UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO

Lucas Lacerda da Costa

A CONVENÇÃO DE BUDAPESTE E A HARMONIZAÇÃO LEGISLATIVA A PARTIR DA RESPONSABILIDADE PENAL DO CÚMPLICE EM CRIMES CIBERNÉTICOS

Florianópolis
2023

Lucas Lacerda da Costa

A CONVENÇÃO DE BUDAPESTE E A HARMONIZAÇÃO LEGISLATIVA A PARTIR DA RESPONSABILIDADE PENAL DO CÚMPLICE EM CRIMES CIBERNÉTICOS

Trabalho Conclusão do Curso de Graduação em Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Direito.
Orientador: Prof. Dr. Cláudio Macedo de Souza

Florianópolis
2023

(FICHA DE IDENTIFICAÇÃO DA OBRA)

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COORDENADORIA DE MONOGRAFIA

ATA DE SESSÃO DE DEFESA DE TCC (VIRTUAL)
(Autorizada pela Portaria 002/2020/PROGRAD)

Aos **05** dias do mês de **dezembro** do ano de 2023, às **15** horas e **30** minutos, foi realizada a defesa pública do Trabalho de Conclusão de Curso (TCC), no modo virtual, através do link: "https://meet.google.com/xnh-bugv-bvm" intitulado **"A Convenção de Budapeste e a harmonização legislativa a partir da responsabilidade penal do cúmplice em crimes cibernéticos",** elaborado pelo acadêmico Lucas Lacerda da Costa, matrícula **nº 16100289**, composta pelos membros **Prof. Dr. Claudio Macedo de Souza, M.ª Soraya Teshima (PPGD UFSC), Rafaela dos Reis Baldissera (Mestranda PPGD/UFSC)**, abaixo assinados, obteve a aprovação com nota 9,75 (nove inteiros e setenta e cinco centésimos), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

(x) Aprovação Integral
( ) Aprovação Condicionada aos seguintes reparos, sob fiscalização do Prof. Orientador

Florianópolis, 05 **de dezembro de 2023**.

ICP-Edu
Documento assinado digitalmente
Claudio Macedo de Souza
Data: 06/12/2023 20:14:09-0300
CPF: ***.565.726-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Cláudio Macedo de Souza (ASSINATURA DIGITAL)
Professor Orientador

ICP-Edu
Documento assinado digitalmente
Soraya Teshima
Data: 07/12/2023 08:31:21-0300
CPF: ***.352.369-**
Verifique as assinaturas em https://v.ufsc.br

M.ª Soraya Teshima (PPGD UFSC) (ASSINATURA DIGITAL)
Membro de Banca

GOV.BR
Documento assinado digitalmente
RAFAELA DOS REIS BALDISSERA
Data: 07/12/2023 14:53:30-0300
CPF: ***.431.330-**
Verifique as assinaturas em https://v.ufsc.br

Rafaela dos Reis Baldissera (Mestranda PPGD/UFSC)(ASSINATURA DIGITAL)
Membro de Banca

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "A Convenção de Budapeste e a harmonização legislativa a partir da responsabilidade penal do cúmplice em crimes cibernéticos"**,** elaborado pelo(a) acadêmico(a) "**Lucas Lacerda da Costa"**, defendido em **05/12/2023** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota **9,75 (nove inteiros e setenta e cinco centésimos)**, cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 05 de dezembro de 2023

Documento assinado digitalmente
Claudio Macedo de Souza
Data: 06/12/2023 20:14:34-0300
CPF: ***.565.726-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Dr. Cláudio Macedo de Souza
Professor Orientador

Documento assinado digitalmente
Soraya Teshima
Data: 07/12/2023 08:31:56-0300
CPF: ***.352.369-**
Verifique as assinaturas em https://v.ufsc.br

M.ª Soraya Teshima (PPGD UFSC)
Membro de Banca

Documento assinado digitalmente
RAFAELA DOS REIS BALDISSERA
Data: 07/12/2023 14:54:09-0300
CPF: ***.431.330-**
Verifique as assinaturas em https://v.ufsc.br

Rafaela dos Reis Baldissera (Mestranda PPGD/UFSC)
Membro de Banca

Universidade Federal de Santa Catarina
Centro de Ciências Jurídicas
COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluno(a): Lucas Lacerda da Costa
RG: 6.302.481
CPF: 107.931.169-61
Matrícula: 16100289
Título do TCC: A Convenção de Budapeste e a harmonização legislativa a partir da responsabilidade penal do cúmplice em crimes cibernéticos
Orientador(a): Prof. Dr. Cláudio Macedo de Souza

Eu, Lucas Lacerda da Costa, acima qualificado; venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 05 de dezembro de 2023.

Documento assinado digitalmente
LUCAS LACERDA DA COSTA
Data: 06/12/2023 11:19:40-0300
CPF: ***.931.169-**
Verifique as assinaturas em https://v.ufsc.br

LUCAS LACERDA DA COSTA

Dedico o trabalho ao meu falecido avô Wilson.

AGRADECIMENTOS

Gostaria de agradecer primeiramente aos meus pais por todo o suporte ao longo dessa minha jornada. Estendo os agradecimentos aos meus avós, que fizeram parte disso tudo, principalmente a Vó Doris, com seu amor incondicional e apoio em todos os momentos.

Agradeço ao professor Macedo, por ter aceitado ser meu orientador, pela sua paciência em compreender as minhas particularidades, e por todas as contribuições, desde o meu projeto de pesquisa, até a finalização do trabalho, sem as quais eu não teria condições de finalizar. Estendo os meus agradecimentos à Universidade Federal de Santa Catarina.

Agradeço à minha companheira Geovanna, por todo o seu suporte durante essa elaboração de trabalho, que se dispôs a cuidar da nossa filha Elisa, a fim de que eu tivesse o tempo necessário para conseguir escrever. Estendo esse agradecimento à minha filha, por ser capaz de me alegrar nos dias mais difíceis, simplesmente com a sua presença.

Agradeço aos meus amigos que me estenderam a mão e me ajudaram a passar pelos momentos mais exaustivos, em especial ao meu amigo, e colega de curso Matheus, que me acompanha até hoje na minha vida profissional.

Agradeço a todas as pessoas que estiveram presentes durante esses momentos, e que contribuíram para a minha formação, até agora.

RESUMO

Esta monografia objetiva compreender a responsabilização penal do cúmplice a partir da tipificação das condutas de disponibilizar ou de possuir um dispositivo ou programa informático e uma palavra passe para a prática de crimes próprios de internet. O surgimento de novas técnicas na era da informação traz consigo um efeito indesejável e inevitável que são os crimes cibernéticos. Esses novos delitos são, em si, um novo risco à sociedade mundial. A necessidade de criminalização dos agentes que praticam as condutas demanda cooperação internacional em razão dos aspectos transfronteiriços desses crimes. A partir dessa perspectiva, o Conselho da Europa, em novembro de 2001, promulga a Convenção de Budapeste, como mecanismo de defesa contra esses novos crimes. As disposições do tratado demandam, dentre outras, compreender a responsabilização penal do cúmplice a partir da tipificação das condutas de disponibilizar ou de possuir um dispositivo ou programa informático e uma palavra passe para a prática de crimes próprios de internet. Nesse sentido indaga-se: "como responsabilizar penalmente o cúmplice que auxilia materialmente na prática dos crimes cometidos contra os sistemas informáticos e dados informáticos?" Levando-se em conta as condutas previstas na Convenção de Budapeste, supõe-se que a responsabilidade penal do cúmplice, baseada no uso abusivo de dispositivos, deverá considerar a tipificação das condutas de disponibilizar ou de possuir código de acesso capaz de acessar o todo ou em parte um dispositivo/sistema informático, e programa informático com a intenção de praticar crimes contra os sistemas informáticos e dados informáticos. Os países que são signatários dessa Convenção, portanto, devem dispor sobre essas condutas típicas, para atender às suas exigências.

Palavras-chave: sociedade de risco; crimes cibernéticos; Convenção de Budapeste; cumplicidade.

ABSTRACT

This dissertation aims to understand the criminal liability of an accomplice based on the typification of behaviors related to providing or possessing a device or computer program and a password for the commission of internet-related crimes. The emergence of new techniques in the information age brings with it the undesirable and inevitable effect of cybercrimes. These new offenses represent a new risk to global society. The need to criminalize individuals engaged in such conduct requires international cooperation due to the cross-border aspects of these crimes. From this perspective, in November 2001, the Council of Europe enacted the Budapest Convention as a defense mechanism against these new crimes. The provisions of this treaty, among other things, require understanding the criminal liability of an accomplice based on the classification of acts involving the provision or possession of a device or computer program and a password for the commission of internet-related crimes. In this regard, the question arises of how to criminally hold an accomplice who materially assists in the commission of crimes against computer systems and data accountable. Taking into account the behaviors outlined in the Budapest Convention, it is assumed that the criminal responsibility of the accomplice, based on the abusive use of devices, should consider the classification of acts involving the provision or possession of access codes capable of accessing all or part of a device/computer system and computer programs with the intention of committing crimes against computer systems and data. Countries that are signatories to this Convention, therefore, should legislate on these typical behaviors to meet its requirements.

Keywords: Risk Society. Cybercrimes. Budapest Convention. Complicity.

