos das áreas especializadas do conhecimento e do saber. Também unidade terminológica.". Com base nessa definição, o termo é uma forma linguística capaz de representar uma dada noção numa área de conhecimento específica. Dessa forma, os termos que designam crimes cibernéticos constituem léxico especializado utilizado em área técnica.

Entendemos que um termo ou unidade terminológica em uma linguagem de especialidade se distinguiria, portanto, de uma palavra do léxico comum devido à relação singular estabelecida com um conceito especializado dentro de uma área do conhecimento

técnico ou científico.

Podemos verificar que as definições citadas se encontram em harmonia teórica, uma vez que o termo se refere à palavra como unidade linguística significativa que designa os conceitos de áreas do conhecimento específico. Essa linha conceitual aplica-se às unidades provenientes do caso de crimes cibernéticos, visto que se referem a unicamente de unidades que designam especificamente delitos cometidos exclusivamente em ambiente cibernético.

Desenvolvemos então uma proposta de estudos capaz de analisar unidades terminológicas selecionadas referentes a crimes cibernéticos, considerando a ênfase na relação atualmente estabelecida entre linguagem, interfaces tecnológicas do ciberespaço e crimes, dentro de uma perspectiva terminológica.

## 2.2 Procedimentos metodológicos

As pesquisas normalmente apresentam particularidades de metodologia e recursos investigativos. Conforme a natureza do trabalho e a área em que se enquadra, faz-se necessário estabelecer a aplicação de um método e uma maneira de proceder para que seja possível alcançar um determinado fim. A esse respeito, Viegas (1999, p. 141) afirma que: "O pesquisador precisa decidir-se pelos métodos mais adequados ao assunto, identificar o universo, definir e dimensionar a amostra e selecionar as técnicas mais apropriadas para a obtenção dos dados".

Os dados que integram as definições para os crimes praticados em ambiente cibernético provêm de diferentes áreas do saber, como informática, tecnologia, comunicação social, computação e direito. Dessarte, compomos uma área particular do conhecimento de forma diversificada, mas que pode contar com conceitos e técnicas próprias que reúnam os dados em uma macroárea do saber.

Os procedimentos metodológicos utilizados para a elaboração desta dissertação possuem caráter qualitativo e descritivo, que buscam identificar os fenômenos específicos da terminologia aplicada acerca de crimes cibernéticos. Adotamos o método descritivo-analítico para apresentar as características dos fenômenos, além de explicar os procedimentos adotados para o tratamento dos dados encontrados, a fim de satisfazer as necessidades científicas e linguísticas da pesquisa.

Inicialmente, tendo delimitado o objeto de estudo, as primeiras decisões tomadas quanto ao procedimento metodológico foram:

i) selecionar e organizar o corpus de análise;

ii) analisar o corpus;

iii) recolher os dados a partir do corpus de análise;

iv) analisar dos dados recolhidos;

v) elaborar o glossário.

Nas subseções subsequentes, descrevemos os procedimentos metodológicos empregados.

### 2.3 Seleção do corpus

A escolha das fontes de dados que compõem o corpus de análise e que servem para a coleta dos termos referentes à área do conhecimento a ser estudado foi uma etapa muito importante na elaboração desta pesquisa. Para tanto, selecionamos alguns tipos de fontes para compor o corpus de análise como instrumento metodológico para a coleta de dados, a saber:

- **Leis:** legislação específica existente no Brasil que trata da área de crimes cibernéticos. São documentos que regulamentam o assunto com vistas à normatização. Escolhemos tais fontes para compor o corpus por se tratar de fonte de documentação e registro formal de termos. Todas estão disponíveis no Diário Oficial da União e constam com o texto na íntegra na seção de Anexos desta dissertação. Estudamos, portanto:

- Lei nº 12.965, de 23 de abril de 2014, também conhecida como o Marco Civil da Internet, que regula o uso da Internet no Brasil;

- Lei nº 12.735, de 30 de novembro de 2012, tipifica condutas realizadas mediante uso de sistema digital ou similares, que sejam praticadas contra sistemas informatizados e similares, e dá outras providências;

- Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de condutas cometidas na internet.

- **Cartilha de segurança para a Internet**: documento publicado pelo Comitê Gestor da Internet no Brasil (2012) divulga informações com recomendações sobre como o internauta pode se comportar a fim de aumentar a sua segurança e se proteger de possíveis ameaças na Internet. O documento apresenta diversos termos e conceitos utilizados na Internet, aborda os riscos de uso dessa tecnologia, além de fornecer dicas e cuidados a serem tomados. A cartilha serviu para que muitas definições fossem elaboradas de acordo com o conteúdo técnico apresentado.

Todo esse material serviu de ponto de partida para a composição de campos e subcampos terminológicos, cujos itens serão discutidos no Capítulo 3.

## 2.4 Metodologia para análise do corpus e recolha de dados

Após essa primeira fase acima descrita, a definição e organização do conjunto de documentos que servem de base para a descrição do nosso assunto, partimos para a coleta de dados, o estudo e análise.

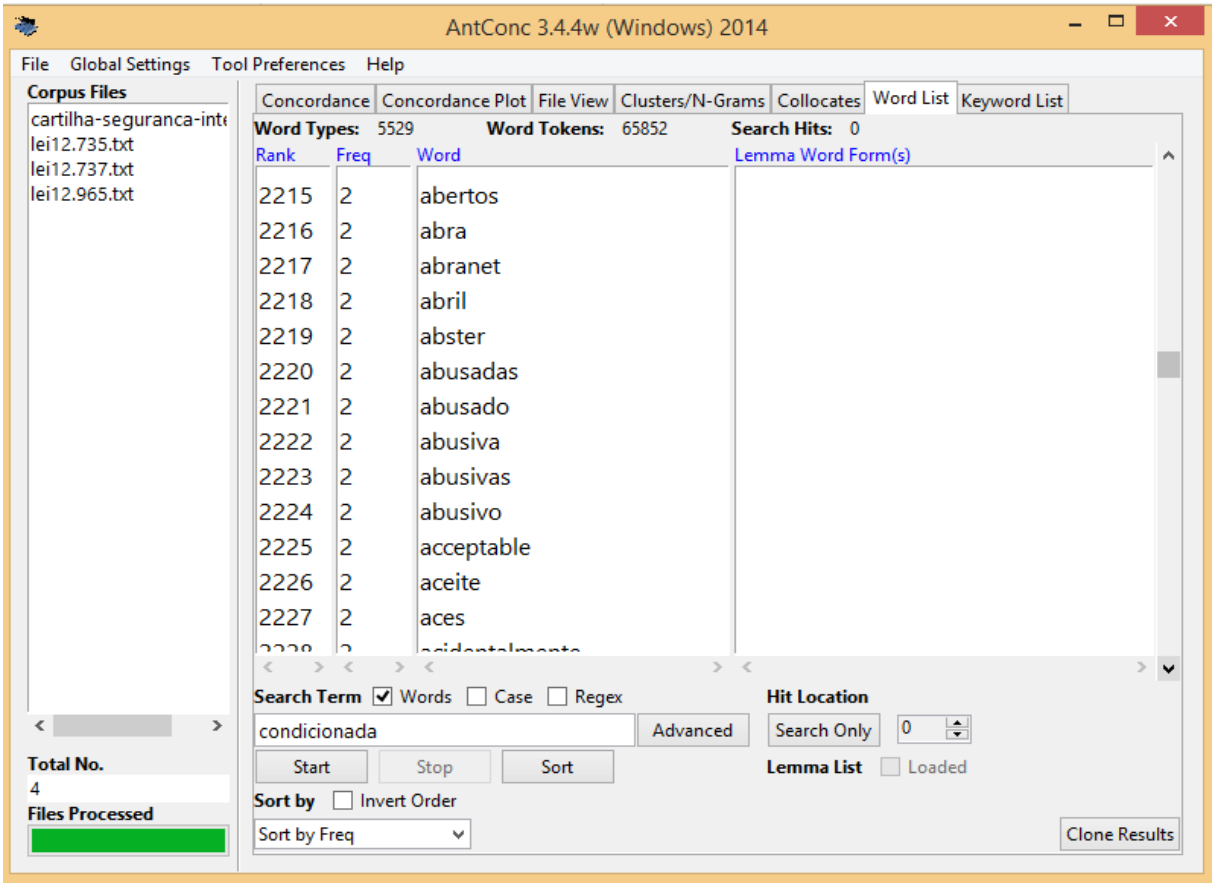
A recolha de unidades terminológicas foi feita a partir dos textos da Lei nº 12.965, de 23 de abril de 2014, Lei nº 12.735, de 30 de novembro de 2012, Lei nº 12.737, de 30 de novembro de 2012, Cartilha de Segurança para a Internet. Utilizamos os seguintes requisitos para a coleta: termos que especificam crimes cibernéticos e termos referentes aos agentes desses crimes.

Utilizamos o *software* AntConc para a recolha das unidades terminológicas. Esse programa é uma ferramenta disponível gratuitamente para download na Internet. O AntCont identifica automaticamente todas as palavras de um corpus e a frequência dessas palavras, além de verificar o contexto de uso dentro dos textos selecionados.

Para que esse trabalho fosse possível, foi necessário realizar a conversão dos documentos que estavam disponíveis em formato .PDF para a extensão .WORD, e em seguida transformá-los para a extensão .TXT, por ser o único formato de arquivo que o programa AntConc reconhece.

Apresentamos na figura a seguir o funcionamento do *software* AntConc:

**Figura 2** – Funcionamento do programa AntConc




Fonte: Justiniano (2015)

Ao observar a figura acima, notamos que, no campo *Corpus Files* estão carregados os quatro arquivos que compõem o corpus de análise, todos em formato .TXT. O campo *Word List* apresenta uma lista com colunas em que é possível ver número de palavras, o número da frequência, e quais são as palavras. O campo *Word Types* mostra o número total de palavras diferentes encontradas pelo programa dentro do texto dos arquivos carregados, somando ao todo 5.529.

Logo em seguida, para exemplificar alguns dados exportados da lista gerada pelo programa, apresentamos o Quadro 1, que contém uma amostra de UTs reconhecidas pelo AntConc e sua frequência no corpus de análise:

**Quadro 1** – Amostra da frequência de UTs reconhecidas pelo Antconc.

| UTs | Frequência |
|---|---|
| Defacement | 5 |
| Defacer | 2 |
| Fraude | 15 |
| Furto de dados | 3 |
| Furto de identidade | 13 |
| Golpe | 19 |
| Invadir | 9 |
| Phishing | 32 |
| Pornografia infantil | 1 |

Fonte: Justiniano (2015)

Durante a nossa atividade de pesquisa, o estudo dos termos empregados para crimes cibernéticos revelou-se muito rico em técnicas. Como podemos ver no quadro acima apresentado, os termos defacement, defacer, phishing, por exemplo, são de unidades terminológicas específicas de uma área altamente técnica. Os termos fraude, furto de dados, furto de identidade, golpe, invadir, são exemplos de termos que denotam crimes, encontrados no material analisado.

### 2.4.1 Recolha de novos dados

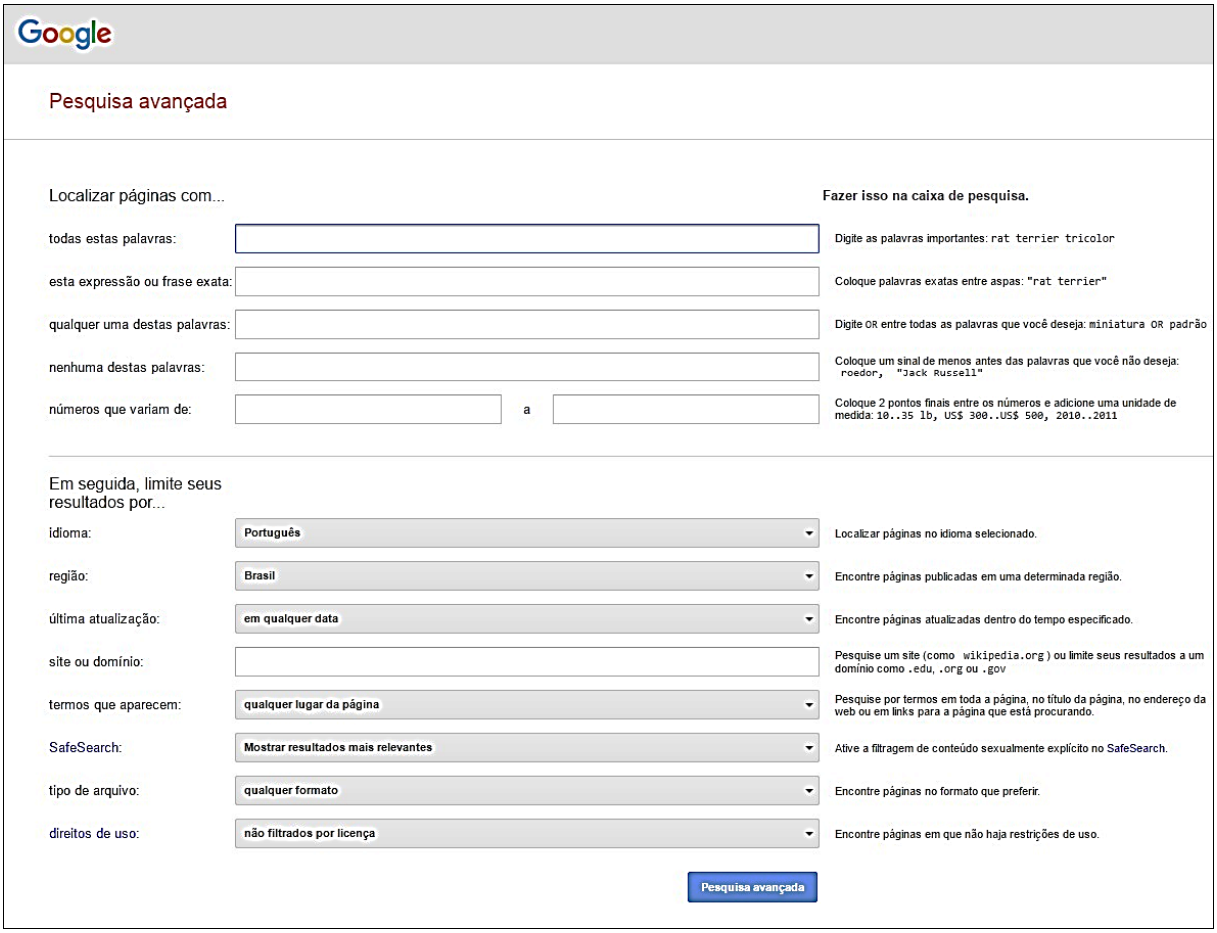
Frequentemente, nós nos deparamos com nomenclaturas desconhecidas, em sua maioria muitas novas e recentes, razão da difícil compreensão dessas nomenclaturas.

Para nossa surpresa, só foi encontrada uma única unidade terminológica que realmente designa um delito a respeito de crimes cibernéticos em toda a legislação brasileira, a saber: "invasão de dispositivo informático". Todos os demais tipos de crimes e seus agentes não são especificados nas leis. Encontramos uma simples e diminuta relação de termos na Cartilha de Segurança da Internet.

Tal fato nos conduziu a uma segunda recolha de dados, dessa vez na própria Internet, visto que a pesquisa virtual pode complementar as tradicionais fontes de informação.

Prosseguimos, então, para uma busca maior e mais ativa, na tentativa de aumentar o repertório linguístico já alcançado, recuperar matérias não consideradas, além de completar e enriquecer os vocábulos já existentes. Para isso, utilizamos como ferramenta o site de pesquisa Google, realizando busca avançada. Refinamos a pesquisa utilizando o formulário de recursos de filtragem para obter resultados otimizados, conforme mostra a figura a seguir:

**Figura 3** – Pesquisa avançada Google




Fonte: Justiniano (2016)

A inclusão do método de pesquisa na Internet mostrou-se bastante eficaz, pois tivemos acesso a um imenso banco de dados composto por sites e blogs de conteúdo jurídico e direito virtual. Esse repertório foi útil na elaboração de algumas definições por apresentar especificações, posto que contém diversos textos da linguagem de especialidade que contempla crimes cibernéticos.

Faulstich (1993) destaca a relevância de considerar, durante o processo de recolha e seleção dos termos, as noções conceituais, os contextos e as definições que farão parte do instrumento lexical a ser elaborado, ressaltando também a necessidade de o terminológo

adquirir conhecimentos do campo do saber e de sua estrutura. Portanto, as fontes pesquisadas também foram muito úteis na construção e recuperação de conceitos, além da constatação das possíveis variações das unidades pesquisadas.

Por meio desse tipo de pesquisa, além de encontrar novos termos, foi possível verificar a frequência das UTs, e utilizar conteúdos na elaboração de algumas definições. Os resultados apresentados em forma de glossário, no Capítulo 4, resultam, portanto, dessa densa investigação, e da compilação dos diversos termos e vocábulos relacionados a crimes cibernéticos.

Abaixo, mostramos no Quadro 2, um exemplo de UT pesquisada na busca virtual avançada, suas variantes identificadas, além das frequências de ocorrência correspondentes.

**Quadro 2** – Frequência de UT em pesquisa avançada Google

| | **UT** | **Frequência aproximada** |
|---|---|---|
| | Crime cibernético | 85.200 |
| **Variantes** | Cibercrime | 86.700 |
| | Crime digital | 11.800 |
| | Crime eletrônico | 6.490 |
| | Crime informático | 2.530 |
| | Crime na Internet | 44.500 |
| | Crime virtual | 43.400 |
| | Delito informático | 1.080 |

Fonte: Justiniano (2016)

Para a unidade terminológica crime cibernético, encontramos 7 variantes após utilizar o formulário de busca avançada do site de pesquisa. Esse resultado foi muito positivo e animador para nós pois nas demais fontes que comporam o corpus, nenhuma delas havia aparecido. Podemos observar no Quadro 2 que algumas variantes apresentam uma frequência muito próxima, como crime na Internet com 44.500, e crime virtual com 43.100. Outras variantes que destoaram das demais devido ao seu baixo uso, como crime informático com apenas 2.530, e delito informático com 1.080. Ressaltamos que os valores são aproximados, pois no caso de pesquisa avançada o site não retorna

um número exato.

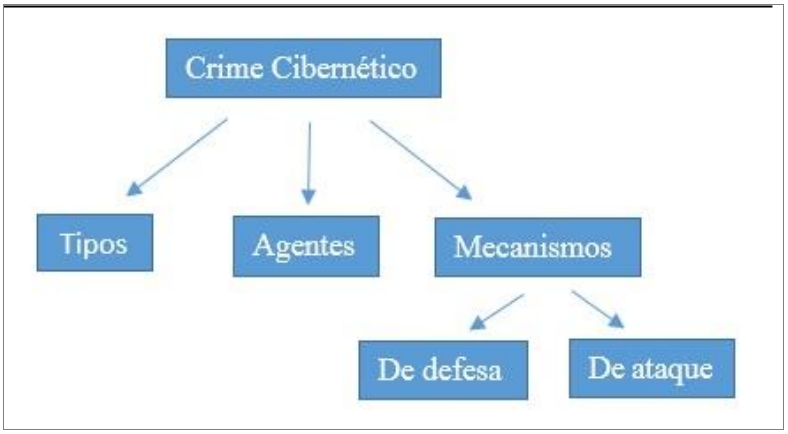
Como material de apoio, utilizamos o Dicionário Houaiss da Língua Portuguesa (2014) para verificar o registro dos termos pesquisados em dicionário de referência de língua comum. O resultado a que chegamos é que dos 80 itens terminológicos selecionados, apenas 9 estão dicionarizados. São eles: pirataria, pirataria informática, cracker, hacker, vírus, antivírus, backup, cópia de segurança, varredura. Ou seja, o equivalente a 11,25% dos termos estudados de crimes cibernéticos tem registro formal em dicionário de língua comum.

## 2.5 Análise de dados

Os dados extraídos foram inventariados e listados. Isso proporcionou a identificação de campos temáticos. Essa forma de organização permitiu analisar as UTs e distribui-las em áreas temáticas de acordo com suas características. Os dados foram então reorganizados dentro de suas respectivas classes, em ordem alfabética, conforme consta no Capítulo 4.

Segue abaixo o mapa conceitual que norteou a organização:

**Figura 4** – Campos temáticos




Fonte: Justiniano (2016)

De acordo com a figura acima, com relação a crimes cibernéticos, encontramos os três campos temáticos, a saber: Tipos, Agentes e Mecanismos. Dentro do campo Mecanismos, identificamos dois subcampos: mecanismos de defesa e mecanismos de ataque.

## 2.6 Metodologia para elaboração de glossário de crimes cibernéticos

Faulstich (1990, p.3) define: “Entendemos glossário como inventário terminológico, de caráter seletivo que tem como finalidade registrar e definir termos de domínios científicos, técnicos, ou culturais, independentemente do suporte material em que se apresenta”.

Nesse sentido, um glossário objetiva principalmente apresentar o significado das palavras utilizadas em determinada área técnica. Optamos por desenvolver o glossário de crimes cibernéticos seguindo um modelo de trabalho terminológico de natureza sistêmica. Isso significa que foi elaborado de modo que, durante sua consulta, seja possível compreender o significado de uma unidade terminológica quando relacionada a outra. Para alcançar esse efeito, segundo Faulstich (1993), o glossário deve apresentar a característica da remissão, que é “o processo de remeter a informação de um ponto a outro” (p. 174); e da remissiva, que se definida como “cada item léxico que, remetido, possui conteúdo semântico próprio” (p. 174).

A remissão no glossário funciona como um sistema de relação de complementaridade entre os termos (Faulstich, 2010, p. 182). A opção pelo modelo sistêmico para natureza do nosso glossário permite a organização e estruturação da obra de maneira remissiva, organizam, ampliando a compreensão dos conceitos expostos nas definições e facilitam o leitor a encontrar informações complementares e mais completas.

### 2.6.1 Fichas terminológicas para composição de verbetes para o glossário

Após a etapa de seleção e organização dos dados, o próximo passo foi adotar um modelo de ficha terminológica para registrar as informações de cada UT que serviu de base para a elaboração do glossário. O método aplicado para essa pesquisa seguiu o modelo de ficha terminológica desenvolvido por Faulstich (1995, p. 4), uma vez que “o registro do termo é feito numa ficha de terminologia a qual funciona como uma “certidão de nascimento”.

A ficha de terminologia tem campos mais ou menos fixos segundo a autora, e a seleção dos campos da ficha depende do tipo de repertório a ser elaborado. O modelo apresentado foi adaptado e é próprio para glossário sistêmico. A ficha terminológica utilizada para a composição dos verbetes desta pesquisa foi a seguinte:

**Quadro 3** – Modelo de ficha terminológica.

| FICHA TERMINOLÓGICA | |
|---|---|
| **1. Número** | |
| **2. Entrada** | |
| **3. Categoria gramatical** | |
| **4. Gênero** | |
| **5. Variante** | |
| **6. Sinônimo** | |
| **7. Definição** | |
| **8. Fonte da definição** | |
| **9. *Contexto** | |
| **10. *Fonte do Contexto** | |
| **11. *Nota** | |
| **12. *Fonte da nota** | |
| **13. Remissiva**<br>**a. Hiperônimo**<br>**b. Hipônimo** | |
| **14. Redator** | |
| **15. Data** | |

Fonte: Adaptado de FAULSTICH (1995, p. 28)

Para esclarecer o que significa as diferentes entradas da ficha terminológica, apresentamos as explicações dos campos de acordo com o estabelecido por Faulstich (2010, p. 180-183):

> **entrada** [ent.]: unidade linguística que possui conteúdo semântico da expressão terminológica na linguagem de especialidade. É o termo propriamente dito, o termo principal.
>
> **categoria gramatical** [cat.]: indicativo da classe gramatical ou da estruturação sintático-semântica do termo. Pode ser s. = substantivo ou n.=nome; v = verbo; utc = unidade terminológica complexa.
>
> **gênero** [gên.]: indicativo do gênero a que pertence o termo na língua descrita, como m = masculino ou f = feminino.
>
> **variante** [var.]: formas concorrentes com a entrada. As variantes correspondem a uma das alternativas de denominação para um mesmo referente.
>
> **sinônimo** [sin.]: formas coocorrentes no discurso da linguagem de especialidade cujo significado é idêntico ao do termo da entrada.

**definição** [def.]: a definição é um sistema de distinções recíprocas que servem para descrever conceitos pertinentes aos termos.

**fonte da definição** [font. def.]: registro do nome do autor, da obra, data etc. de onde foi compilada a definição.

**contexto** [cont.]: o contexto é um fragmento de texto no qual o tempo principal aparece registrado, transcrito com o fim de demonstrar como é usado na linguagem de especialidade.

**fonte do contexto** [font. cont.]: registro do autor, obra, data etc. de onde foi extraída a frase contextual, também chamada de abonação.

**remissivas**: sistema de relação de complementaridade entre termos. Os termos remissivos se relacionam de maneiras diversas, dependendo da contiguidade de sentido. Podem ser: termos hiperônimos e termos conexos, assim:

- hiperônimo [hiper.]: Termos cujo significado inclui o significado de outros, por isso é também chamado de termo genérico. Num dicionário ou glossário, o hiperônimo é, normalmente, a expressão léxica que inicia a definição.

- hipônimo [hip.]: Termo cujo significado representa uma subclasse em relação a um hiperônimo, por isso é também chamado de termo específico. Num dicionário ou glossário, o hipônimo é o termo que contribui na constituição do conteúdo da definição, por isso, pode haver mais de um [...]. A soma do conteúdo semântico do hiperônimo mais a do hipônimo delimita e distingue os conceitos na descrição do termo.

**nota**: comentário prático, linguístico ou enciclopédico, que serve para complementar as informações da definição.

**fonte da nota**: registro do autor, obra, data etc. de onde foi extraído o comentário prático, linguístico ou enciclopédico, que serve para complementações da definição.

Os campos marcados com o sinal de asterisco (*) nas fichas terminológicas são facultativos, podem ou não ser preenchidos. Como planejamos desenvolver um glossário sistêmico, fixamos o campo da remissiva, que se tornou obrigatório e deixou de ser opcional. Nem todos os campos que foram preenchidos aparecem no verbete, como Redator e Data, pois a ficha terminológica tem a intenção de registrar as informações de cada UT e servir de base para a elaboração do glossário.

A seguir, apresentamos o exemplo de ficha terminológica preenchida para a elaboração do verbete “crime cibernético”.