SUMÁRIO

1 INTRODUÇÃO…….…….……12
2 A SOCIEDADE DE RISCO E DA INFORMAÇÃO…….……..15
2.1 A relação entre sociedade de risco e os crimes cibernéticos……..…..…16
2.2 A informação como bem jurídico tutelado…….……...…19
3 LEGISLAÇÕES SOBRE CRIME CIBERNÉTICO PRODUZIDAS NOS PAÍSES MUNDO AFORA…….…...….24
3.1 Legislação sobre o *cibercrime* produzida em Portugal…….……...24
3.2 Legislação sobre o *cibercrime* produzida nos Estados Unidos da América…..…..31
3.3 Legislação nacional sobre crimes cibernéticos…….…36
4 CUMPLICIDADE NOS CRIMES CIBERNÉTICOS…….……42
4.1 Teoria de concurso de pessoas……...…….…….…...43
4.2 Diferenciação entre crimes próprios e impróprios na Convenção……...……..44
4.3 Crimes próprios previstos na Convenção de Budapeste……..…….……..45
4.3.1 Acesso ilegítimo……45
4.3.2 Intercepção ilegítima……47
4.3.3 Interferência em dados……..47
4.3.4 Interferência em sistemas…….…….48
4.3.5 Uso abusivo de dispositivos…….…….49
5 CONCLUSÃO…….……51
REFERÊNCIAS

1 INTRODUÇÃO

Esta monografia objetiva compreender a responsabilização penal do cúmplice a partir da tipificação das condutas de disponibilizar ou de possuir um dispositivo ou programa informático e uma palavra passe para a prática de crimes próprios de internet.

Vivemos em uma época de constantes mudanças em nossa sociedade, e grandes avanços técnicos em praticamente todas as áreas humanas. Essas mudanças e avanços são percebidos, dentre tantos, no âmbito jurídico-penal, com destaque para o surgimento de novos tipos delituosos, que são os *cibercrimes*. A atuação dos indivíduos nesse novo meio criminoso demandou a cooperação internacional, em razão das características transnacionais dos delitos, e dessa parceria surgiu a Convenção de Budapeste, promulgada no Conselho da Europa, em novembro de 2001. Dentre as previsões da Convenção, uma delas estabelece a necessidade de punir não só as pessoas que praticam os atos reprováveis, mas também aqueles que contribuem para o resultado dessas condutas. Nesse contexto, a partir do exame desse novo acordo internacional, surge a necessidade de compreender a responsabilização penal do cúmplice, a partir da tipificação das condutas de disponibilizar ou de possuir um dispositivo ou programa informático e uma palavra passe para a prática de crimes próprios de internet.

Os crimes cibernéticos são praticados, via de regra, por meio da invasão de dispositivos conectados ou não à rede mundial de computadores, e para o sucesso desses ataques, são necessários o desenvolvimento de ferramentas apropriadas, dispositivos concebidos para este fim, ou códigos de acesso, palavras-passe que permitam aos criminosos o pleno acesso aos sistemas, dispositivos, e dados alheios, daí a necessidade de se criminalizar também o cúmplice.

A partir desse contexto, surge a seguinte indagação:"Como responsabilizar penalmente o cúmplice que auxilia materialmente na prática dos crimes cometidos contra os sistemas informáticos e dados informáticos?"

Levando-se em conta as condutas previstas na Convenção de Budapeste, supõe-se que a responsabilidade penal do cúmplice, baseada no uso abusivo de dispositivos, deverá considerar a tipificação das condutas de disponibilizar ou de possuir código de acesso capaz de acessar o todo ou em parte um dispositivo/sistema informático, e programa informático com a intenção de praticar crimes contra os sistemas informáticos e dados informáticos.

Para o exame apropriado da hipótese apresentada, utilizou-se, durante toda a pesquisa, o método dedutivo, pois parte-se de uma ideia geral, para se chegar a um conceito mais específico.

Buscou-se o marco teórico que abarque os crimes cibernéticos como um fenômeno a ser estudado, dentro do contexto social em que estamos inseridos. Apresenta-se, nesse sentido, as ideias desenvolvidas pelo sociólogo alemão Ulrich Beck na sua obra "Sociedade de risco: rumo a uma nova modernidade", na qual são encontradas longas discussões sobre os aspectos dos riscos na sociedade: o surgimento, distribuição, desenvolvimento e aparentes efeitos.

Os *cibercrimes* surgem nessa nova configuração social que se forma, em que o sociólogo se aprofundou, nos trazendo, por seus estudos, que a revolução acontece diuturnamente de forma silenciosa por todo o mundo, a partir dos avanços das técnicas nos diversos âmbitos sociais. Esse desenvolvimento sem limites acumula consigo a difusão cada vez maior de "riscos", que atingem toda a população de forma geral (Beck, 2010, p. 16-17).

Os crimes cibernéticos são, em si mesmos, um novo tipo de risco, e nesse contexto, a informação, ou, os dados informáticos, surgem como fonte de riqueza. A partir dessa premissa, será feito no primeiro capítulo o estudo sobre a informação como bem jurídico apto a ser penalmente protegido, junto à investigação sobre as características da sociedade de risco desenvolvidas por Beck, e sua relação com os crimes cibernéticos.

A pesquisa será realizada com suporte da doutrina brasileira, assim como das disposições contidas na Constituição Federal de 1988 acerca do conceito de bem jurídico. Quanto à sociedade de risco e sua relação com os crimes cibernéticos, utiliza-se a obra de Ulrich Beck para servir como fonte dessa investigação.

Os crimes cibernéticos têm como pressuposto a previsão da informática como bem jurídico a ser protegido, e isso ocorre de variadas formas pelo mundo. A fim de oferecer essa proteção, os países são signatários da Convenção de Budapeste, a qual conta com mecanismos de cooperação internacional, ferramenta necessária para o combate efetivo aos delitos, e como assinantes, as nações precisam dispor no seu ordenamento jurídico algumas condutas, consideradas no texto da Convenção como indispensáveis. Dentre elas, se observa a criminalização do cúmplice que auxilia materialmente, ao disponibilizar códigos de acesso, ou dispositivos, concebidos para o fim específico de praticar as condutas descritas na Convenção.

A partir dessa premissa, serão investigadas, no segundo capítulo, as legislações produzidas em diferentes países, a fim de observar como ocorre essa criminalização do cúmplice, e se ocorre de modo a atender às disposições da Convenção. Como fonte de pesquisa, será utilizada a base de dados disponibilizada pela Organização das Nações Unidas (ONU) em seu *site* (sherloc.unodc.org), que contém, dentre outras informações, um acervo

compilando as leis de muitos países que dispõem sobre diversos crimes, incluídos os cibernéticos.

Um fator limitador da pesquisa diz respeito ao objeto de investigação, que são os crimes cibernéticos próprios, ou seja, aqueles cujo o foco de proteção são a informática e os dados informáticos. Sendo assim, apesar de supor-se que nas legislações a serem analisadas estão incluídas condutas típicas próprias e impróprias cibernéticas, opta-se por investigar somente as condutas próprias, tendo em vista que apenas essas demandam a criação de novas leis e delitos a serem criminalizados. As condutas impróprias, diga-se, aquelas cujo foco de proteção são outros bens, ficam inseridas dentro de tipos penais que já são previstos nos ordenamentos, como furto e dano, de modo que apenas o meio informático acaba mudando.

Depois de verificadas as legislações no âmbito internacional, aproxima-se da hipótese da pesquisa, para ser realizada, no capítulo terceiro, a investigação sobre a legislação penal brasileira em face das diretrizes previstas na convenção, para a criminalização da conduta do cúmplice que auxilia materialmente na prática dos crimes cibernéticos.

A investigação do terceiro capítulo tem como base a doutrina brasileira sobre o concurso de pessoas, para ser compreendida como como se dá a previsão de criminalização dos cúmplices no nosso ordenamento, além da própria legislação nacional, que dispõe sobre crimes cibernéticos, igualmente a partir da base de dados da ONU, mantendo-se a coerência aos outros países que se busca analisar. Além disso, a Convenção de Budapeste serve como apoio para a pesquisa, no que diz respeito às suas disposições sobre os crimes cibernéticos próprios, e sobre como ocorre a criminalização do cúmplice que auxilia materialmente para a prática desses delitos.

2 A SOCIEDADE DE RISCO E DA INFORMAÇÃO

Este capítulo objetiva investigar o bem jurídico tutelado nos crimes próprios cibernéticos a partir da sua relação com a ideia do risco teorizada na obra de Ulrich Beck, intitulada "Sociedade de risco: rumo a uma outra modernidade". Beck defende a ideia de que a modernidade (considerada por muitos como pós-modernidade) passa por um momento de ruptura histórica. Todavia, essa ruptura não representa o fim da sociedade moderna, e sim a sua reconfiguração. Neste contexto, busca-se, também, incluir o bem jurídico tutelado mediante a utilização da doutrina pátria, sobretudo, dos conceitos desenvolvidos pelos autores Damásio de Jesus e José Antônio Milagre, intitulado "Manual de Crimes Informáticos".

Nesse manual dos crimes informáticos, os autores fazem uma aprofundada investigação sobre os temas que circundam o *cibercrime*, desde a concepção, com o surgimento da chamada "sociedade da informação", que tem no seu núcleo a informação como nova fonte de riqueza, passando pela evolução histórica dos *cibercrimes*, no Brasil e no mundo, e se discorre sobre as técnicas utilizadas para a prática desses delitos, e sobre os tipos penais em específico, em vários países. Além disso, os autores analisam a legislação produzida nacionalmente sobre os *cibercrimes*, e todos os aspectos técnicos que decorrem a partir dos crimes, como sujeito ativo e passivo, tipo objetivo e subjetivo, dentre outros.