**Quadro 4** – Ficha terminológica do verbete crime cibernético

| **FICHA TERMINOLÓGICA** | |
|---|---|
| **1. Número** | **01** |
| **2. Entrada** | CRIME CIBERNÉTICO |
| **3. Categoria gramatical** | Nome (n.) |
| **4. Gênero** | Masculino (m.) |
| **5. Variante** | Crime virtual; crime digital; crime na internet; crime informático; crime eletrônico; delito informático, cibercrime. |
| **6. Sinônimo** | Crime virtual; crime digital; crime na internet; crime informático; crime eletrônico; delito informático, cibercrime. |
| **7. Definição** | Ato que utiliza o sistema informático para a prática de condutas ilícitas. |
| **8. Fonte da definição** | Adapt. SOUSA, S. S. (2016) |
| **9. *Contexto** | Esta CPI foi criada para investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade brasileiras. |
| **10.*Fonte do contexto** | CÂMARA DOS DEPUTADOS, 2016. |
| **11. *Nota** | Ø |
| **12. *Fonte da nota** | Ø |
| **11 Remissivas:**<br>a.Hiperônimo<br>b.Hipônimo | <br>a. Ø<br>b.Ver crime virtual; crime digital; crime na internet; crime informático; crime eletrônico; delito informático, cibercrime. |
| **12. Redator** | Nara Fernanda Justiniano (NFJ) |
| **13. Data** | 15/03/2015 |

Fonte: Justiniano (2015)

### 2.6.2 Modelo adotado para o verbete

A elaboração dos verbetes foi feita a partir das fichas terminológicas. Após o preenchimento das fichas**,** os verbetes do glossário apresentam uma estrutura padronizada do seguinte modo:

**Figura 5 –** Modelo adotado para o verbete

| |
|---|
| **entrada** + categoria gramatical + gênero + definição + fonte da definição ± contexto ± fonte do contexto ± nota ± fonte da nota ± remissiva |

Fonte: Justiniano (2015)

A estrutura da definição pragmática foi elaborada, principalmente, com base na proposição seguinte, de Faulstich (2014): o que é e para que serve? Explicando melhor, seria a preocupação em dizer o que é aquilo, ou seja, uma proposição de conteúdo que se exibe sob a representação de uma palavra. E também uma proposição funcional, sobre qual é a função, para que serve aquilo. Esquematizando o raciocínio, temos abaixo:

- Proposição funcional: Servir: uso/função (Qual é a função de X? Para que serve?)
- Proposição de conteúdo: Conter: inclui (O que X é / contém?)

### 2.6.3 Validação dos dados

Após a etapa de confecção das fichas terminológicas, o glossário foi montado e os verbetes foram submetidos ao parecer de um profissional especialista no assunto e que atua especificamente na área de crimes cibernéticos. Para tanto, entrevistamos o Delegado Chefe do Grupo de Repressão a Crimes Cibernéticos, da Superintendência Regional da Polícia Federal no Distrito Federal, Stênio Santos Sousa.

Esse profissional nos auxiliou na compreensão de conceitos específicos e de conhecimentos especializados da área pesquisada, contribuiu com valiosas informações e sugestões, e validou as definições contidas no trabalho terminográfico, produto desta dissertação.

Nesta pesquisa, a atuação do especialista foi uma característica fundamental para lapidar e interpretar os termos da melhor maneira possível para elaborar definições de acordo com o conteúdo técnico que os termos exigem.

# CAPÍTULO 3 – FENÔMENOS LINGUÍSTICOS NA CONSTITUIÇÃO DOS TERMOS

Após o processo de coleta de dados, seguindo a metodologia aplicada neste trabalho terminológico descrita no capítulo anterior, prosseguimos para a análise e interpretação dos termos. A análise também considerou os aspectos semânticos, pragmáticos, e metafóricos nos pilares de uma perspectiva de pesquisa qualitativa.

Estudamos os termos que compõem a terminologia referente aos crimes cibernéticos, visando à interpretação conceitual, de forma e de conteúdo, com vistas aos processos de formação dos itens terminológicos. Identificamos e compreendemos os fenômenos presentes para a formação dos termos, e chegamos a um corpus de 80 unidades terminológicas da área temática escolhida. Após a análise, pudemos então definir cada um dos termos e elaborar o glossário.

Assim sendo, este capítulo apresenta a análise dos dados, organizada da seguinte maneira:

1. análise das 80 unidades terminológicas, que foram recolhidas conforme expomos nos processos metodológicos;
2. identificação de UTCs, de acordo com pressupostos teóricos;
3. delimitação dos procedimentos linguísticos que regem as formações do conjunto de UTCs, de acordo com Faulstisch (2011);
4. exame da ocorrência de variantes, de acordo com o Constructo de Faulstich (2001), sobre variação terminológica.

## 3.1 Análise e interpretação de dados

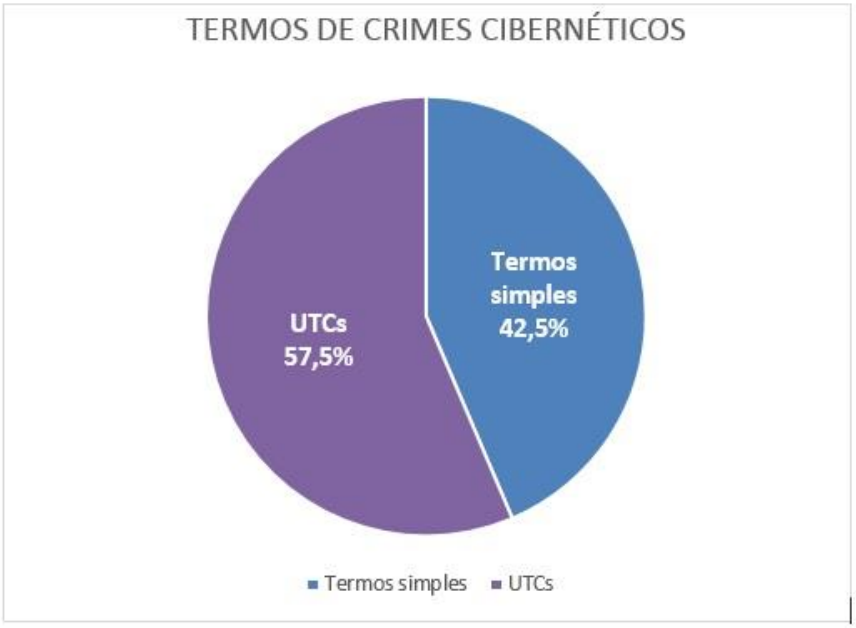
Observamos durante nossa investigação, que inventariou 80 termos, que todos são itens lexicais nominais, ou seja, 100%, não havendo ocorrência de outras categorias gramaticais. Trata-se da "nomeação" de crimes, o que é função primária dos nomes, ou expressões nominais. Sobre isso, Cabré (1993, p. 88) afirma que "em uma obra terminológica, a presença de nomes é quase exclusiva e a de verbos, adjetivos e locuções muito escassa". Nossa pesquisa entra em consonância com essa afirmativa, juntando-se a tantos outros trabalhos terminológicos, que seguem essa constatação, visto que são muito mais frequentes os itens lexicais nominais.

Faulstich (2011, p. 1) define unidade terminológica complexa, cuja sigla é UTC, da seguinte maneira:

> Combinação entre termos, segundo regras de lexicalização, para formar o conceito e possibilitar a elaboração da definição. Nota 1: A unidade terminológica complexa se compõe de formativos, organizados em uma sequência de base mais predicado, até que as combinações sucessivas atinjam a exaustão semântica. Nota 2: um termo atinge a exaustão semântica quando: i) é formulado de acordo com as regras da gramática da língua, ii) encera um conceito evidente; iii) proporciona que seja formulada uma definição.

De acordo com essa definição, do total de 80 itens terminológicos do corpus analisado, 46 são UTCs. Logo, o percentual de ocorrência equivalente às UTCs é de 57,5% do total. As demais 34 unidades terminológicas são termos simples, o que corresponde a 42,5% do total analisado. Nesta análise consideramos apenas uma casa decimal após a vírgula. Conforme o Gráfico 3:

**Gráfico 3** – Percentual de UTCs e termos simples




Fonte: Justiniano (2016)

Isso significa, em relação ao corpus, que a diferença de ocorrência entre termos simples e UTCs é próxima e equilibrada, não havendo grande disparidade ou predomínio entre os grupos na linguagem de especialidade de crimes cibernéticos. Para demonstrar a análise realizada, reunimos as UTCs no Grupo A, conforme apresentamos mais adiante.

### 3.1.1 Unidades terminológicas Complexas – UTCs

Os conceitos elaborados por Faulstich no que se refere a UTCs aplicam-se a este trabalho, visto que elucidam a situação de grande parte dos itens estudados, tais como: crime cibernético, invasão de dispositivo informático, roubo de identidade, dentre outros. Todos os itens que se enquadram como UTCs foram analisados em fichas terminológicas próprias, cujo modelo já apresentamos.

Ao falar de UTCs, consideramos primeiramente o Constructo Faulstich (2003). Nele é apresentado um conjunto de regras que tornam visíveis os padrões típicos de formação de UTCs. Podemos compreender os princípios que evidenciam a natureza morfológica, sintática e semântica dos formativos derivados, ao analisar a maneira como os argumentos operam e reoperam os conjuntos sintagmáticos antecedentes. O postulado estabelece que:

$$C = < T (F), LT, R >$$

Onde:

C = constructo;

T = terminologia;

F = formativo;

LT = fundo lexical terminológico;

R = regra

A fórmula apresentada acima representa que: o constructo C é igual à equação formada por terminologia (T), que se compõe de formativo (F). Um formativo terminológico pode ser ou um termo simples (F→A), ou predicado (AB, ABC, etc) (FAULSTICH, 2003, p.14). Desse modo, entendemos a unidade terminológica simples como (F→A) e a unidade terminológica complexa como (AB; ABC etc.).

De acordo com esse fundamento da formação dos termos de Faulstich (2003, p. 12), há regras que evidenciam a construção de uma UTC, que possui um contínuo conceitual que, segundo a autora, vai de base +geral a +específico, isto é, uma base genérica que recebe um significado mais específico atribuído pelo termo que lhe segue.

Dos nossos dados de pesquisa, podemos mencionar, por exemplo, o termo "invasão de dispositivo informático". Essa UTC é formada por uma base com conceito + geral, nesse caso "invasão", que sustenta outros predicados por meio de argumentos + específicos. A definição da UTC ocorre até o esgotamento semântico, conforme esquematizamos a seguir:

[ [ [furto] de identidade] virtual]

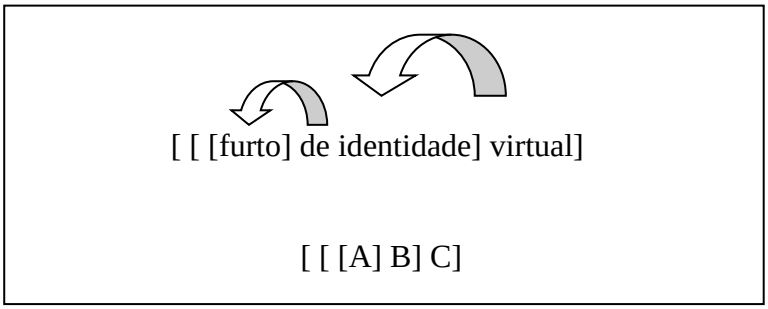
[ [ [ A ] B ] C ]

C = < T (F), LT, R > em que LT [A], F = {R} e R [F →ABC]

Outro fato importante a se considerar é que "no contínuo de uma UTC, os argumentos são reoperados do significado de cada conjunto sintagmático antecedente, com função de especificar, de tal forma que, no intervalo que vai do + geral ao + específico processa-se o novo conceito" (FAULSTICH, 2003, p. 15).

Logo abaixo, demonstramos o exemplo do processo de formação de uma UTC selecionada de termos de crimes cibernéticos, em que cada elemento composicional descreve a organização conceitual e atribui à base o caráter de um termo especializado. Por exemplo:

**Figura 6** – Processo de formação de UTC




Fonte: Justiniano (2016)

Esse exemplo, aplicado à luz do postulado de Faulstich (2003), evidencia que "a construção de terminologias complexas é um fenômeno que se dá num contínuo conceitual que vai do + geral ao + específico". Dessa forma, a base [furto], correspondente ao formativo A, é a unidade geral, que opera o conceito. O argumento [de identidade], correspondente ao formativo B, reopera o conceito + geral de A. O argumento [virtual], formativo C, influencia a base AB, conferindo o grau de especificidade almejada, fato que completa em um processo de cadeias derivadas o conceito na formação do termo.

Assim sendo, foi possível corroborar os princípios formulados por Faulstich, partindo da aplicação do constructo apresentado acima, no sentido de descrever a formação dos termos de crimes cibernéticos.

É preciso considerar que uma UTC se comporta como uma única unidade lexical, porque ocorre o processo de lexicalização, que é quando um lexema pode receber traços categoriais gramaticais e traços semânticos para compor uma nova unidade de discurso. A combinação entre categorias lexicais, na ordem do sintagma, por meio de traços contextuais específicos, como regência, concordância, adjetivo atributivo e outras idiossincrasias gramaticais de natureza fonológica, morfológica e semântica constitui também o processo de lexicalização.

Um exemplo de termo pesquisado em nossa dissertação que forma uma UTC é "crime cibernético", conforme mostramos a seguir:

"crime cibernético" = crime + cibernético.
[ [crime] cibernético]
[ [ A ] B ]

A combinação entre "crime" e "cibernético" resulta em uma única unidade lexical, porque há extensão conceitual do que tradicionalmente compreendemos como crime. O adjetivo cibernético, quando associado ao substantivo crime, afeta o entendimento do conceito, especificando-o com novas propriedades semânticas. Na sequência combinatória, o termo que entra à direita é um predicado do termo anterior e, no conjunto, compõe a unidade terminológica complexa.

O termo "golpe 419", variante de "fraude de antecipação de recursos" é especialmente interessante, pois apesar de "419" não ser um vocábulo e sim um número, configura-se como um formativo já que especifica e reopera a base "golpe" e comporta-se junto a ela como uma única unidade terminológica. O número 419 refere-se à seção do Código Penal da Nigéria sobre a "obtenção de bens sob falsas pretensões" equivalente ao artigo 171 do Código Penal Brasileiro, ou seja, crime de estelionato.

Os elementos formados por base + predicação correspondem às UTCs, que se apresentam, nos textos especializados, em uma sequência de caracteres entre espaços, com uma estrutura determinada, e com ordem fixa, representando um conceito específico, e comportando-se como uma única unidade terminológica. A UTC é composta por base mais predicação cuja elaboração se dá pela necessidade de especificidade do conceito, pertinente à linguagem de especialidade.

Identificamos, neste trabalho terminológico, 46 UTCs que, para fins de organização, reunimos no Grupo A, conforme apresentamos no quadro seguinte:

**Quadro 5** – Grupo A: UTCs encontradas no estudo de crimes cibernéticos

| GRUPO A: UTCs EM TERMOS DE CRIMES CIBERNÉTICOS | | | |
|---|---|---|---|
| 1 | assédio virtual | 24 | golpe nigeriano |
| 2 | advance fee fraud | 25 | golpe da Nigéria |
| 3 | assinatura digital | 26 | golpe 419 |
| 4 | boato virtual | 27 | interceptação de tráfego |
| 5 | cavalo de Troia | 28 | identify theht |
| 6 | código malicioso | 29 | invasão de dispositivo informático |
| 7 | cópia de segurança | 30 | noiva russa |
| 8 | crime cibernético | 31 | pedofilia na Internet |
| 9 | crime digital | 32 | pedofilia digital |
| 10 | crime eletrônico | 33 | pichação virtual |
| 11 | crime informático | 34 | perfil fake |
| 12 | crime na Internet | 35 | perfil falso |
| 13 | crime virtual | 36 | pichador virtual |
| 14 | delito informático | 37 | pirataria virtual |
| 15 | desfiguração de página | 38 | pirataria digital |
| 16 | drive-by pharming | 39 | pirataria informática |
| 17 | e-mail spoofing | 40 | pedofilia virtual |
| 18 | falsificação de e-mail | 41 | pornografia de vingança |
| 19 | falsa identidade | 42 | revenge porn |
| 20 | fraude de antecipação de recursos | 43 | roubo de identidade |
| 21 | fraude de identidade | 44 | scam romance |
| 22 | furto de identidade virtual | 45 | trojan horse |
| 23 | furto de identidade | 46 | vírus de computador |

Dos nossos dados de pesquisa, podemos observar que as 46 UTCs são formadas por uma base com conceito geral, que sustenta outros predicados por meio de argumentos + específicos, o que ocorre até o esgotamento semântico.

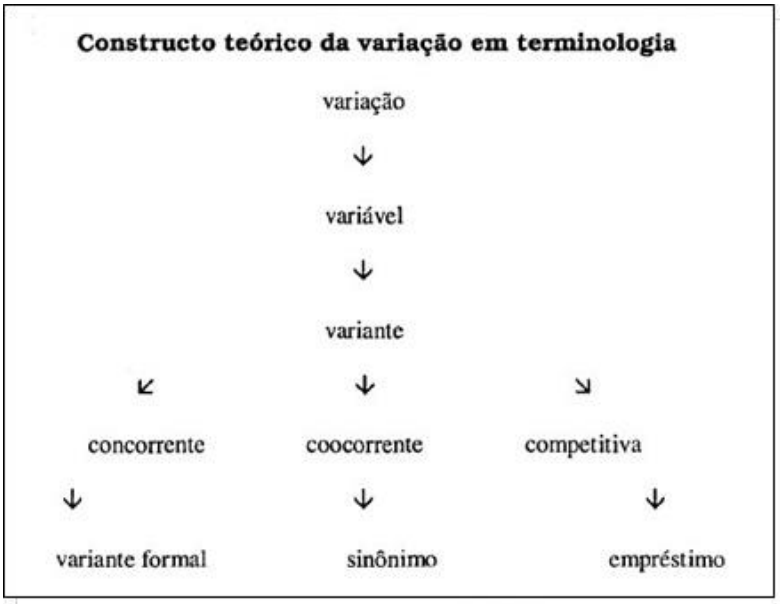
### 3.1.2 Variação terminológica: termos de crimes cibernéticos em uso

Os estudos terminológicos contemporâneos de Faulstich (2001, p. 25) mostram

os fundamentos teóricos que sustentam a questão da variação em terminologia. Para estudar os termos pesquisados e solucionar as questões de análise dos mesmos, adotamos tais pressupostos teóricos. Seus postulados apresentam a ideia de abandono do isomorfismo categórico entre termo-conceito-significado associado à aceitação de que, sendo a terminologia um fato de língua, acomoda elementos variáveis.

Na figura que segue, apresentamos o esquema gráfico do Constructo teórico da variação em terminologia, proposto por Faulstich (2001), no qual podemos visualizar a distribuição das categorias em concorrentes, coocorrentes e competitivas:

**Figura 7** – Constructo teórico da variação em terminologia




Fonte: Faulstich (2001, p. 26)

As definições e explanações acima são importantes, pois, em nossa pesquisa, identificamos diferentes fenômenos de variação dentre as unidades terminológicas selecionadas do contexto da linguagem empregada para designar crimes cibernéticos. No processo de investigação nos dados de pesquisa, constatamos a ocorrência de variantes coocorrentes na maioria dos termos, e alguns termos foram classificados como variantes competitivas.

A observação direta do uso dos termos de crimes cibernéticos ocorreu sob a perspectiva da teoria da variação em terminologia proposta por Faulstich (2001), que aplica-se ao nosso trabalho, pois privilegia o estudo do termo e do conceito com base na observação do uso e no registro social. Importa-nos, portanto, averiguar como ocorre a variação dos

termos de crimes cibernéticos.

Faulstich (2001, p.26) apresenta, as categorias de variantes dos termos, a saber: concorrentes, coocorrentes e competitivas. A autora define variantes concorrentes como:

> As variantes concorrentes são aquelas que podem concorrer entre si, e permanecer, como tais, no estrato, ou que podem concorrer para a mudança. Nessa condição, uma variante que concorre com outra ao mesmo tempo não ocupa o mesmo espaço, por causa da própria natureza da concorrência. Se uma variante está presente no plano discursivo, outra não aparece. São variantes formais. A variante formal é uma forma linguística ou forma exclusiva de registro que corresponde a uma das alternativas de denominação para um mesmo referente, podendo concorrer num contexto determinado.

Faulstich (2001, p.31) define variantes coocorrentes como:

> As variantes coocorrentes: são aquelas que têm duas ou mais denominações para um mesmo referente**.** Estas variantes têm por função fazer progredir o discurso e organizam, na mensagem, a coesão lexical. Entre variantes coocorrentes há compatibilidade semântica, uma vez que elas se equivalem no plano do conteúdo. As variantes coocorrentes formalizam a sinonímia terminológica. A sinonímia terminológica relaciona o sentido de dois ou mais termos com significados idênticos e podem coocorrer num mesmo contexto, sem que haja alteração no plano do conteúdo.

Detectamos a presença de variação coocorrente em nossa pesquisa. Um exemplo é o termo crime cibernético, que possui as variantes: crime virtual, crime digital, crime eletrônico, crime informático, crime na internet, cibercrime, delito informático. As variantes de crime cibernético se enquadram como variantes coocorrentes, pois são mais denominações para um mesmo referente.

Verificamos a compatibilidade semântica nesse caso de crimes cibernéticos e suas variantes coocorrentes, uma vez que fazem progredir o discurso dentro do texto, com equivalência no plano do contéudo. Não se trata de variantes concorrentes, pois a ocorrência delas não exclui a ocorrência dos seus equivalentes formais. Também não é o caso de variante competitiva, já que não se trata de empréstimos linguísticos. Crime virtual, crime digital, crime eletrônico, crime informático, crime na internet, cibercrime, delito informático aparecem nos textos técnicos como alternativas compatíveis para o termo crime cibernético.

Faulstich (2001, p.32) define variantes competitivas como:

> As variantes competitivas são aquelas que relacionam significados entre itens lexicais de línguas diferentes, quer dizer, itens lexicais de uma língua B preenchem lacunas de uma língua A. As variantes competitivas sofrem, em seu desempenho, intersecções, devido a própria natureza estrangeira da expressão. Esse fenômeno se dá quando a estrutura da língua do termo estrangeiro é perturbada por estruturas da língua vernacular, a mistura de

> formantes ativa a variação. As variantes competitivas formalizam os empréstimos linguísticos. Os empréstimos linguísticos são itens lexicais que se originam de língua estrangeira e, depois no contexto social da língua recebedora, se tornam variantes porque provocam o surgimento de uma forma vernacular equivalente, por causa do ambiente linguístico estranho à sua permanência natural. (p.32)

Também identificamos o tipo de variante competitiva, visto que relaciona itens lexicais de uma língua B para preeencherem lacunas de uma língua A. Exemplos de variantes competitivas, são: backup, *cyberbullying, fake, phishing*, entre outros.

Relacionamos, no quadro seguinte, os termos de crimes cibernéticos e suas variantes correspondentes:

**Quadro 6** – Variação terminológica em termos de crimes cibernéticos

| **VARIAÇÃO TERMINOLÓGICA** | |
|---|---|
| **Hiperônimo** | **Variantes** |
| backup | cópia de segurança |
| crime cibernético | crime virtual; crime digital; crime na internet; crime informático; crime eletrônico; delito informático, cibercrime. |
| Cyberbullying | Assédio virtual |
| defacement | desfiguração de página; deface; pichação virtual |
| defacer | pichador virtual |
| fake | perfil fake; perfil falso. |
| Fraude de antecipação de recursos | advance fee fraud |
| furto de identidade virtual | identify theht; falsa identidade; roubo de identidade; fraude de identidade |
| golpe da Nigéria | golpe nigeriano; golpe 419 |
| hoax | boato virtual |
| malware | código malicioso |
| pharming | drive-by pharming |
| pirataria | pirataria virtual; pirataria digital; pirataria informática |
| Pornografia de vingança | revenge porn |
| pedofilia virtual | pedofilia na Internet; pedofilia digital |
| pharming | drive-by pharming |
| phishing | phishing-scam; scam; furto de dados; roubo de senha. |

| | |
|---|---|
| spoofing | falsificação de e-mail; e-mail spoofing |
| scam romance | noiva russa |
| snniffing | interceptação de tráfego |
| tojan | cavalo de Troia; trojan horse |
| varredura | scan |
| vírus | vírus de computador |

Fonte: Justiniano (2016)

A análise do corpus ocorreu com o auxílio das regras de formação dos termos, adotando este consistente arcabouço teórico que considera os conceitos de variação terminológica envolvidos na área escolhida. Os fundamentos teóricos explanados neste capítulo foram cruciais e serviram de base para a identificação e compreensão do conjunto de termos recolhidos, os quais fazem parte do trabalho terminográfico.

### 3.1.3 Estrangeirismos

Um dos fenômenos linguísticos averiguados, que nos chamou a atenção, foi a presença maciça de termos do inglês para denominar crimes cibernéticos, mecanismos utilizados, e agentes envolvidos. Sobre esse assunto, Faraco (2001, p. 15) define estrangeirismo como:

> o emprego, na língua de uma comunidade, de elementos oriundos de outras línguas. No caso brasileiro, posto simplesmente seria o uso de palavras e expressões estrangeiras do português. Trata-se de fenômeno constante no contato entre comunidades linguísticas, também chamado de empréstimo.

Há ocorrências de estrangeirismos nos dados analisados, tais como: *backup, cyberbullying, fake, advance fee fraud, scam, firewall, worm*, entre outros. Alguns apresentam termos equivalentes em português, como "furto de dados" para *phishing*, ou "cópia de segurança" para backup, outros não, como *antimalware, worm,* hacker e cracker.

No fenômeno do estrangeirismo presente dos termos pesquisados, notamos que todos os termos estrangeiros são oriundos do inglês, configurando um estrangeirsimo específico, o anglicismo. Sobre isso, Faraco (2001, p. 21-22) afirma:

> A discussão atual contra os estrangeirismos se concentra no uso de elementos do inglês: os anglicismos. Por um lado, há os termos da tecnologia e da pesquisa, desenvolvida e registrada quase hegemonicamente nessa língua. De outro lado, há o universo dos negócios.

Como apresentado no Capítulo 1 desta pesquisa, sabemos que grande parte da tecnologia que compõe o ciberespaço e que compõe a terminologia de crimes cibernéticos foi

elaborada e é proveniente do inglês dos Estados Unidos da América. Todo tipo de nova tecnologia que é importada desse país para o Brasil vem naturalmente acompanhada de seu nome de origem. Porém, a cada termo anglo que entra no país não se pode garantir que surgirá um correspondente no português do Brasil.