Na obra do sociólogo alemão Ulrich Beck, o autor discorre sobre a emergência de um novo tipo de sociedade, denominada "sociedade de risco", que surge no contexto do desenvolvimento desenfreado de novas técnicas, e tem como consequência a falta de preocupação, de todos os integrantes da sociedade, acerca dos inúmeros riscos que surgem conjuntamente à essas técnicas desenvolvidas, sobretudo as tecnologias. Se aborda no texto os "riscos dos riscos", uma ideia revelada por Beck que trata sobre o desenvolvimento tecnológico ser acompanhado de apenas previsões sobre os maus acontecimentos, ou seja, não há uma certeza sobre os próprios riscos que essas tecnologias, técnicas de geração energética, alimentos, etc. podem trazer às pessoas, de modo que contamos apenas com uma estimativa sobre as possíveis consequências.

Nesse contexto de sociedade da informação e sociedade de risco é que ganham destaque os crimes cibernéticos, como nova fonte de riscos, oriundos das tecnologias em ascensão, como a *internet*, e os próprios dispositivos informáticos. A sociedade, ao aumentar a sua dependência tecnológica, não aumenta igualmente a sua preocupação com os riscos intrínsecos que tal dependência ocasiona.

A falta de preocupação acaba dando margem para o surgimento de criminosos que se aproveitam desse novo estágio social, no qual as informações mais sensíveis estão sendo veiculadas por meio eletrônico sem o devido cuidado dos usuários que as veiculam.

2.1 A relação entre sociedade de risco e os crimes cibernéticos

Os crimes cibernéticos são um dos frutos do desenvolvimento sem limites da sociedade, pois ocorrem na medida em que a tecnologia proporciona às pessoas novas ferramentas de comunicação, tais como a internet e a transmissão de dados, e a dependência operacional a partir dessas novas ferramentas produz os riscos sociais, tais como a violação de dados de setores públicos e privados, esquemas de fraude contra particulares e empresas. A criminalidade cibernética deve ser considerada uma ameaça à sociedade como um todo, sendo em si uma nova categoria de risco, tendo em vista que afeta diferentes setores de forma específica.

No contexto da "sociedade de risco", pode-se afirmar que tais riscos surgem em razão de uma falsa percepção sobre o estágio atual da sociedade modernizada. Segundo Ulrich Beck (2010, p.13) há um aspecto fundamental sobre a sociedade que não foi previsto nos livros de história, e diz respeito à forma como as mudanças sociais ocorrem: não de maneira revolucionária, mas como resultado das mudanças cotidianas, em consonância com os avanços tecnológicos.

Essa divergência em relação à história registrada e às previsões feitas nos livros diz respeito ao que o autor chama de "mito": o mito de que o estágio atual da sociedade constitui o ápice do que se pode considerar moderno e, por essa razão, somente uma ruptura poderia desencadear grandes mudanças. Esse mito se repete nos livros históricos em diferentes épocas, como no século XIX e XX. O fato é que as mudanças ocorrem quase que de maneira invisível, aos poucos, mediante o incremento das novas criações humanas nos ambientes (Beck, 2010, p. 14).

O estágio atual da sociedade é definido pela herança recebida desses agentes que mal viram os efeitos a longo prazo de uma modernização desenfreada. Beck faz considerações sobre a riqueza acompanhar os riscos, aduzindo que, na nova era, os riscos se sobrepõem às riquezas: não há mais limites territoriais, ou sociais, ou seja, as pessoas afetadas não são mais apenas aquelas que sempre se prejudicaram ao longo da história - os mais pobres - porém, os riscos agora afetam a todos, independentemente de classe social, gênero, etc. E não afetam

somente os humanos: foram expandidos para a natureza, afetando as plantas e animais (Beck, 2010, p. 16-17).

Essa dinâmica da distribuição dos riscos em acompanhamento à distribuição da riqueza se dá em razão da *aparente* carência material que as sociedades acabam causando nas pessoas. É aparente porque não se trata de uma escassez real, mas uma imagem assim criada e desenvolvida como justificativa para a produção desenfreada de novos produtos (tecnologias, alimentos, vestuário), e ocorre com mais força nos países emergentes, nos quais essa ideia da escassez se difunde, por óbvio, com mais facilidade (Beck, 2010, p. 23-24).

Ainda sobre a distribuição dos riscos, observa-se que ocorre de maneira geral, porém diversa nas amplas camadas sociais: enquanto em alguns lugares, por exemplo, há uma escassez verdadeira de comida, ocasionando o risco da fome, em países mais ricos a relação com o alimento é inversa, e as pessoas "sofrem" com o excesso de comida, que, se mal consumida, leva a riscos como a obesidade (Beck, 2010, p. 24).

Essa mesma lógica pode ser observada nos crimes cibernéticos, na medida em que o acesso à tecnologia e aos meios de comunicação mais recentes ocasionam efeitos distintos a depender do meio social. Nas camadas mais abonadas, denota-se a ocorrência de crimes como a invasão de dispositivo eletrônico com o objetivo de "sequestro" de dados sensíveis, como fotos íntimas, que somente terão o acesso restabelecido mediante o pagamento de altas quantias (Teixeira, 2023). Tal exemplo, inclusive, é o que dá origem à "Lei Carolina Dieckmann" (Lei N.º 12.737, de 30 de Novembro de 2012), que foi foi rapidamente aprovada após um episódio que ocorreu com a atriz global, em que teve seus dados sensíveis acessados de forma ilegítima (Jesus, Milagre, 2016, p. 74).

Nas camadas mais pobres da sociedade, as pessoas são vítimas de golpes aplicados por meio de mensageiros como o *WhatsApp*, nos quais os criminosos se aproveitam da falta de instrução e da miserabilidade dos cidadãos, e acabam se apropriando de quantias diversas mediante a obtenção dos dados sensíveis dessas pessoas (Editoria Segurança Pública, 2023).

Nos exemplos citados, vemos a ocorrência de um crime próprio, "invasão de dispositivo informático", e um crime impróprio, nesse caso "estelionato", praticado com auxílio da *internet* (mensageiros eletrônicos) - tais classificações serão abordadas futuramente. Vê-se, portanto, a relação da sociedade de riscos com os crimes cibernéticos, por meio da sua dinâmica de distribuição de riquezas, em comparação à distribuição dos riscos, que ocorre de maneira ampla por todos os estratos sociais, porém de formas distintas.

As diferenças na distribuição dos riscos também revelam o aspecto reflexivo da sua criação. Os próprios criadores, sejam eles donos de grandes empresas, acionistas, ou até

mesmo, em aproximação ao crimes cibernéticos, criadores de novos meios de comunicação, irão acabar sofrendo, cedo ou tarde, as consequências de suas criações, tendo vista o aspecto global dos efeitos que delas decorrem (Beck, 2010, p. 27).

Outro reflexo importante que pode ser observado, quanto à mudança da criação e disseminação dos riscos, em uma sociedade histórica em relação à atual, diz respeito à própria origem: enquanto os riscos nas épocas mais antigas ocorriam por uma *falta* de tecnologia e bens de consumo, na atual conjuntura ocorrem pelo *excesso*, ou pela *super*produção desses recursos (Beck, 2010, p. 26). E a circunstância observada está diretamente ligada aos crimes cibernéticos, eis que surgiram concomitantemente às novas tecnologias de comunicação, ou seja, não em razão da falta, como no passado, mas pelo excesso, no agora, e provável futuro.

A tendência de disseminação dos riscos é acompanhada pela lógica capitalista, porém, para os riscos não há limite, diferente da riqueza acumulável. E só tende a aumentar, a ponto de se tornar - os riscos - um aspecto que afeta a política da nossa sociedade (Beck, 2010, p. 28). Atualmente, pode-se afirmar que os crimes cibernéticos mais perigosos são aqueles em que as vítimas são os próprios governos, que mantêm em sua base de dados os conteúdos sensíveis da sua população, e a crescente ameaça desses crimes, que não parece frear, se torna uma questão que precisa de um forte enfrentamento por parte das forças estatais (Jesus, Milagre, 2016, p. 23-25).

Outro aspecto da sociedade de riscos que se liga aos crimes cibernéticos diz respeito à maneira como são calculados os riscos. Em razão de usarmos os instrumentos de medida que estão disponíveis atualmente, e que não necessariamente acompanham a evolução das tecnologias que produzem os resíduos a serem analisados, estamos presos a dados que, muitas vezes, não refletem a realidade. E isso ocorre também em razão do método de avaliação desses dados, que nem sempre levam em conta os aspectos sociais e culturais, mas, em muitas vezes, apenas os números, friamente (Beck, 2010, p. 29-30).

A conexão mencionada ocorre na medida em que, ao criar novos meios tecnológicos - aplicativos de comunicação, transferência de dados - seus criadores não possuem os meios necessários a fim de calcular as possíveis implicações, como os crimes que surgem aliados a essas novas criações. E essa condição é crescente, pois o desenvolvimento dessas novas tecnologias não parece estar diminuindo, ao contrário, todos os dias surgem novas possibilidades para os criminosos, e ficamos à mercê desses indivíduos, que se aproveitam dessa falta de preocupação, ou aptidão, para desvendar as consequências negativas desse desenvolvimento.

Essa falta de percepção, ou dos instrumentos adequados, torna os riscos e ameaças invisíveis, até o ponto em que acabam afetando invariavelmente todas as pessoas, que não os percebem até que seja tarde demais (Beck, 2010, p. 32), e isso ocorre também nos crimes cibernéticos, pois, em muitos casos, sequer há uma punição adequada aos criminosos, em vista da total ausência de legislações que descrevem as condutas.