A respeito da questão da hegemonia do inglês no domínio de termos de tecnologias, Duran (2004, p. 15) afirma que existem variações translinguísticas de vocabulário entre as diversas línguas. Isso seria o equivalente a dizer que as diferenças averiguadas nas diversas línguas se referem às diferentes visões de uma mesma realidade, que podemos considerar também como variação. Para isso, Duran (2004, p.26) utiliza o interessante exemplo do "vocabulário esquimó", estudo que investigou se os esquimós teriam centenas de palavras para designar a neve.

Nesse caso, quando toda uma cultura é perita e especialista em um domínio específico, como os esquimós são a respeito da neve, a língua terá um léxico apropriadamente amplo. Isso é conhecido como algo culturalmente específico. Esquimós realmente têm uma riqueza de distinções terminológicas para se referir à neve. Essa riqueza parece natural, já que em muito do tempo de suas vidas, esse povo passa na neve.

Não é incomum observar que qualquer sociedade que tem uma especialização em alguma experiência de domínio apresenta necessariamente um grande vocabulário nesse domínio. O oposto também é verdadeiro: as pessoas que vivem em uma área onde a neve é rara têm poucos ou mesmo um único termo sobre a esse fenômeno natural. Sociedades sem acesso à Internet como tecnologia praticamente não apresentam termos de crimes cibernéticos.

Os norte-americanos são pioneiros nos estudos, descobertas e criação de tecnologias informáticas, e até hoje se destacam, trazendo constantes inovações na área. O inglês é uma língua que acumulou grande diversidade de termos em vários domínios da realidade, inclusive no que tange a ciberespaço e crimes cibernéticos, o que justifica a presença maciça de estrangeirismos nos termos na linguagem de especialidade de crimes cibernéticos.

# CAPÍTULO 4
# GLOSSÁRIO DE CRIMES CIBERNÉTICOS

## 5.1 Apresentação

Elaboramos o **Glossário de crimes cibernéticos** seguindo uma organização metodológica e observando fundamentos teóricos, expostos nos capítulos anteriores. O Glossário compõe-se de 80 verbetes descritivos, organizados em quatro áreas temáticas, a saber: tipos de crimes, agentes envolvidos, mecanismos de ataque, e defesa.

Primeiramente, explicamos os aspectos macroestruturais de como foi estruturado o glossário, e expomos informações importantes sobre como consultá-lo nos aspectos microestruturais. Em seguida, apresentamos os verbetes organizados em ordem alfabética.

O público-alvo do presente trabalho são os delegados e policiais investigadores de crimes cibernéticos, analistas e técnicos em informática, profissionais de segurança da informação, *designers* e engenheiros de computação, professores e alunos de cursos de informática, ciências e engenharia da computação. Outras pessoas que porventura se interessem pelo tema também são usuários em potencial do Glossário.

Como produto final, o Glossário de termos de crimes cibernéticos será disponibilizado no site do Centro de Estudos Lexicais e Terminológicos, <http://www.centrolexterm.com.br/>, como uma via de divulgação e socialização do conhecimento produzido, onde estará mais facilmente acessível para aqueles que se interessarem em consultar a obra.

Esperamos que este glossário se torne uma ferramenta de consulta e aplicação, visto que a terminologia aqui descrita é um instrumento linguístico que, ao relacionar Internet, ciberespaço, segurança, e cidadania, contempla a política linguística, a internacionalização da língua portuguesa, e serve de ponto de partida para novas pesquisas terminográficas.

## 5.2 Macroestrutura do glossário

Descrevemos logo abaixo os passos seguidos para a composição do glossário.

### 5.2.1 Metodologia do Plano de Trabalho

Primeiramente, os dados para a constituição dessa terminologia foram extraídos da legislação do tema existente no Brasil, a saber: Lei nº 12.965, de 23 de abril de 2014, também conhecida como o Marco Civil da Internet, Lei nº 12.735, de 30 de novembro de 2012, e Lei nº 12.737, de 30 de novembro de 2012. Além disso, consultamos a Cartilha de segurança para a Internet, publicada pelo Comitê Gestor da Internet no Brasil (2012), como literatura especializada; e foi utilizada a ferramenta de pesquisa avançada no site de busca Google.

O segundo passo foi inventariar com a ajuda do programa AntCont, e em seguida registrar os termos preenchendo as fichas terminológicas.

Adotamos uma postura de trabalho descritivo para o tratamento dos termos, ou seja, o termo deveria ser descrito, e não prescrito. Essa atitude ocorreu a partir do viés sociterminológico, observando o emprego do termo no discurso escrito e oral. Verificou-se também necessidade de suprir níveis de variações linguísticas nos termos, levando-se em consideração a pragmática linguística.

O último passo foi a redação do repertório terminológico que atenda às necessidades linguísticas do público-alvo, registrando os termos em um glossário sistêmico, uma vez que o mesmo apresenta rede de remissivas. Por fim, analisamos globalmente o repertório, ajustando alguns verbetes, que se mostrou próprio de um glossário de termos, no caso, um glossário de crimes cibernéticos.

### 5.2.2 Consultoria especializada

Consultamos um especialista no campo do conhecimento da área para validar os termos. Contamos com a colaboração de um especialista que, no nosso entendimento, por se tratar de crimes cibernéticos, foi o chefe delegado especialista do Grupo de Repressão a Crimes Cibernéticos da Polícia Federal. Realizamos entrevista, em anexo, com consultor com aplicação de questionário, e os verbetes foram submetidos ao parecer e análise desse profissional, que atua especificamente na área de crimes cibernéticos.

## 5.3 Microestrutura do glossário

Descrevemos logo em seguida a estrutura interna de composição do glossário.

### 5.3.1 Campos temáticos

A terminologia coletada, descrita e organizada foi analisada, e de acordo com a natureza técnica dos termos, foi dividida em 4 campos temáticos: Tipo de crimes cibernéticos, Agentes, Mecanismos de ataque, e Mecanismos de defesa. O termo “crime cibernético” e suas variantes abrem o glossário e porque é o tema central, e aparecem sem categoria por serem o cerne da questão.

### 5.3.2 Estrutura do verbete do glossário

Organizamos os verbetes em ordem alfabética, apresentando a seguinte estrutura padronizada:

| |
|---|
| entrada + categoria gramatical + gênero + definição + fonte da definição + contexto ± fonte do contexto ± nota ± fonte da nota ± remissiva |

Os campos onde constam com o sinal "+" são áreas de informações básicas na composição do verbete, ou seja, são campos definidos e de preenchimento obrigatório. O sinal "±" significa "quando houver", ou seja, os campos assinalados dessa forma podem compor ou não o verbete. Devemos esclarecer o que significado de cada campo:

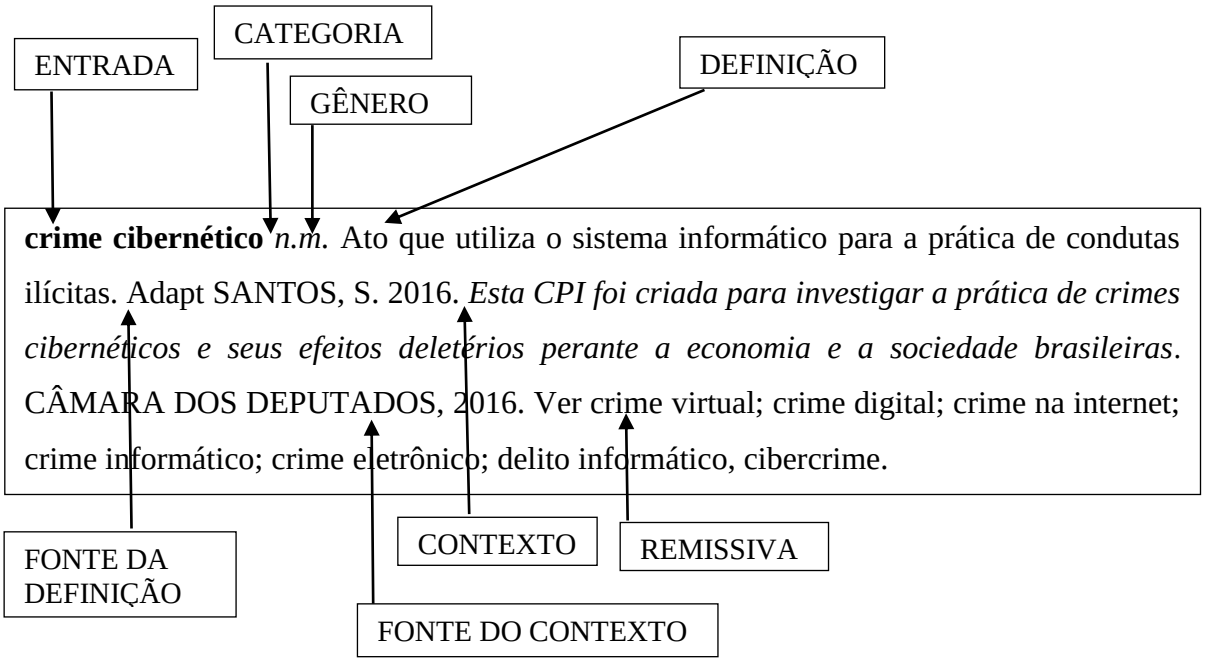
- entrada: aparece, sempre, com todas as letras em minúsculas, e em negrito, seguida da informação gramatical. É o termo propriamente dito, possui o conteúdo semântico da expressão terminológica na linguagem de especialidade.
- categoria gramatical: aparece sempre em itálico e caixa baixa. É o indicativo da categoria na gramática da língua a que pertence o termo, ou da estruturação sintático-semântica do termo. Indicado por *n.* = nome.
- gênero: aparece em itálico logo após a indicação da categoria gramatical. Pode ser *m.* = masculino ou *f.* = feminino. Indica o gênero a que pertence o termo na língua descrita.
- definição: aparece com a primeira letra em maiúscula. É o indicativo do(s) conceito(s) pertinente(s) aos termos. Adotamos o tipo de definição pragmática com as proposições o que é? e para que serve?
- fonte da definição: é o registro do nome do autor, da obra, data etc. de onde foi compilada a definição. Aparece após a definição, e quando for o caso, apresenta a abreviatura Adapt., indicando que a definição foi adaptada em benefício da descrição.
- contexto: fragmento de texto marcado em itálico, no qual o verbete aparece registrado, com o fim de demonstrar como é usado na prática da linguagem de especialidade.
- fonte do contexto: é o registro do nome do autor, da obra, data etc. de onde foi extraída a frase contextual. Aparece após a definição, e quando for o caso, apresenta a abreviatura Adapt., indicando que a definição foi adaptada em benefício da descrição.
- nota: é o comentário prático, linguístico ou enciclopédico, que serve para complementar as informações da definição.
- fonte da nota: é o registro do nome do autor, da obra, data etc. de onde foi extraído o

comentário prático, linguístico ou enciclopédico, de complementação da definição. Quando for o caso, apresenta a abreviatura Adapt., indicando que foi adaptada em benefício da descrição. Registro do autor, obra, data etc. de onde foi extraído.

- remissiva: aparece precedida de 'Ver', podendo ser hiperônimos, hipônimos (sinônimos, variantes) e termos conexos. São termos que se relacionam de maneiras diversas com o verbete estabelecendo uma relação de complementariedade.

A seguir, apresentamos um modelo de verbete estruturado:

**Figura 8** – Modelo de verbete estruturado




Fonte: Justiniano (2016)

### 5.3.3 Lista de abreviações

Adapt. ..... Adaptado

*n.* ..... nome

*f.* ..... feminino

*m.* ..... masculino

## 5.4 Os verbetes

**cibercrime** *n.m.* Ver crime cibernético.

**crime cibernético** *n.m.* Ato que utiliza o sistema informático para a prática de condutas ilícitas. Adapt SANTOS, S. 2016. *Esta CPI foi criada para investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade brasileiras.* CÂMARA DOS DEPUTADOS, 2016. Ver cibercrime; crime digital; crime eletrônico; crime informático; crime na internet; crime virtual; delito informático.

**crime digital** *n.m.* Ver crime cibernético.

**crime eletrônico** *n.m.* Ver crime cibernético.

**crime informático** *n.m.* Ver crime cibernético.

**crime na Internet** *n.m.* Ver crime cibernético.

**crime virtual** *n.m.* Ver crime cibernético.

**delito informático** *n.m.* Ver crime cibernético.

## TIPOS DE CRIME CIBERNÉTICO

**advance fee fraud** *n.m.* Ver fraude de antecipação de recursos.

**assédio virtual** *n.m.* Ver cyberbullying.

**cyberbullying** *n.m.* Ato que utiliza o uso do sistema informático para agressões verbais e/ou violência psicológica praticado por um indivíduo ou grupo de indivíduos com a intenção de agredir moralmente, ameaçar ou constranger outra pessoa. Adapt. De CYBERBULLYING, 2016. *Muitas vezes as vítimas do cyberbullying não denunciam por medo de represálias de seus agressores.* CYBERBULLYING, 2016. Ver assédio virtual; cyberbully.