Ou seja, essa "dependência cognitiva" dos riscos é uma consequência também observada nos crimes cibernéticos, tendo em vista que não podemos puni-los, sem antes sabermos como ocorrem, e contra quem são cometidos, ou, de que forma identificar os criminosos. A falta de identificação desses fatores, aprioristicamente, dificulta o enfrentamento apropriado, e isso é consequência do novo modelo social criado a partir da sociedade de risco (Beck, 2010, p. 33).

2.2 A informação como bem jurídico tutelado

A conceituação de bem jurídico passou por várias transformações ao longo do tempo, porém, de maneira simplificada, poderia ser definido como um objeto, comportamento, ou idéia, que merece uma atenção maior por parte do Estado, a fim de ser elevado à uma categoria que o difere dos demais, ou seja, são as coisas que devemos dar uma proteção maior, por diferentes motivos, dentre eles, o econômico.

A visão de "bem jurídico" serve como fator limitador da atuação estatal, e pode ser considerado uma garantia dos cidadãos, eis que o Estado é obrigado a observar o chamado "Princípio da Ofensividade", o qual estabelece, em linhas gerais, que o Direito Penal somente pode interferir em situações em que o bem jurídico penal se encontra ameaçado ou lesionado (Smanio, 2004).

A teoria do bem jurídico sofre críticas, porém os seus defensores afirmam que a delimitação do "bem jurídico" penal se realiza na medida em que são tipificadas as condutas. Essa visão não serve para definir o conceito do bem jurídico, mas para definir quais são os bens efetivamente protegidos pela legislação, em determinado momento histórico. Isso porque, a norma positivada não é o único elemento de formação do Direito, sendo apenas o estágio "final", quando o bem jurídico deixa de se tornar uma ideia, e passa a ser protegido juridicamente pela legislação penal (Smanio, 2004).

É por essa razão que deve ser analisado o conceito a partir da perspectiva social, ou seja, do ponto de vista do interesse à sociedade e a sua manutenção, como condições imprescindíveis, para então, após manifestada como uma preocupação social, sofrer a

tipificação penal, com a punição adequada aos indivíduos que acabam violando esses bens que foram antes manifestamente considerados como importantes no meio social (Smanio, 2004).

A tipificação penal também exprime uma ideia de disponibilidade: a possibilidade do indivíduo desfrutar dos bens jurídicos penais, que no fim são considerados objetos materiais. Esses objetos materiais, conforme dito, passam por uma valoração maior por parte da sociedade, de acordo com a reprovabilidade das condutas que interferem na fruição dos objetos, e assim merecedores da tutela penal (Smanio, 2004).

No fim das contas, a tutela penal deve ser a última alternativa para a proteção desses bens socialmente relevantes, devendo, sempre que possível, ocorrer a proteção por outros ramos do Direito, como o Direito Civil ou Administrativo (Smanio, 2004).

Nesse sentido, a própria Constituição Federal se apresenta como um fator de limitação à perspectiva social de bens jurídicos, com a criação dos princípios que auxiliam os legisladores na tipificação das condutas. Isso significa que na Constituição não serão encontrados os bens jurídicos penais a serem tutelados, mas um direcionamento, por meio dos princípios, para que ocorra a punição de maneira adequada, assim como diretrizes gerais sobre formas de punição mais graves em determinados casos extremos, e condutas abertas, que devem ser delimitadas pelos legisladores (Smanio, 2004).

Essas limitações, inicialmente, os princípios, podem ser encontradas no artigo 5º da Constituição Federal de 1988, no qual se encontra disposto o "Princípio da Legalidade" no inciso XXXIX, o qual estabelece que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal" (Brasil, 1988, art. 5º, XXXIX). Encontra-se também o "Princípio da irretroatividade da lei penal", conforme o inciso XL: "a lei penal não retroagirá, salvo para beneficiar o réu"(Brasil, 1988, art. 5º, XL). Assim como o "Princípio da responsabilidade pessoal" incluso no inciso XLV: "nenhuma pena passará da pessoa do condenado, podendo a obrigação de reparar o dano e a decretação de perdimento de bens ser, nos termos da lei, estendidas aos sucessores e contra eles executadas [...]" (Brasil, 1988, art. 5º, XLV). Há também o "Princípio da presunção da inocência" no inciso LVII: "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória" (Brasil, 1988, art. 5º, LVII). E ainda, "Princípio da individualização da pena", encontrado no inciso XLVI: "a lei regulará a individualização da pena e adotará, entre outras, as seguintes: a) privação ou restrição de liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão ou interdição de direitos" (Brasil, 1988, art. 5º, XLVI, *in* Smanio, 2004).

Observa-se, a partir das disposições constitucionais, que não há definição dos bens a serem juridicamente tutelados, mas se encontra uma série de limitações ao legislador, que devem ser observadas no momento da criação das leis que levarão à punição dos agentes que oferecem ameaça, ou lesão aos bens (Smanio, 2004).

Além de impor limites nos princípios, a Constituição também impõe uma vedação aos legisladores, que não podem proteger, por exemplo, bens incompatíveis com o racismo e discriminações decorrentes do sexo, religião, ou crença (Smanio, 2004).

Além dos limites impostos pelos princípios, denota-se a maior preocupação da Constituição com relação a determinados temas - sem definir precisamente as tutelas penais -, que também são incluídos no artigo 5º (Smanio, 2004):

> Art. 5.º […]
> XLI – a lei punirá qualquer discriminação atentatória aos direitos e liberdades fundamentais;
> XLII – a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;
> XLIII – a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática de tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem;
> XLIV – constitui crime inafiançável e imprescritível a ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático;
> [...] (Brasil, 1988, art. 5º).

Infere-se a tipificação da necessidade de se punir condutas que atentem aos direitos e liberdade fundamentais, porém se observa também a preocupação com o tipo de pena que deve incorrer a pessoa que pratica o racismo. Outrossim, há disposições de cunho processual criminal, quanto à fiança, atribuída a crimes específicos: tortura e tráfico de entorpecentes, o terrorismo, e mais genericamente, os crimes hediondos, com a punição de copartipantes, tais como, o mandante do crime.

Essa preocupação acentuada nos incisos do artigo 5º acima mencionados se deve ao momento histórico em que foi elaborada a Constituição - pós ditadura - e exprime a tentativa de evitar esse trágico episódio de ruptura política ocorrida no país, levando à criminalização, conforme anotado, de crimes que atentam contra a ordem constitucional e o Estado Democrático, e a direitos e liberdades fundamentais, o terrorismo, entre outros (Smanio, 2004).

Outra razão para essa estrutura constitucional são os fatores socioeconômicos do país, quando se observa a punição mais severa aos crimes de tráfico e racismo, que ressaltam os

princípios que norteiam a própria Constituição, e a resposta que se busca oferecer a tais ilícitos penais (Smanio, 2004).

Essa estrutura socioeconômica também levou à tipificação dos artigos 225, § 3.º, e 227, § 4.º:

> Art. 225. […]
> § 3.º As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados.
> […]
> Art. 227. […]
> § 4.º A lei punirá severamente o abuso, a violência e a exploração sexual da criança e do adolescente.
> […] (Brasil, 1988, artigos 225 e 227).

Nesse trecho da Constituição revela-se a preocupação em se proteger o futuro da sociedade, a partir da conservação ambiental, e o cuidado com crianças e adolescentes, considerando que são os indivíduos em desenvolvimento destinados a serem os futuros cidadãos do país. A partir dessa significativa preocupação, a Constituição determina a necessidade de proteção através de medidas criminais. O critério que determina a imposição dessas previsões constitucionais pode ser considerado como a relevância do bem jurídico, que, em última instância, leva à necessária tutela penal, com a disposição de leis incriminadoras (Smanio, 2004).

No caso da informação, o principal motivo que eleva esse bem à categoria de ser juridicamente tutelado pelo direito penal é o seu alto valor econômico, tendo em vista que na sociedade atual, a informação, ou, os dados, sejam eles pessoais, ou não, constituem uma parte enorme das relações sociais (Fuller, Tateoki, p. 4).

Nesse sentido, a relevância econômica das informações, ou dados, deve ser acompanhada por uma relevante atuação jurídica em correspondência. Surge então a necessidade de proteger a integridade das informações, abrangendo dados bancários, financeiros e outras informações manipuladas por indivíduos e entidades jurídicas.

Há a necessidade também de proteger o meio em que circulam os dados e informações, que são, atualmente, os sistemas computacionais, responsáveis pelo processamento e tratamento de dados eletrônicos, gerando significado e informações valiosas. Portanto, merecem igualmente a proteção jurídica estatal, dado que as informações que circulam nesses meios são consideradas bens preciosos (Jesus, Milagre, 2016, p. 48).

Sendo assim, ao tratarmos de “crimes informáticos”, os definimos em razão da violação às informações e dados privados que circulam no meio eletrônico, e essa violação

dos dados e informações é o que constitui o juízo de reprovação por parte do Estado (Jesus, Milagre, 2016, p. 48).

Nos crimes informáticos, portanto, a informação em si constitui o bem jurídico a ser tutelado pelo Estado, diante do seu elevado valor econômico, que decorre das mais diferentes fontes: dados bancários, informações sensíveis de particulares e entes públicos, fotos e vídeos íntimos, dentre outros. Essa relevância constitui o motivo pelo qual são criadas as legislações a fim de proteger esse bem jurídico, e no mundo inteiro são editadas e aprovadas novas leis, em atenção à Convenção de Budapeste.

Entretanto, a partir da análise das legislações editadas mundo afora se observa que o bem jurídico tutelado pelas condutas descritas vai além da informação em si. A própria "informática" poderia ser considerada como o bem jurídico a ser tutelado nesses casos, pois constitui, não somente o meio, porém o fim escolhido pelos criminosos que pretendem obter alguma vantagem ilícita (Jesus, Milagre, 2016 p. 49).

Ao serem previstas condutas que utilizam a informática como meio para a prática de delitos comuns, os países manifestam a preocupação com os bens "acessórios" da informação, ou seja, os dispositivos de armazenamento, e a preservação deles, assim como os sistemas em si, que fazem o tratamento dessas informações.

Além disso, se observa que, em atenção à Convenção de Budapeste, os países se preocuparam em oferecer uma proteção preventiva, ao penalizar a tentativa dos crimes cibernéticos, e também, abrangente, em razão da previsão da punição aos agentes que auxiliam no resultado na conduta final, mediante a disponibilização dos meios para a prática das condutas previstas.

A dificuldade em se definir o "bem jurídico" está relacionada com a própria natureza desse conceito, sendo considerado dinâmico, variável de acordo com os avanços da ciência e da própria sociedade (Smanio, 2004).

Em razão dessa dinamicidade, estabelecer o bem jurídico protegido nos crimes cibernéticos também se apresenta uma tarefa delicada, como se observa, sendo aptos a figurar como significantes desse conceito, tanto a informação em si, como a informática - abrangendo dispositivos, sistemas, palavras-chave (que em última análise são dados) -, ou ainda, a privacidade dos indivíduos que são vítimas de alguns crimes previstos, sendo exemplos a invasão de dispositivo informático - crime previsto na legislação brasileira, conforme será detalhado no tópico 3.3.

3 LEGISLAÇÕES SOBRE CRIMES CIBERNÉTICOS PRODUZIDAS NOS PAÍSES MUNDO AFORA

No presente capítulo será examinada a legislação penal aplicada sobre crimes cibernéticos produzida mundialmente quanto à previsão da cumplicidade. São muitos os países em que são encontradas legislações sobre o *cibercrime*, e segundo a base de dados da ONU (sherloc.unodc.org), existem pelo menos 1.564 leis que tratam do tema.

A partir da base de dados mencionada, foram filtradas as leis que tratam sobre o *cibercrime* - *cybercrime* -, e a partir dessa lista são trazidos os resultados que serão a seguir discutidos.

3.1 Legislação sobre o *cibercrime* produzida em Portugal

Primeiramente, optou-se pela escolha de Portugal, por ser um país europeu, continente do qual o Brasil possui referências históricas no âmbito do direito, e em razão do idioma falado ser o Português.

A partir dos resultados obtidos na base de dados da ONU - Unodc -, buscou-se a legislação original na *internet*, para ser observada nos seus próprios termos, tendo em vista que na base de dados é realizada a tradução para o inglês, mas não se considera uma tradução oficial.

Nesse país são encontradas disposições específicas sobre crimes cibernéticos no Código Penal Português, com a presença do artigo n.º 221, que trata do crime "Burla informática e nas comunicações". Assim está disposto o artigo:

> Burla informática e nas comunicações
> 1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de dados, estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.
> 2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.
> 3 - A tentativa é punível.
> 4 - O procedimento criminal depende de queixa.
> 5 - Se o prejuízo for:
> a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;

> b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.
> 6 - É correspondentemente aplicável o disposto no artigo 206.º (Portugal, 1995, art. 221).

Observa-se no artigo alguns pontos-chaves: o autor do crime é punível com pena de prisão de até 3 anos, quando manifesta intenção de obter para si mesmo, ou para terceiro, um enriquecimento ilegítimo, causando a outra pessoa um prejuízo patrimonial. Ou seja, o agente é punível ainda que a vantagem seja obtida para outra pessoa, e além disso, pressupõe-se que essa vantagem seja econômica, não sendo punidas as condutas que não tenham esse fim específico.

Além disso, se observa no tipo penal que não é necessário um resultado material, sendo punível a tentativa, bem como, observa-se que o crime se processa mediante queixa. Outra característica interessante é a inclusão de termos abertos, como prejuízo de "valor elevado", e "consideravelmente elevado". Essa previsão está presente em praticamente todos os crimes analisados na legislação portuguesa.

Na parte final do artigo se encontra a disposição acerca da aplicação, correspondentemente, do disposto no artigo 206º. Esse artigo trata da "restituição ou reparação", conforme o texto integral:

> Restituição ou reparação
> 1 - Nos casos previstos nas alíneas a), b) e e) do n.º 1, na alínea a) do n.º 2 do artigo 204.º e no n.º 4 do artigo 205.º, extingue-se a responsabilidade criminal, mediante a concordância do ofendido e do arguido, sem dano ilegítimo de terceiro, até à publicação da sentença da 1.ª instância, desde que tenha havido restituição da coisa ou do animal furtados ou ilegitimamente apropriados ou reparação integral dos prejuízos causados.
> 2 - Quando a coisa ou o animal furtados ou ilegitimamente apropriados forem restituídos, ou tiver lugar a reparação integral do prejuízo causado, sem dano ilegítimo de terceiro, até ao início da audiência de julgamento em 1.ª instância, a pena é especialmente atenuada.
> 3 - Se a restituição ou a reparação forem parciais, a pena pode ser especialmente atenuada (Portugal, 1995, art. 206).

Aparentemente, a partir da leitura do artigo, depreende-se que, mediante a concordância da vítima, e sem que haja dano a terceiro, até que seja publicada a sentença, se houver a restituição da coisa, no caso da "Burla informática", a vantagem econômica obtida, será extinta a responsabilidade criminal do agente. Denota-se que também é possível uma atenuação da pena, em casos específicos, como a restituição parcial da vantagem, ou na hipótese dessa restituição ocorrer em outro momento. Nessa conduta típica não se verifica a punição do cúmplice que eventualmente auxilia mediante fornecimento de dispositivo.

Além do Código Penal, são encontradas disposições sobre crimes cibernéticos numa legislação específica sobre o tema, intitulada "Lei do *Cibercrime*", ou, Lei n.º 109/2009.

A Lei do *Cibercrime* de Portugal conta com uma parte geral na qual são dispostas definições próprias desses tipos penais, em observância à Convenção de Budapeste, para elucidar conceitos que não estão presentes nos crimes de outra espécie, como a definição de "sistema informático", "dados informáticos", "dados de tráfego", "fornecedor de serviço", "intercepção", "topografia", e "produto semicondutor".

Nos crimes em específico, se encontra tipificada a conduta de "Falsidade informática", que assim está disposta:

> Artigo 3.º
> Falsidade informática
> 1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.
> 2 - Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.
> 3 - Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.
> 4 - Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos.
> 5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos (Portugal, 2009, art. 3.º).

A partir do artigo citado, observa-se que é uma conduta específica para punir o agente que causa "engano nas relações jurídicas", por meio de várias ações (introduzir, modificar etc.) no tratamento de dados informáticos, aptas a produzir outros dados, ou documentos, com informação falsa, e assim angariar vantagem em situações jurídicas.

Importantes trechos do artigo citado são encontrados no n.º 2 e 4, que tratam sobre os dispositivos que auxiliam na prática da falsidade informática, e do agente que os produz, adquire, importa etc. esses dispositivos, sendo ele punível com pena equivalente a do autor da conduta principal.

Infere-se, portanto, que não somente será punido o criminoso que atua diretamente na alteração (introduzir, modificar, apagar ou suprimir) dos dados informáticos, como também

aquele que auxilia materialmente, provendo dispositivo, ou programa, ou ainda dados, destinados à prática dessa alteração.

Outro crime encontrado na Lei do *Cibercrime* é o de "Dano relativo a programas ou outros dados informáticos":

> Artigo 4.º
> Dano relativo a programas ou outros dados informáticos
> 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.
> 2 - A tentativa é punível.
> 3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.
> 4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.
> 5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.
> 6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa (Portugal, 2009, art. 4.º).

Esse tipo penal prevê a conduta do agente que acessa um sistema informático, de maneira ilegítima (sem permissão), ou ainda parte do sistema, e altera (apagar, destruir etc.) os programas ou dados informáticos, com o objetivo de afetar a capacidade de uso.

Depreende-se que o agente nesse caso não obtém, diretamente, uma vantagem para si, ou para outrem, mas procura unicamente causar dano no sistema informático, a fim de torná-lo inutilizável, ou afetar o seu potencial de utilização.

Igualmente como na tipificação do Código Penal Português para "Burla informática e nas comunicações", a tentativa é punível, não sendo, portanto, necessário o resultado material. Outrossim, se encontra disposta a punição para o agente que auxilia materialmente o autor da conduta principal, mediante fornecimento (produzir, vender etc.) de dispositivo, programa, ou dados, destinado à prática dessa conduta. Outra característica que se repete são as disposições de termos abertos: "valor elevado", e "valor consideravelmente elevado", assim como, o procedimento penal depende de queixa em casos específicos. Trata-se o tipo descrito de um crime impróprio, os quais não serão tratados nas legislações analisadas adiante.