**deface** *n.m.* Ver defacement.

**defacement** *n.m.* Ato que utiliza o sistema informático para modificar sem permissão o conteúdo ou danificar a aparência de uma página de um domínio da internet, geralmente com cunho político ou ideológico. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *O grupo ativistas Anonymous usou defacement para protestar contra a Copa do Mundo no Brasil publicando as mensagens #Fifagohome #nãovaitercopa #Opboicoteacopa em sites do governo e empresas patrocinadoras do evento*. R7, 2013. Ver desfiguração de página; deface; pichação virtual.

**desfiguração de página** *n.f.* Ver defacement.

**drive-by pharming** *n.m.* Ver pharming.

**e-mail spoofing** *n.m* Ver spoofing.

**falsa identidade** *n.f.* Ver furto de identidade virtual.

**falsificação de e-mail** *n.f.* Ver spoofing.

**fraude de antecipação de recursos** *n.f.* Crime de estelionato que utiliza o sistema informático para induzir uma pessoa a fornecer informações confidenciais, realizar pagamento adiantado, ou depositar dinheiro, com a promessa receber algum benefício futuro. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *A fraude de antecipação de recursos possui diversas variações que, apresentam diferentes discursos mas assemelham-se pela forma de aplicação e pelo objetivo de conseguir dinheiro, como: loteria internacional, crédito fácil, doação de animais, oferta de emprego.* Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver advance fee fraud; golpe da Nigéria; scam romance.

**fraude de identidade** *n.f.* Ver furto de identidade virtual.

**furto de identidade virtual** *n.m.* Crime de falsa identidade onde uma pessoa utiliza o sistema informático para se passar por outra. Adapt. de CARTILHA DE SEGURANÇA PARA

INTERNET, 2012. Ver identify theht; furto de identidade; falsa identidade; roubo de identidade; fraude de identidade.

**furto de identidade** *n.m.* Ver furto de identidade virtual.

**golpe da Nigéria** *n.m.* Modalidade de fraude de antecipação de recursos. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Nota: Também conhecido como "Nigerian 4-1-9 Scam". O número 419 refere-se à seção do Código Penal da Nigéria sobre a "obtenção de bens sob falsas pretensões" equivalente ao artigo 171 do Código Penal Brasileiro, ou seja, crime de estelionato. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *O FBI criou uma unidade especial para investigar esse tipo de crime nos Estados Unidos, onde um nigeriano convenceu pessoas a doarem US$ 1,3 milhão. Ao explicar o que leva pessoas instruídas a cair no golpe da Nigéria, policiais apontam a cobiça pelo dinheiro fácil como fator preponderante.* ISTOÉ, 2016. Ver fraude de antecipação de recursos; golpe nigeriano; golpe 419.

**golpe nigeriano** *n.m.* Ver golpe da Nigéria.

**golpe 419** *n.m.* Ver golpe da Nigéria.

**identify theht** *n.m.* Ver furto de identidade virtual.

**invasão de dispositivo informático** *n.f.* Ato de 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, podendo resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, ou o controle remoto não autorizado do dispositivo invadido. Adapt. de LEI 12.737/12. *A nova lei trata de invasão de dispositivo informático, fato da vida moderna que vinha gerando insegurança e intranquilidade nas relações e merecia a atenção do legislador*. ESTADÃO, 2013.

**noiva russa** *n.f.* Ver scam romance; crime cibernético.

**pedofilia virtual** *n.f.* Crime de pedofilia que utiliza o sistema informático para apresentar, obter, trocar, produzir, disponibilizar, vender, fornecer, divulgar, arquivar, transmitir, ou publicar, fotografia, vídeo,imagem, ou outro registro que contenha pornografia, ou cenas de sexo explícito envolvendo criança ou adolescente. Adapt. de ECA, 2008. *A pedofilia virtual transcende fronteiras e as leis variam muito de país para país, enfrentar o problema requer, no lugar de armamento sofisticado, conhecimento técnico, contribuição por parte dos provedores para bloquear sites criminosos e, acima de tudo, a colaboração de todos.* ISTOÉ, 2004. Ver pedofilia na Internet; pedofilia digital.

**pedofilia na Internet** *n.f.* Ver pedofilia virtual

**pedofilia digital** *n.f.* Ver pedofilia digital

**pharming** *n.m.* Modalidade de phishing que utiliza o sistema informático para redirecionar a navegação do usuário para sites falsos sem o seu conhecimento. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *Para prevenir o pharming, caso o site de comercio eletrônico ou Internet Banking que você está acessando não utilize conexão segura desconfie imediatamente.* Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver phishing; drive-by pharming.

**pharming** *n.m* Ato que utiliza o sistema informático para redirecionar a navegação do usuário de um site legítimo para um site falso ou página falsa. Ver drive-by pharming

**phishing** *n.m.* Ato que utiliza o sistema informático para obter dados pessoais de diversos tipos, como: senhas, dados financeiros, número de cartões de crédito, entre outras informações de um usuário. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *Seja cuidadoso ao acessar a página de seu webmail para não ser vítima de phishing.* CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Nota: Do inglês “fishing”, vem de uma analogia criada pelos fraudadores, onde “iscas” (mensagens eletrônicas) são usadas para “pescar” informações de usuários da Internet. CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver phishing-scam; scam; furto de dados; roubo de senha.

**phishing-scam** *n.m.* Ver phishing.

**pirataria** *n.f.* Crime de violação de direito autoral que utiliza o sistema informático caracterizado pelo download de material protegido por propriedade intelectual, como músicas, filmes e softwares, para cópia, reprodução, distribuição, gratuita ou cobrada, sem a autorização do proprietário. Adapt. de BRASIL ESCOLA, 2016. *A Interpol considera a pirataria o crime do século. A Associação Brasileira das Empresas de Software (Abes) divulgou que, em 2008, somente no DF, a pirataria causou um prejuízo de R$ 121 milhões ao setor de softwares. É crime, mas muita gente aceita, não vê problema em levar para casa CD ou DVD pirata, por exemplo.* CORREIO BRAZILIENSE, 2010. Ver pirataria virtual; pirataria digital; pirataria informática.

**pirataria digital** *n.f.* Ver pirataria

**pirataria virtual** *n.f.* Ver pirataria

**pirataria informática** *n.f.* Ver pirataria

**pichação virtual** *n.f.* Ver Defacement

**pornografia de vingança** *n.f.* Ato que utiliza o sistema informático para divulgar fotos ou vídeos de conteúdo íntimo ou sensual de outrem sem o seu consentimento. Adapt. SAFERNET, 2016. *A ONG Marias da Internet auxilia vítimas de pornografia de vingança. Entre as atividades do grupo, estão estabelecer a ponte entre vítimas e especialistas em cibercrime e oferecer suporte emocional a essas mulheres.* Adapt. Época, 2016. Nota: Geralmente motivado por vingança após rejeição ou não aceitação do término de um relacionamento. Adapt. SAFERNET, 2016. Ver revenge porn.

**revenge porn** *n.m.* Ver pornografia de vingança.

**roubo de identidade** *n.m.* Ver furto de identidade virtual.

**scam** *n.m.* Ver phishing.

**scam romance** *n.m.* Modalidade de fraude de antecipação de recursos com falsas intensões românticas visando conquistar o afeto e confiança da vítima. Ver noiva russa; fraude de

antecipação de recursos.

**spoofing** *n.m.* Ato que utiliza o sistema informático para alterar campos e cabeçalho de e-mail para ocultar a verdadeira origem do endereço da mensagem. Adapt. SUPPORT GOOGLE, 2016. *Se encontrar mensagens em Spam provenientes de remetentes como mim ou Eu, ou respostas a uma mensagem que você nunca enviou, é possível que você esteja sendo vítima de um ataque de spoofing.* Adapt. SUPPORT GOOGLE, 2016. Ver falsificação de e-mail.

## AGENTES DE CRIME CIBERNÉTICOS

**cibercriminoso** *n.m.* Indivíduo que pratica crime cibernético. Ver crime cibernético.

**ciberquadrilha** *n.f.* Grupo de indivíduos que se associam para a prática de crime cibernético. Ver crime cibernético.

**craker** *n.m.* Indivíduo especializado em conhecimentos técnicos de informática e programação que utiliza o sistema informático para invadir computadores, programas, e sistemas informáticos, decodificar códigos de segurança, de forma ilícita e antiética, em benefício pessoal ou coorporativo . Adapt. SAFERNET, 2016. *Mitnick foi um cracker famoso nos anos 90 que conseguiu obter acesso não autorizado a alguns dos mais seguros sistemas desenvolvidos, das maiores corporações do mundo, incluindo telefonia celular, empresas de tecnologia e provedores de internet. Acabou sendo preso em 1995 e ficou três anos em liberdade condicional sem poder se conectar à internet.* Adapt. SUPERINTERESSANTE, 2010. Nota: Termo oriundo da língua inglesa “crack”, significa “quebrar” um sistema. Adapt. CRONKHITE e McCULLOUGH, 2001. Ver cibercriminoso.

**cyberbully** *n.m* Aquele que pratica cyberbullying. Ver cyberbullying.

**defacer** *n.m.* Aquele que pratica defencement. Ver defacement; pichador virtual.

**fake** *n.m.* Indivíduo que utiliza o sistema informático para criar conta ou perfil falso na Internet com a finalidade de ocultar sua real identidade ou se passar por outra pessoa. Adapt. CRONKHITE e McCULLOUGH, 2001. Podem ser usurpadas identidades de famosos ou até mesmo outras pessoas anônimas. Ver perfil fake; perfil falso.

**hacker** *n.m.* Indivíduo especializado em conhecimentos técnicos de informática e programação que utiliza o sistema informático para conhecer, encontrar falhas, acessar, decodificar, e reprogramar sistemas, programas e redes de computadores. Adapt. SAFERNET, 2016. *Os Hackers criaram a Internet e conceberam seu caráter livre, criaram a World Wide Web, os padrões abertos de comunicação em rede e milhares de softwares livres respeitados, como o Linux*. Nota: Oriundo da palavra inglesa "hack" que significa "cortar", o termo "hacker" muitas vezes tem o uso equivocado, sendo utilizado pejorativamente para definir vândalos e invasores de sistemas. Adapt. SAFERNET, 2016. Ver cibercriminoso.

**perfil fake** *n.m*. Ver fake.

**perfil falso** *n.m*. Ver fake.

**pichador virtual** *n.m*. Ver defacer. Ver defacer.

**spammer** *n.m* Aquele que envia spam. Ver spam.

**scammer** *n.m* Aquele que pratica scam. *O scammer usam softwares maliciosos, phishing ou técnicas de engenharia social para acessar informações pessoais, geralmente com o objetivo de roubar dinheiro.* AVAST, 2016. Ver scam.

## MECANISMOS DE ATAQUE

**boato virtual** *n.m*. Ver hoax.

**cavalo de Troia** *n.m* Ver trojan. Ver trojan.

**código malicioso** *n.m.* Ver malware.

**hoax** *n.m.* Mensagem eletrônica utilizada no sistema informático que possui conteúdo alarmante e falso, e pode conter malware. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Nota: Geralmente, tem como remetente, ou informa como autor alguma instituição, empresa importante ou órgão governamental. Podem causar diversos problemas, como: espalhar desinformação pela Internet, comprometer a credibilidade e a reputação de pessoas ou entidades; resultar em sérios danos ao sistema operacional instalado no

computador; resultar em golpes, como correntes e pirâmides. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver boato virtual; malware.

**malware** *n.m*. Código ou programa que que utiliza o sistema informático para executar ações danosas e atividades maliciosas em um sistema informático. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *No atual ambiente computacional em rede, o código malicioso, ou malware, é um problema seríssimo. Em 2015, foram descobertos cerca de 430 milhões destes, um aumento de 36% em relação ao ano anterior. Os programas maliciosos causam bilhões de dólares em prejuízos para empresas. Diariamente, são noticiados ataques a nações e órgãos governamentais. Não raro, ficamos sabendo de casos de pessoas que tiveram o seu patrimônio ou intimidade violadas.* MYCYBERSECURITY, 2016. Nota: É a junção das palavras 'malicious' e 'software' (software malicioso). MYCYBERSECURITY, 2016. Ver código malicioso.

**spam** *n.m.* Mensagem eletrônica não solicitada pelo remetente com conteúdo publicitário, irrelevante, inapropriado, ou comercial, enviada por e-mail, celular, ou redes sociais, para um grande número de destinatários que não forneceram seu endereço para esse fim. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *Um spam pode conter códigos maliciosos que uma vez instalados, tem acesso à lista de endereços e permitem o envio de novos spams sem o conhecimento do usuário.* Adapt. de ANTISPAM, 2016. Ver crime cibernético.

**trojan** *n.m.* Malware que entra em um dispositivo informático disfarçado como um programa aparentemente comum, inofensivo e legítimo, e quando executado pelo usuário abre porta de invasão a sistemas, libera acesso externo, e permite roubo de dados e atividades maliciosas sem o conhecimento do usuário, sem necessitar de arquivo hospedeiro ou autoreplicação. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver trojan horse; cavalo de Troia; malware.

**trojan horse** *n.m* Ver trojan.

***vírus*** *n.m*. Programa de computador malicioso que utiliza o sistema informático para se propagar inserindo cópias de si mesmo sem permissão do usuário tornando-se parte de outros programas e arquivos, que depende da execução do programa ou arquivo hospedeiro para que

possa se tornar ativo e dar continuidade ao processo de infecção, podendo causar diversos danos ao dispositivo, como controlar sistemas, destruir dados, enviar informações privadas, ou permitir invasão. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. *O principal meio de propagação de vírus eram os disquetes. Estas mídias caíram em desuso e surgiram novas maneiras, como o envio de e-mail. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, principalmente, pelo uso de pen-drives.* Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver vírus de computador.