A conduta típica seguinte, o artigo 5º da legislação, descreve a "Sabotagem informática", que possui redação bastante semelhante ao crime descrito no artigo 5º da Convenção de Budapeste - que será tratada em específico no tópico 4.3 e seguintes:

> Artigo 5.º
> Sabotagem informática
> 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.
> 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
> 3 - Nos casos previstos no número anterior, a tentativa não é punível.
> 4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.
> 5 - A pena é de prisão de 1 a 10 anos se:
> a) O dano emergente da perturbação for de valor consideravelmente elevado;
> b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos (Portugal, 2009, art. 5.º).

Esse crime parece ser uma versão mais grave do dano informático, eis que são descritas mais verbos de ação, e necessita de complemento, pela introdução, transmissão, deterioração etc. de programas, dados, ou qualquer outra forma de interferência nos sistemas informáticos, com acréscimo de pena. Nesse tipo também se verifica a punição ao cúmplice que auxilia com dispositivos, programas ou dados destinados a produzir o resultado da conduta principal.

Diferente do tipo anterior, neste a tentativa não é punível, e são encontrados novamente as expressões abertas: “valor elevado” e “valor consideravelmente elevado”. Um aspecto relevante é a punição ainda maior nos casos de perpetuação da conduta - perturbação duradoura - ou quando ocorre de maneira “grave” contra “funções sociais críticas”, a exemplo das “cadeias de abastecimento”, a “saúde”, a “segurança e o bem-estar económico das pessoas”, ou ainda “o funcionamento regular dos serviços públicos”.

O artigo seguinte também demonstra-se relevante para a pesquisa:

> Artigo 6.º
> Acesso ilegítimo
> 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
> 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros

> dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
> 3 - A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.
> 4 - A pena é de prisão até 3 anos ou multa se:
> a) O acesso for conseguido através de violação de regras de segurança; ou
> b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.
> 5 - A pena é de prisão de 1 a 5 anos quando:
> a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
> b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
> 6 - A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3.
> 7 - Nos casos previstos nos n.os 1, 4 e 6 o procedimento penal depende de queixa (Portugal, 2009, art. 6.º).

Esse dispositivo tipifica como conduta criminal o mesmo "Acesso ilegítimo" que se encontra na Convenção de Budapeste (tópico 4.3.1), e aprofunda-o, com disposições sobre o cúmplice que auxilia materialmente para alcançar o fim descrito na conduta principal.

No artigo citado são encontrados, ainda, aplicações de penas de modo diferenciado a depender da gravidade ou fim obtido com a conduta. Novamente é encontrado o mesmo termo aberto: "valor consideravelmente elevado". E igualmente é punível a tentativa, e também há previsão da necessidade de queixa, em determinadas hipóteses.

Os legisladores nesse caso foram além do que se exige, ou recomenda, na Convenção de Budapeste, ao prever o aumento de pena no caso agravamento das condutas, como "Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei".

O próximo artigo da lei ora analisada, que trata da "Intercepção ilegítima", também encontra correspondente quase idêntico na Convenção de Budapeste (tópico 4.3.2):

> Artigo 7.º
> Intercepção ilegítima
> 1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.
> 2 - A tentativa é punível.
> 3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número (Portugal, 2009, art. 7.º).

Denota-se uma diferença nesse tipo penal que diz respeito ao modo como é praticado: é consignada a expressão “através de meios técnicos”, o que não consta nas outras condutas, tratando-se de um termo aberto, eis que podem ser incluídos nessa expressão os mais variados “meios”.

Assim como na maior parte dos crimes descritos até agora, a tentativa é punível, além de haver uma punição para o cúmplice que auxilia materialmente o autor da conduta principal mediante fornecimento de dispositivos, programas ou outros dados informáticos que se destinam a produzir os resultados da conduta principal.

Por fim, em observância aos parâmetros filtrados a partir da base de dados da ONU (Unodc), na Lei do *Cibercrime*, está disposto o art. 8º, que trata, basicamente, de uma espécie de pirataria[1] de programa informático:

> Artigo 8.º
> Reprodução ilegítima de programa protegido
> 1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.
> 2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.
> 3 - A tentativa é punível (Portugal, 2009, art. 8.º).

Conforme mencionado, a conduta descrita é conhecida popularmente como “pirataria”, sendo bastante comum essa prática desde o surgimento da *internet*, e é considerada “o crime do século XXI”, capaz de movimentar mais recursos do que o narcotráfico (Dantas, 2023).

Mais uma vez, a tentativa é punível, e surge uma conduta de participação diferente daquela encontrada nos demais crimes, que a é de reprodução de “topografia de um produto semicondutor”[2], ou a exploração comercial, ou importação para este fim, uma topografia de ou o próprio produto semicondutor, que é fabricado a partir dessa topografia.

A Lei do *Cibercrime* de Portugal, conta com outros diversos artigos, que dispõem sobre outras condutas criminosas em âmbito eletrônico, além de artigos sobre procedimentos a serem adotados no combate desses crimes, porém aqui foram trazidos os trechos identificados a partir do filtro para “*Cybercrimes*”, junto ao banco de dados Unodc.

---

[1] Pirataria ou pirataria moderna, como alguns denominam, é a prática de vender ou distribuir produtos sem a expressa autorização dos proprietários de uma marca ou produto. A pirataria é considerada crime contra o direito autoral, a pena para este delito pode chegar a quatro anos de reclusão e multa (Dantas).

[2] Definição de topografia de um produto semicondutor:
Topografia de um produto semicondutor é o conjunto de imagens relacionadas, quer fixas, quer codificadas, que representem a disposição tridimensional das camadas de que o produto se compõe, em que cada imagem possua a disposição, ou parte da disposição, de uma superfície do mesmo produto, em qualquer fase do seu fabrico (Portugal, 2018, art. 154).

A partir das leis aqui trazidas foi possível observar que o legislador português foi bastante atento às previsões contidas na Convenção de Budapeste, sendo registrados na legislação todos os crimes próprios da Convenção, além de estar previsto, em quase todas as condutas, a punição ao agente que auxilia materialmente o autor do crime principal.

Outras condutas criminosas, impróprias, também estão presentes na legislação Portuguesa, como é o caso do "Dano relativo a programas ou outros dados informáticos", anteriormente analisado, que nada mais é do que o crime de "Dano", encontrado no artigo 163 do Código Penal brasileiro, e igualmente no artigo 212º do Código Penal português:

> Dano
> Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:
> Pena - detenção, de um a seis meses, ou multa (Brasil, 1940, art. 163).
>
> Artigo 212.º
> Dano
> 1 - Quem destruir, no todo ou em parte, danificar, desfigurar ou tornar não utilizável coisa ou animal alheios, é punido com pena de prisão até três anos ou com pena de multa.
> 2 - A tentativa é punível.
> 3 - O procedimento criminal depende de queixa.
> 4 - É correspondentemente aplicável o disposto nos artigos 206.º e 207.º (Portugal, 1995, art. 212).

Observa-se, portanto, que a legislação portuguesa sobre crimes cibernéticos está bastante completa, quando analisada em comparação à Convenção de Budapeste e os crimes próprios nela previstos, sendo que há inclusões além do que se recomenda nos artigos da Convenção.

3.2 Legislação sobre o *cibercrime* produzida nos Estados Unidos da América

O Estados Unidos da América (EUA) possui um sistema jurídico amplamente diferente do Brasil, porém, possuem leis escritas que podem ser analisadas em comparação às previsões contidas na Convenção de Budapeste, a fim de investigar se nessas legislações são encontradas as referências, exigências, ou recomendações previstas na Convenção.

Tal como realizado na pesquisa sobre Portugal, utilizou-se a ferramenta disponibilizada pela ONU (Unodc), e a partir do filtro de legislações sobre *cibercrime* - *Cybercrime* no original do site - foi selecionada a legislação que trata especificamente de crimes próprios.

Na lei encontrada são dispostos vários aspectos procedimentais, assim como uma parte geral, com a definição de termos que são utilizados no texto legal, e por tal razão, serão exibidos os trechos da lei que se demonstram relevantes à pesquisa - as condutas criminosas, basicamente.

Tendo em vista que a legislação é escrita originalmente no idioma inglês, será feita a tradução livre, com apoio do "Google tradutor".

A legislação a ser analisada é intitulada originalmente como "United States Code, Title 18, Section 1030", que, traduzida, pode ser lida como "Código dos Estados Unidos, Título 18, seção 1030":

> 1030. Fraude e atividades relacionadas relacionadas a computadores
> (a) Quem-
> (1) ter acessado (ou, acessar) conscientemente um computador sem autorização ou excedendo o acesso autorizado, e por meio de tal conduta ter obtido informações que foram determinadas pelo Governo dos Estados Unidos de acordo com uma ordem executiva ou estatuto para exigir proteção contra divulgação não autorizada por motivos de interesse nacional defesa ou relações exteriores, ou quaisquer dados restritos, conforme definido no parágrafo y. da seção 11 da Lei de Energia Atômica de 1954, com motivos para acreditar que tais informações assim obtidas poderiam ser usadas em prejuízo dos Estados Unidos ou em benefício de qualquer nação estrangeira que deliberadamente comunique, entregue, transmita ou faça com que seja comunicado, entregue ou transmitido, ou tenta comunicar, entregar, transmitir ou fazer com que seja comunicado, entregue ou transmitido o mesmo a qualquer pessoa sem direito a recebê-lo, ou retém intencionalmente o mesmo e não o entrega ao oficial ou funcionário dos Estados Unidos com direito a recebê-lo;
> (2) **acessa intencionalmente um computador sem autorização ou excede o acesso autorizado** e, assim, obtém-
> (A) informações contidas em um registro financeiro de uma instituição financeira ou de um emissor de cartão, conforme definido na seção 1602 (n) 1 do título 15, ou contidas em um arquivo de uma agência de relatórios ao consumidor sobre um consumidor, conforme tais termos são definido no Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> (B) informações de qualquer departamento ou agência dos Estados Unidos; ou
> (C) **informações de qualquer computador protegido**;[3] (Estados Unidos, 1986, seção 1030 - grifo próprio; tradução própria).

[3] Em inglês: §1030. Fraud and related activity in connection with computers
(a) Whoever-
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) 1 of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer;

Os trechos destacados trazem disposições semelhantes àquelas encontradas no artigo 2º da Convenção de Budapeste, que trata do "acesso ilegítimo" (tópico 4.3.1), e a partir da simples leitura da legislação americana se percebem as diferenças em comparação à lei brasileira e portuguesa. Logo no início é indicado a "subseção" (no original *subsection*) "(a) Quem", para se referir a qualquer pessoa, e abaixo utiliza-se números "(1)", "(2)" para indicar a conduta penalizada. Além disso, há outra divisão, utilizando-se letras em maiúsculo, "(A)", "(B)" a fim de indicar um complemento da conduta.

A penalização das condutas é indicada somente depois, com a escrita: "*shall be punished as provided in subsection (c) of this section.*", que traduzida, pode ser lida como "será punido conforme previsto na subseção (c) desta seção." As penas também são descritas de maneira bastante diversa da lei brasileira e portuguesa, conforme se observa da subseção "(c)":

> (c) A punição por uma infração nos termos da subseção (a) ou (b) desta seção é-
> (1)(A) uma multa sob este título ou prisão por não mais de dez anos, ou ambos, no caso de um delito nos termos da subseção (a)(1) desta seção que não ocorra após uma condenação por outro delito nos termos desta secção, ou uma tentativa de cometer um crime punível nos termos desta alínea; e
> (B) uma multa sob este título ou prisão por não mais de vinte anos, ou ambos, no caso de um delito nos termos da subseção (a) (1) desta seção que ocorra após uma condenação por outro delito nos termos desta seção, ou uma tentativa de cometer um crime punível nos termos desta alínea;
> (2)(A), exceto conforme previsto no subparágrafo (B), uma multa sob este título ou prisão por não mais de um ano, ou ambos, no caso de um delito nos termos da subseção (a)(2), (a) (3), ou (a)(6) desta seção que não ocorra após uma condenação por outro delito nos termos desta seção, ou uma tentativa de cometer um delito punível nos termos deste subparágrafo;
> (B) uma multa sob este título ou prisão por não mais de 5 anos, ou ambos, no caso de um delito nos termos da subseção (a) (2), ou uma tentativa de cometer um delito punível nos termos deste subparágrafo, se-
> (i) o crime foi cometido para fins de vantagem comercial ou ganho financeiro privado;
> (ii) o crime foi cometido em prol de qualquer ato criminoso ou ilícito que viole a Constituição ou as leis dos Estados Unidos ou de qualquer Estado; ou (iii) o valor das informações obtidas excede US$ 5.000;[4](Estados Unidos, 1986, seção 1030 - tradução própria)

[4]Em inglês: (c) The punishment for an offense under subsection (a) or (b) of this section is-
(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if-
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000;

Observa-se que as penas são aplicadas a partir do preenchimento de critérios diversos, como o caso de ser o agente reincidente ou não, "que não ocorra **após uma condenação por outro delito** nos termos desta secção, ou uma tentativa de cometer um crime punível nos termos desta alínea" (grifou próprio), ou com agravantes, "o crime foi cometido **para fins de vantagem comercial** ou ganho financeiro privado" (grifo próprio).

Denota-se que ocorre uma combinação, do que seria no Brasil, da parte geral junto à parte especial do Código Penal, ao ser previsto, na mesma seção, hipóteses classificadoras da reincidência, por exemplo.

Igualmente como é previsto na legislação portuguesa analisada anteriormente, são punidas a tentativa, e o auxílio material do cúmplice: "(b) Quem **conspirar para cometer** ou **tentar cometer** um delito nos termos da subseção (a) desta seção **será punido conforme previsto na subseção (c)** desta seção." (grifo próprio).

Nas disposições seguintes da Seção, são encontradas várias descrições de resultados que ocasionam punições diferentes em cada caso, o que demonstra uma busca por abarcar a maior quantidade de condutas possível, a fim de deixar a lei o menos aberta possível, ou seja, com termos indeterminados, tal como ocorre em alguns trechos da lei portuguesa.

A lei dos EUA demonstra uma robustez maior em comparação à lei portuguesa, pois são abarcadas várias situações diferentes no próprio texto legislativo, deixando uma margem menor ao juiz para subjetividades, ou seja, a própria legislação conta com a descrição de condutas finais, e dão maior segurança acerca da efetividade da punição, tendo em vista que não são necessárias interpretações delongadas sobre as situações fáticas.

Conforme mencionado, nas demais "subseções" da lei são encontradas as definições dos termos utilizados no texto que descreve as condutas a serem punidas, revelando, novamente, uma maior preocupação em evitar termos abertos:

> (5) o termo "registro financeiro" significa informações derivadas de qualquer registro mantido por uma instituição financeira referente ao relacionamento de um cliente com a instituição financeira;
> (6) o termo "excede o acesso autorizado" significa acessar um computador com autorização e usar esse acesso para obter ou alterar informações no computador que o acessante não tem o direito de obter ou alterar;
> (7) o termo "departamento dos Estados Unidos" significa o poder legislativo ou judicial do Governo ou um dos departamentos executivos enumerados na secção 101 do título 5;
> (8) o termo "dano" significa qualquer prejuízo à integridade ou disponibilidade de dados, um programa, um sistema ou informações;
> (9) o termo "entidade governamental" inclui o Governo dos Estados Unidos, qualquer Estado ou subdivisão política dos Estados Unidos, qualquer país

> estrangeiro e qualquer estado, província, município ou outra subdivisão política de um país estrangeiro;
> (10) o termo "condenação" incluirá uma condenação ao abrigo da lei de qualquer Estado por um crime punível com pena de prisão superior a um ano, cujo elemento seja o acesso não autorizado, ou que exceda o acesso autorizado, a um computador;
> (11) o termo "perda" significa qualquer custo razoável para qualquer vítima, incluindo o custo de responder a um delito, conduzir uma avaliação de danos e restaurar os dados, programas, sistemas ou informações à sua condição anterior ao delito, e qualquer perda de receita, custos incorridos ou outros danos consequentes incorridos devido à interrupção do serviço;
> (12) o termo "pessoa" significa qualquer indivíduo, empresa, corporação, instituição educacional, instituição financeira, entidade governamental ou entidade legal ou outra entidade;
> (13) o termo "eleição federal" significa qualquer eleição (conforme definido na seção 301(1) da Lei de Campanha Eleitoral Federal de 1971 (52 U.S.C. 30101(1))) para cargos federais (conforme definido na seção 301(3) da Lei de Campanha Eleitoral Federal de 1971 (52 U.S.C. 30101(3))); e (14) o termo "sistema de votação" tem o significado atribuído ao termo na seção 301 (b) da Help America Vote Act de 2002 (52 U.S.C. 21081 (b)).[5](Estados Unidos, 1986, seção 1030 - tradução própria).

Em resumo, a lei americana é mais completa do ponto de vista das lacunas, e isso é uma condição descrita por Damásio de Jesus e José Antônio Milagre no "Manual de Crimes informáticos" (2016, p. 65), no qual se discorre que, os EUA, apesar não ser o país a legislar primeiramente sobre os crimes cibernéticos, são uma das nações que combate com mais força esses delitos, e o que difere o país dos demais é a aplicação de leis federais e estaduais em conjunto, sendo que a lei federal serve como subsidiária, oferecendo uma liberdade para legislar maior, e assim uma capacidade para englobar um número maior de condutas descritas.

---

[5] Em inglês: (5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity;
(13) the term "Federal election" means any election (as defined in section 301(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(1))) for Federal office (as defined in section 301(3) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(3))); and
(14) the term "voting system" has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)).

Importante observação dos autores é acerca da exigência do dano, ou obtenção de dados para a punição dos cibercriminosos, conforme destacado anteriormente. Como exemplo, podemos juntar as alíneas, ou seções e subseções, e encontramos algo semelhante ao direito brasileiro: (a) Quem (2) acessa intencionalmente um computador sem autorização ou excede o acesso autorizado e, assim, obtém (C) informações de qualquer computador protegido será punido conforme previsto na subseção (c) desta seção.

Quanto à pena, nos termos já expostos, está condicionada a determinadas características, como a reincidência. A pena vem acompanhada pela indicação das seções e subseções: (c) A punição por uma infração nos termos da subseção (a) ou (b) desta seção é (1)(A) uma multa sob este título ou prisão por não mais de dez anos, ou ambos, no caso de um delito nos termos da subseção (a)(1) desta seção que não ocorra após uma condenação por outro delito nos termos desta secção, ou uma tentativa de cometer um crime punível nos termos desta alínea (ou subseção).

3.3 Legislação nacional sobre crimes cibernéticos

O Brasil está relativamente atrasado em comparação aos outros países signatários da Convenção de Budapeste, e apesar de ser um fato notório os avanços tecnológicos e a necessidade da criação de leis aptas a combater a nova criminalidade, verifica-se que os responsáveis estão longe de ter um conhecimento técnico apto para tanto (Jesus, Milagre, 2016, p. 71).