**vírus de computador** *n.m.* Ver vírus.

**zombie** *n.m.* Dispositivo informático comprometido por malware que uma vez instalado permite que o uso remoto do dispositivo, sem a autorização do titular para executar atividades. Ver malware.

**worm** *n.m.* Malware capaz de se propagar automaticamente pelo sistema informático, enviando cópias de si mesmo de computador para computador, sem necessitar de outro programa hospedeiro ou de infectar arquivos, causando danos na rede e no dispositivo informático. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012 e Adapt. SAFERNET, 2016. Ver malware.

## MECANISMOS DE DEFESA

**antimalware** *n.m.* Ferramenta que detecta, anula, e remove malwares. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver malware.

**antivírus** *n.m* Antimalware desenvolvido para detectar, anular e eliminar de um computador vírus e outros malwares. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver antimalware.

**assinatura digital** *n.f.* Código usado para comprovar a autenticidade e a integridade de uma informação. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET 2012. Ver crime cibernético.

**backup** *n.m.* Cópia de dados de um dispositivo informático para segurança no caso de eventual perda de informação. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver cópia de segurança.

**cópia de segurança** *n.f.* Ver backup

**firewall** *n.m.* Antimalware de segurança usado para dividir e controlar o acesso entre redes de computadores e proteger o dispositivo informático contra acessos não autorizados. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver antimalware.

**interceptação de tráfego** *n.f.* Técnica que inspeciona dados trafegados em redes de computadores para detectar problemas, analisar desempenho do computador e monitorar atividades maliciosas. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver snniffing.

**varredura** *n.f.* Técnica que consiste em efetuar buscas minuciosas em redes com o objetivo de identificar computadores infectados. Adapt. de CARTILHA DE SEGURANÇA PARA INTERNET, 2012. Ver sacan.

**scan** *n.m.* Ver varredura.

**sniffing** *n.m.* Ver interceptação de tráfego.

# CAPÍTULO 5 - CONSIDERAÇÕES FINAIS

Esse estudo teve como norte a identificação e a descrição do conjunto de termos que fazem parte da denominação de crimes cibernéticos, para a compreensão da relação entre os conceitos e os termos que constituem o assunto. Trata-se de uma terminologia recente, em uso há cerca de apenas duas décadas, o que reflete o caráter novo, atual e contemporâneo do tema. Junto a esse reconhecimento, constatamos também a carência de pesquisas, de publicações científicas e de sistematicidade nessa área.

Ao verificarmos que o estudo possui caráter interdisciplinar, houve a necessidade de conhecer e pesquisar a respeito de tecnologia, terminologia, ciberespaço, acompanhados de conceitos do direito e segurança da informação.

O desenvolvimento desta pesquisa almejou principalmente promover um léxico especializado que esteja disponível para ser consultado, que sirva de apoio para profissionais e para os usuários da web. O conteúdo deste estudo é matéria que promove o acesso ao conhecimento e à informação, de forma que pretendemos fomentar a discussão do assunto, contribuir para a formação dos profissionais e estudantes envolvidos com o tema e despertar o interesse de outros pesquisadores, inclusive de áreas afins para essa terminologia, visto que é um campo promissor para novos estudos técnicos.

Do trajeto de todo este estudo, resultou um importante produto: o glossário de termos de crimes cibernéticos. Esse trabalho terminológico possui grande validade social, pois contribui para a construção de um ciberespaço seguro. O que desejamos é oferecer condições apropriadas para a concepção de conceitos e significados para o público-alvo, durante o processo de estudo, análise e investigação de crimes cibernéticos, por meio de uma linguagem acessível e eficaz.

A contribuição de um especialista da área de crimes cibernéticos, que atuou como consultor de nosso trabalho, validando termos e participando de entrevista, prestando informações relevantes para o melhor entendimento do tema, foi de extrema importância para a depreensão de conceitos e fez toda a diferença no processo de reflexão e elaboração do material.

Foi feita a análise do corpus e identificamos 80 unidades terminológicas que compõem o glossário. Percebemos que não é conveniente afirmar que a terminologia de crimes cibernéticos seja de natureza predominantemente simples ou composta, dada a grande proximidade entre o resultado de frequência: 56% para UTCs e 44% para termos simples.

Uma das características relevantes do estudo foi a constatação de variação dos termos

analisados, porque identificamos casos de variantes coocorrentes e variantes competitivas, fato que atesta e corrobora a teoria variacionista da terminologia, o que demonstra que as mesmas regras de construção, formação e elaboração do discurso também promovem variações linguísticas.

A análise de fenômenos linguísticos dos dados foi de total relevância para a elaboração do glossário, que descreveu e sistematizou 80 termos averiguados, na tentativa de preencher a lacuna de estudos linguísticos que descrevam a terminologia de crimes cibernéticos no Português do Brasil. Apesar dos avanços dos estudos terminológicos, são raros os trabalhos aprofundados que se ligam ao tema de crimes cibernéticos que, por sua alta relevância, acreditamos que carece de maior atenção.

Assim, o percurso desta dissertação procurou desenvolver um trabalho linguístico com vistas a ajudar a resolver a problemática existente da ausência de um estudo terminológico dos termos que designam crimes cibernéticos, a fim de suprir equívocos entre significados.

Este estudo também pretendeu auxiliar a falta de legislação específica no Brasil a respeito de crimes cibernéticos, visto que levantamos e analisamos as leis pertinentes ao assunto, e concluímos que a ausência de designação a respeito de crimes cibernéticos confere um intenso grau de impunidade no ambiente virtual. Assim sendo, desbravamos um tema novo e relevante, que pode auxiliar a definir as fronteiras do que é lícito ou não no ciberespaço, ampliar o entendimento das condutas delituosas no ambiente virtual, especificar os agentes que praticam tais condutas, e facilitar a compreender melhor o ambiente digital.

# REFERÊNCIAS

## Referências do glossário


AMORIM, Diego. **Prejuízos à economia e à sociedade**. 2010. Disponível em: <http://www.correiobraziliense.com.br/app/noticia/cidades/2010/04/29/interna_cidadesdf,189487/prejuizos-da-pirataria-a-economia-e-a-sociedade.shtml>. Acesso em: 6 abr. 2015.

AVAST. **Academia de ameaças online.** Disponível em: <https://www.avast.com/pt-br/c-online-threats>. Acesso em: 23 abr. 2016.

AVAST. **Scam.** Disponível em: <https://www.avast.com/pt-br/c-scam>. Acesso em: 23 abr. 2016.

CÂMARA DOS DEPUTADOS. **CPI dos Crimes Cibernéticos**. Março, 2016. Disponível em <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125>. Acesso em: 6 abr. de 2016.

CÂMARA DOS DEPUTADOS. **Marco Civil da Internet.** 2014. Disponível em <http://www2.camara.leg.br/documentos-e-pesquisa/fiquePorDentro/temas/marco-civil>. Acesso em: 6 mar. 2015.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. São Paulo, 2012.

COSTA, Fábio. **Golpe Nigeriano**. ISTOÉ, 2016. Disponível em: <http://istoe.com.br/150287_GOLPE+NIGERIANO/>. Acesso em: 23 fev. 2016.

CRESPO, Marcelo. **As diversas terminologias do universo hacker**. Canal Ciências Criminais. 30 de setembro de 2015. Disponível em: <https://canalcienciascriminais.com.br/as-diversas-terminologias-do-universo-hacker/> Acesso em: 23 fev. 2016.

Cyberbullying Research Center. Disponível em: <http://cyberbullying.org/>. Acesso em: 7 out. 2015

DANTAS, Tiago. **Pirataria.** Brasil Escola. Disponível em <http://brasilescola.uol.com.br/curiosidades/pirataria.htm>. Acesso em: 29 nov. 2016.

FARES, Marcelo. **Terminologia hacker**. ProfissionaisTI. 18 de maio de 2015. Disponível em: <https://www.profissionaisti.com.br/2015/05/terminologia-hacker/>. Acesso em: 27 abr. 2016.

INTERNETSEGURA.PT. **Roubo de identidade**: o que é? Disponível em: <http://www.internetsegura.pt/riscos-e-prevencoes/roubo-de-identidade>. Acesso em: 21 mar. 2015.

MÜLLER, Leonardo. **O que é Phishing?** 2012. Disponível em: <http://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm>. Acesso em: 14 mar. 2015.

MYCYBERSECURITY. **Entendendo as ameaças:** malware – parte I. 25 de maio de 2016. Disponível em: <://www.mycybersecurity.com.br/entendendo-as-ameacas-digitais-e-suas-diferencas-malware/>. Acesso em: 11 jun. 2016.

MYCYBERSECURITY. **Romance Scam:** golpe fatura milhões. 22 de novembro de 2015. Disponível em: <http://www.mycybersecurity.com.br/romance-scam-quem-e-peace-mabry/>. Acesso em: 22 fev. 2016

PROGRAMA BULLYING e Cyberbullying. Disponível em: <*http://bullyingcyberbullying.com.br/*>. Acesso em: 15 nov. 2015.

RODRIGUES, Alan; FILHO, Mário, S. **Pedofilia prolifera pela Internet e transforma o Brasil no quarto país do ranking mundial da pornografia infantil**. 27 de outubro de 2004. Disponível em: http://istoe.com.br/9581_PERIGO+DIGITAL/. Acesso em: 2 out. 2014.

SAFERNET. **Crimes na Internet**. Disponível em: <http://new.safernet.org.br/>. Acesso em: 12 mar. 2015.

**Referências documentais**

BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Vade mecum**. São Paulo: Saraiva, 2008.

_____. Constituição da República Federativa do Brasil. Brasília, DF. Senado Federal: Centro Gráfico, 1998.

_____. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial República Federativa do Brasil, Poder Executivo, Brasília, DF.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Dispõe sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial República Federativa do Brasil, Poder Executivo, Brasília, DF.

_____. **Lei nº 11.829, de 25 de novembro de 2008**. Altera a Lei nº 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente. Dispõe sobre a pedofilia. Diário Oficial República Federativa do Brasil, Poder Executivo, Brasília, DF.

**Referências de Literatura**

CABRÉ, Maria. T. **La terminologia**: teoría, metodología, aplicaciones. Editorial Antártida Empúries: Barcelona, 1993.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 2. ed. São Paulo: Saraiva, 2002.

CRYSTAL, David. **A Revolução da Linguagem**. Rio de Janeiro: Jorge Zahar, 2005.

DE OLIVEIRA, Luiz G. C; DANI, Gabriela S. **Os crimes virtuais e a impunidade real**. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963>. Acesso em: 16 nov. 2014.

DODEBEI, Vera. **Patrimônio digital virtual.** Herança, documento e informação. In E o patrimônio? Desafios para o século XXI. Universidade Federal do Estado do Rio de Janeiro - UNIRIO, 2008.

FAULSTICH, Enilde L. de J. **A Socioterminologia na comunicação científica e técnica.** Ciência e Cultura, São Paulo, v. 58, n. 2, 2006.

_____. **Aspectos de terminologia geral e terminologia variacionista**. Trad. Term. São Paulo: [s.n.], v. 7, 2001.

_____. **Características do que é e para que serve nas definições de terminologias científica e técnica.** In: ISQUERDO, Aparecida Negri; DAL CORNO, Giselle Olivia Mantovani (Org.). As Ciências do Léxico: lexicologia, lexicografia, terminologia. Vol. VII. Campo Grande, MS: Ed. UFMS, 2014.

_____. **Formação de termos:** do constructo e das regras às evidências empíricas. In: FALSTICH, Enilde; ABREU, Sabrina Pereira. (Orgs.). Linguística aplicada à terminologia e à lexicografia: cooperação internacional: Brasil e Canadá. Porto Alegre: UFRGS, Instituto de Letras, NEC, 2003.

_____. **Glossário de Termos Empregados nos estudos da Terminologia, da Lexicografia e da Lexicologia.** Centro Lexterm. Brasília: Universidade de Brasília, 2011.

_____. **Glossário sistêmico de léxico terminológico para pesquisadores surdos.** Brasília, centro Lexterm, 2012. Em elaboração.

_____. **Metodologia para projetos terminográficos**. Léxico e Terminologia Coletânea de textos. Centro LexTerm. Brasília: Universidade de Brasília, 1993.

_____. **Metodologia para projeto terminográfico**. Unb/IBICT. Brasília, 1990.

_____. **O léxico 'lexical'; o léxico 'lexicográfico'; o léxico 'terminológico'** – onde está o LÉXICO? VI Semana de Estudos Lexicais. UnB/LIP/Centro Lexterm, 2011.

_____. **Para gostar de ler um dicionário**. In. RAMOS, Conceição de M. de A; BEZERRA, José de R. M; ROCHA, Maria de F. S. (org). Pelos caminhos da dialetologia e sociolinguística: entrelaçando saberes e vidas – homenagem a Socorro Aragão. São Luís: EDUFMA, 2010.

_____. **Proposta metodológica para a elaboração de léxicos, dicionários e glossários**. LIV/IL/UnB/Centro Lexterm. Brasília, 2001.

**_____. Rede de remissivas em um glossário técnico.** In: MACIEL, A. M. B. (org.) Cadernos do Instituto de Letras. n.10, Porto Alegre, UFRGS, jul. 1993a, p. 91-98. 1993.

_____. **Socioterminologia:** mais que um método de pesquisa, uma disciplina. Ciência da Informação, v. 24, n. 3, 1995.

FREIRE-MAIA, Newton. **A ciência por dentro**. 7. ed. Petrópolis: Vozes, 1998.

HABERMANN, Josiane C. A. **As normas da ABNT em trabalhos acadêmicos**: TCC, dissertação e tese. 2. ed. São Paulo: Globus, 2011.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de. Janeiro: Objetiva, 2014.

LÉVY, Pierre. **Cibercultura**. 3. ed. São Paulo: Editora 34, 2001.

_____. **O que é o virtual**. 2 ed. São Paulo: Editora 34, 1999.

MARCO CIVIL DA INTERNET. Seus direitos e deveres em discussão. Disponível em <http://culturadigital.br/marcocivil/. Acesso em: 23 de maio de 2015.

PAVEL, Silvia; NOLET, Diane. **Manual de Terminologia**. Adaptação para a língua portuguesa de FAULSTICH, Enilde. Canada: Bureau de la traduction, Travaux publics et Services gouvernementaux Canada, 2002.

PREREIRA, Luciana F. **O princípio da Legalidade na constituição Federal**: análise comparada dos princípios da reserva legal, legalidade ampla e legalidade estrita. 01 abr. 2012. Disponível em <http://www.direitonet.com.br/artigos/exibir/7125/O-principio-da-legalidade-na-Constituicao-Federal-analise-comparada-dos-principios-da-reserva-legal-legalidade-ampla-e-legalidade-estrita> Acesso em 13 de março de 2015.

SCIARRETTA, Toni. **Brasil perde até 8 US$ bilhões com crime cibernético**. Folha de São Paulo, 09 de junho de 2014. Disponível em <http://www1.folha.uol.com.br/mercado/2014/06/1467110-brasil-perde-ate-us-8-bilhoes-com-crime-cibernetico.shtml> Acesso em 06 ago. 2015.

SOUSA, Stênio S. **Questionário de entrevista acadêmica sobre crime cibernéticos.** Brasília, Superintendência Regional da Polícia Federal no Distrito Federal. 03 de maio de 2015. Entrevista concedida a Nara Fernanda Justiniano.

VIEGAS, Waldyr. **Fundamentos de Metodologia Científica**. 2. ed. Brasília: Editora da UnB, 1999.

# ANEXOS

## Anexo 1 – Entrevista sobre crimes cibernéticos

Neste tipo de pesquisa, a atuação do especialista é uma característica fundamental para lapidar o grande volume de informação bruta recebida e interpretar da melhor maneira possível.

Para o completo desenvolvimento deste trabalho fez-se necessário consultar um profissional especialista no assunto e que atua especificamente na área de crimes cibernéticos. Para tanto, entrevistamos o Delegado de Polícia Federal Chefe do Grupo Repressão a Crimes Cibernéticos, da Superintendência Regional da Polícia Federal no Distrito Federal Stênio Santos Sousa.

Mestre em Ciências Policiais, Criminologia e Investigação Criminal (2013-2015), pelo Instituto Superior de Ciências Policiais e Segurança Interna (Lisboa, Portugal). Possui Pós-Graduação (lato sensu) em Ciências Policiais pelo ISCPSI (2013-2014), e Pós-Graduação (lato sensu) em Ciências Criminais pela UNAMA/UVB/LFG (2005-2007), Graduação em Direito pela Universidade Federal do Maranhão (1997-2002). Atualmente é professor e tutor EaD da Academia Nacional de Polícia (2006) e Delegado de Polícia Federal. Tem experiência nas áreas de Direito Penal, Processual Penal, Direitos Humanos e Investigação de Crimes Cibernéticos.

Ao
GRUPO DE REPRESSÃO A CRIMES CIBERNÉTICOS DA POLÍCIA FEDERAL

QUESTIONÁRIO DE ENTREVISTA ACADÊMICA SOBRE CRIMES CIBERNÉTICOS

1. **Qual é a definição mais adequada para “crime cibernético”?**

**Resposta:** Utilizo o conceito de crime cibernético como a ação humana que utiliza o sistema informático como meio para a prática de condutas ilícito-típicas ou como o fim último daquelas. No primeiro caso, diz-se crime cibernético impróprio; no segundo, próprio.

2. **Quais são os principais crimes cibernéticos cometidos no Brasil?**

**Resposta:** Em termos quantitativos, as fraudes contra o sistema bancário demandam atuação

permanente dos órgãos de investigação criminal e causam prejuízos bilionários ao país. Por outro lado, em face do disposto no art. 227, da Constituição Federal, os crimes cibernéticos mais graves são aqueles que atingem a dignidade sexual de crianças e adolescentes, previstos nos art. 240 (produção de imagens de exploração sexual infantil), 241-A (publicação de tais imagens), 241-B (posse, aquisição, armazenamento), 241-D (aliciamento virtual) do Estatuto da Criança e do Adolescente (Lei 8.069/90). Além desses, devemos citar os casos de ataques contra as infraestruturas críticas do país, em geral por meio de invasão de sistemas e ataques distribuídos de negação de serviço (DDoS). Além disso, com menos gravidade, temos o defacement (ou pichação virtual) de páginas na Internet, que causam prejuízos a serviços prestados ao cidadão, tornando-os temporariamente indisponíveis. Em termos de disseminação, devemos citar os crimes de ódio e os crimes contra a honra, tão em voga em tempos de redes sociais.

3. **Qual é a legislação existente no país quando se trata de crimes cibernéticos? Existem leis que especificam esse tipo de crime?**

**Resposta:** Os crimes cibernéticos impróprios, que são aqueles que utilizam o sistema informático como meio para a prática de condutas ilícito-típicas já existentes, estão previstos na legislação penal tradicional. A alteração que ocorre é apenas instrumental, não havendo necessidade de legislação específica. Um furto pode ser praticado de forma pessoal ou de forma cibernética, mas será tratado pelo mesmo Código Penal, no art. 155. Por outro lado, quando pensamos em crimes cibernéticos próprios, quando o sistema computacional é o fim da conduta ilícito-típica, pode haver necessidade de legislação especial. Para tratar, por exemplo, da invasão de um computador, não há legislação tradicional, pois, o nosso Código Penal é de 1940, quando os computadores não existiam e, portanto, não poderiam ser considerados como bens jurídicos demandantes de proteção jurídica. A Lei nº 12.737, de 30 de novembro de 2012, veio suprir essa lacuna é previu o crime de "invasão de dispositivo informático", inserindo o art. 154-A, no Código Penal. Além disso, alterou a redação do art. 266, do Código Penal para prever a conduta de "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", que se refere ao ataque distribuído de negação de serviço ou ataque de negação de serviço (DDoS ou DoS), que ocorre quando uma máquina é exigida para além de sua capacidade de transmissão de pacotes na rede, ocasionando sua interrupção.

4. **Existe alguma publicação (livro, glossário) consultada por profissionais da área que oriente e auxilie a definir, identificar e especificar os crimes cibernéticos?**

**Resposta:** Os crimes cibernéticos estão definidos na legislação penal. A Polícia Federal possui manuais internos que auxiliam no trabalho de atualização doutrinária, legislativa e jurisprudencial. Além disso, existem livros disponíveis tanto na literatura jurídica nacional quanto internacional que tratam do tema e servem de norte para a nossa atuação. Alguns livros que eu poderia citar são: Cibercrimes: limites e perspectivas à investigação policial de crimes cibernéticos, do Maciel Colli; Direito Digital, da Patrícia Peck, Crimes de Informática, do Sandro D´Amato Nogueira; Criminalidade informática, do Roberto Chacon Albuquerque; Investigação Criminal Cibernética: por uma política criminal de proteção à criança e ao adolescente na Internet, de minha autoria. Na literatura internacional, dentre outros, recomendo Mercado Sombrio, de Misha Gleny, que tem uma leitura fluida e com muito conteúdo. Estou participando, com um capítulo, de uma obra coletiva, com o provável título Crimes Cibernéticos – doutrina e prática (A visão do Delegado de Polícia), organizada pelo Clayton da Silva Bezerra e pelo Giovani Celso Agnoletto que será lançada em breve pela editora Letras Jurídicas, e que provavelmente será uma excelente referência na temática.

5. **É possível coibir a ocorrência de crimes desta natureza? Como?**

**Resposta:** Quando se fala em crimes, é sempre melhor pensar em redução que em extinção, pois o próprio sistema de controle penal cria o delito. É possível extinguir a tipicidade da conduta, mas não a sua materialidade. A prevenção, em nosso entendimento, seria a melhor maneira de redução da criminalidade. Atuar de forma preventiva, implica tomar medidas de segurança específicas, as quais vão variar de acordo com a modalidade criminosa, devendo ser incluídas ações como navegação segura, backup de dados, atualização de dados, compra de software original, ações éticas na rede. Na área de repressão, é fundamental que os órgãos de repressão criminal sejam adequadamente estruturados, sistematicamente treinados, atualizados e atuem de forma coordenada e centralizada. No meu livro Investigação Criminal Cibernética: por uma política criminal de proteção à criança e ao adolescente na Internet, há uma proposta de Política Criminal para dar maior efetividade à prevenção da criminalidade cibernética contra a criança e o adolescente, que é a criação do CENAPOL, um Centro Nacional Policial de Proteção Online à Criança e ao Adolescente, que congrega a maior parte desses princípios fundamentais visando à redução da criminalidade e fortalecimento do cidadão na rede.

6. **Como a população pode se proteger de crimes cibernéticos?**

**Resposta:** Buscando informações sobre navegação segura, realizando o backup sistemático de seus dados pessoais, realizando a atualização periódica de seus programas de computador, adquirindo software original, realizando ações éticas na rede. Cada modalidade criminosa demanda uma ação específica, mas, de um modo geral, esses são procedimentos que ajudam bastante na autoproteção.

7. **Como a vítima de uma modalidade desse tipo de crime deve proceder? Existem delegacias especializadas em crimes cibernéticos?**

**Resposta:** A Polícia Federal possui Grupos de Repressão a Crimes Cibernéticos na maioria das capitais. Alguns Estados também possuem delegacias especializadas na repressão a crimes cibernéticos como é o caso de São Paulo, Rio de Janeiro e Rio Grande do Sul. De um modo geral, se o computador foi infectado por um vírus, será preciso identificar onde está, por meio de uma ação pericial. A partir daí, pode-se chegar ao criminoso. Se o crime foi praticado por meio de correio eletrônico é importante preservar esse conteúdo, inclusive o cabeçalho completo da mensagem, a fim de facilitar o trabalho de investigação. No caso de um crime praticado em redes sociais, preservar a página, tirando foto, imprimindo e utilizando aplicações específicas para capturar a publicação é um bom começo para viabilizar o trabalho de investigação criminal. Quanto antes a polícia for acionada, maior a possibilidade de chegar ao autor do delito. Evitar a disseminação do material ilícito para todos os órgãos policias também é uma medida que evita a duplicidade ou multiplicidade de investigações, contribuindo para uma maior eficácia da ação policial.

**Anexo 2 – Lei nº 12.965, de 23 de abril de 2014, Marco Civil**

**MARCO CIVIL, OU LEI 12.965, DE 23 DE ABRIL DE 2014.**

**Presidência da República**

**Casa Civil**

**Subchefia para Assuntos Jurídicos**

**LEI Nº 12.965, DE 23 DE ABRIL DE 2014.**

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

**A PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II

DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III

DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

**Seção I**

**Da Neutralidade de Rede**

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

**Seção II**

**Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas**

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

**Subseção I**

**Da Guarda de Registros de Conexão**

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

**Subseção II**

**Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão**

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

**Subseção III**

**Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações**

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a

aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

**Seção III**

**Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros**

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

**Seção IV**

**Da Requisição Judicial de Registros**

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

## CAPÍTULO V
## DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações

sobre o uso dos programas de computador previstos no**caput**, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF

*José Eduardo Cardozo*

*Miriam Belchior*

*Paulo Bernardo Silva*

*Clélio Campolina Diniz*

Este texto não substitui o publicado no DOU de 24.4.2014

**Anexo 3 – Lei nº 12.737, de 30 de novembro de 2012**

**LEI 12.737 DE 30 DE NOVEMBRO DE 2012**

**Presidência da República**

**Casa Civil**

**Subchefia para Assuntos Jurídicos**

**LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.**

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

**A PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

**"Invasão de dispositivo informático**

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 obtidos.

§ 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."

**"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."

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." (NR)

**"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." (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012;
191º da Independência e 124º da República.

DILMA ROUSSEFF

*José Eduardo Cardozo*

Este texto não substitui o publicado no DOU de 3.12.2012

**Anexo 4 – Lei nº 12.735, de 30 de novembro de 2012**

**Presidência da República**
**Casa Civil**
**Subchefia para Assuntos Jurídicos**

LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.

Mensagem de veto

Vigência

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.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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. 2º (VETADO)

Art. 3º (VETADO)

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.

Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20. .....

.....

§ 3º .....

.....

II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

.....” (NR)

Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
*José Eduardo Cardozo*
*Paulo Bernardo Silva*
*Maria do Rosário Nunes*

Este texto não substitui o publicado no DOU de 3.12.2012

*