O próprio Código Penal brasileiro há bastante tempo contém tipificações de condutas que podem ser consideradas como crimes cibernéticos, porém, a parte cibernética é compreendida nesses artigos apenas como o meio para a prática de ilícitos comuns (Jesus, Milagre, 2016, p. 72).

Como o objetivo é analisar tão somente as condutas próprias, ou seja, as quais o bem jurídico tutelado são os dados privados que circulam em meio eletrônico, ou a própria segurança dos dispositivos que armazenam essas informações, serão listadas apenas estas.

Tal como realizado na análise das leis dos países anteriores, será utilizada a base de dados disponibilizada pela ONU. A partir dos resultados obtidos por meio da aplicação do filtro “tipo de crime: *cibercrime*”, e país “Brasil”, encontra-se, por ordem de resultado, o crime descrito no art. 154-A do Código Penal, que foi incluído por meio da Lei n.º 12.737/2012, além do art. 154-B, que complementa a descrição discorrendo acerca da Ação Penal:

> **Invasão de dispositivo informático**
> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, 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 1/3 (um terço) a 2/3 (dois terços) 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 2 (dois) a 5 (cinco) anos, e multa.
> § 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 (Brasil, 1948, art. 154-A).
>
> **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. (Brasil, 1948, art. 154-B).

Ao analisar o tipo, verifica-se que faz correspondência ao artigo 2º da Convenção de Budapeste, que trata do Acesso Ilegítimo, sendo que, é exigido o fim específico de obter, adulterar, ou destruir dados ou informações, sem autorização, expressa ou tácita, do usuário do dispositivo, ou ainda, como fim específico, instalar vulnerabilidade destinada a obter vantagem ilícita.

Denota-se que a inclusão do fim específico atende à sugestão declarada na Convenção de Budapeste, acerca da obtenção de dados, ou alguma outra intenção ilegítima. Na Convenção também há a sugestão para que seja incluída que a infracção seja cometida com a violação de medidas de segurança, porém, nesse caso, não há tal previsão, de modo que, a "invasão" do dispositivo pode ocorrer por mero abuso de confiança, por exemplo, quando o autor detém o acesso ao dispositivo de outra pessoa, bastando que tenha o fim de obter/adulterar/destruir os dados ou informações, ou que pretenda instalar uma vulnerabilidade.

A previsão de “violação indevida de mecanismo de segurança” estava presente na redação original, e foi substituída pela atual versão após a promulgação da Lei 14.155/2021.

A retirada dessa exigência acaba expandindo a aplicação da lei, conforme exemplificado, mediante o abuso de confiança. Apesar de ter sido retirada a exigência de violação do mecanismo de segurança, foi mantida a expressão “invadir”, o que acaba gerando, possivelmente, uma confusão, ou interpretação indevida, no momento da subsunção aos fatos que levarão à prisão do agente que comete a conduta. Além disso, na redação original era prevista a pena de detenção, de 3 (três) meses a 1 (um) ano, e multa, porém foi posteriormente alterada, igualmente pela Lei 14.155/2021, passando a vigorar a versão atual, e foi aumentada a pena das agravantes dos §§ 2º e 3º.

Assim como ocorre na legislação de Portugal e Estados Unidos, incorre na mesma pena o cúmplice que auxilia materialmente para a consumação da conduta principal, ao produzir, oferecer etc. um dispositivo ou programa de computador destinado a prática da conduta definida no caput, e também depende de representação, exceto nos casos em que o crime é cometido contra a administração pública.

Outrossim, se observa a inclusão de agravante para o casos em que ocorre proveito econômico, e uma outra pena base para situações em que acontece a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, ou informações sigilosas, sendo que, há ainda outro aumento da pena, em forma de agravante, se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, desses conteúdos, segredos, ou informações.

Outra conduta incluída no Código Penal a partir da Lei 12.737/2012 é aquela descrita pelo §1º do art. 266:

> **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 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 (Brasil, 1948, art. 266).

Nesse caso, a conduta se trata de crime próprio cibernético, eis que o bem jurídico tutelado é o sistema (serviço) telemático[6] ou de informação, e se aproxima ao crime descrito

[6] A palavra telemática é a mistura das palavras telecomunicações + informática, ou seja, pode ser interpretada como "telecomunicações computadorizadas". A parte "telecomunicações" significa que a telemática permite enviar, receber e recolher dados a partir de sensores e dispositivos (Telemática, 2022).

no artigo 5º da Convenção de Budapeste, que trata da "Interferência em sistemas" (tópico 4.3.4), porém, na Convenção a conduta é complementada pela expressão "através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.", ou seja, na legislação brasileira não é especificado de que maneira deve ocorrer a interrupção. Ademais, denota-se que não há punição para o agente que auxilia materialmente, mediante a disponibilização de dispositivo concebido para a prática do crime.

A Lei 12.737/2012 acrescentou, ainda, o crime de "Falsificação de cartão", mediante a inclusão da equiparação à documento particular, "o cartão de crédito ou débito", tratando-se de crime cibernético impróprio, tendo em vista que o bem jurídico tutelado é a fé pública.

Em continuidade, a partir da ordem de aparição na pesquisa junto ao banco de dados da ONU, se encontram os crimes tipificados no art. 313-A e 313-B, incluídos no Código Penal pela Lei nº 9.983, de 2000, que são assim descritos:

> **Inserção de dados falsos em sistema de informações**
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa (Brasil, 1948, art. 313-A).
>
> **Modificação ou alteração não autorizada de sistema de informações**
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado (Brasil, 1948, art. 313-B).

As condutas ora descritas são as primeiras em que o sujeito ativo se trata de pessoa específica, nesse caso, um funcionário público que detém o poder de inserir dados no sistema da administração, ou, que possui acesso aos meios para tanto, considerando a tipificação de "facilitar" a inserção de dados falsos.

Verifica-se que o tipo descrito no art. 313-A exige o fim específico "obter vantagem indevida para si ou para outrem ou para causar dano", e dessa forma, aproxima-se à conduta tipificada no art. 8º da Convenção de Budapeste, que trata da "Burla informática":

> **Artigo 8º - Burla informática**
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, **o acto intencional e ilegítimo, que origine a perda de bens a terceiros** através:
> a) Da **introdução, da alteração, da eliminação ou da supressão de dados informáticos**,

> b) De **qualquer intervenção no funcionamento de um sistema informático**, **com a intenção de obter um benefício económico ilegítimo para si ou para terceiros** (Conselho da Europa, 2001, art. 8º; grifo próprio).

Infere-se que as condutas se assemelham, em razão do fim específico também exigido na alínea "b" do artigo 8º: "com a intenção de obter um benefício económico ilegítimo para si ou para terceiros", sendo que é precedida de "**qualquer intervenção** no funcionamento de um sistema informático", o que leva a presumir que se encaixa a conduta descrita no art. 313-A de inserir/facilitar inserção de dados falsos, ou alterar/excluir indevidamente dados corretos.

Já o art. 313-B trata da modificação/alteração do sistema/programa sem autorização, porém não se exige um fim específico, como ocorre no artigo anterior. Essa conduta é semelhante ao crime descrito no artigo 5º da Convenção de Budapeste, que trata da "Interferência em sistemas". A diferença se observa a partir do verbo utilizado, enquanto na Convenção utiliza-se "obstrução grave" (obstruir), e mediante "introdução, transmissão, danificação, eliminação [...] de dados informáticos" , enquanto que, na legislação brasileira, se encontra apenas "modificar ou alterar [...] sistema de informações ou programa de informática [...]".

Assim, vê-se que a conduta descrita no artigo 5º da Convenção de Budapeste parece ser mais grave, além de estar especificado de que maneira ocorre, que é por meio do tratamento dos dados (introdução, transmissão etc.), ao passo que o crime previsto no art. 313-B do Código Penal não especifica de que maneira ocorre a modificação ou alteração do sistema. Por fim, igualmente ao art. 266 do Código Penal - anteriormente analisado -, não se verifica a punição ao agente que auxilia materialmente mediante a disponibilização de dispositivo concebido para a prática da conduta descrita, porém, não parece ser necessário, tendo em vista que pressupõe-se que o autor da conduta é funcionário público, que já possui o acesso pleno ao sistema.

Os crimes seguintes encontrados por meio da base de dados da ONU são crimes cibernéticos impróprios: os descritos na Lei 7.716/1989, que define os crimes resultantes de preconceito de raça ou de cor, sendo considerado como cibernético apenas o meio pelo qual são praticadas as condutas (por intermédio dos meios de comunicação social, de publicação em redes sociais, da rede mundial de computadores).

E os crimes tipificados no Estatuto da Criança e do Adolescente, que se referem à pornografia infantil, sendo que, nos mesmos termos dos crimes de preconceito de raça ou de cor, cibernético seria o meio de divulgação desse tipo de conteúdo (por meio de sistema de informática ou telemático), ou ao acesso (por rede de computadores), ao conteúdo.

O resultado posterior da busca por legislações de crimes cibernéticos junto ao banco de dados da ONU nos traz a conduta tipificada no art. 10 da Lei 9.296/1996.

Trata-se do crime de interceptação de comunicações sem autorização, sendo assim descrito:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei (Brasil, 1996, art. 10).

Em correspondência à Convenção de Budapeste, a conduta ora descrita apresenta semelhança ao seu artigo 3º, que trata de "Intercepção Ilegítima", especificamente a parte "interceptação [...] de informática ou telemática", "sem autorização judicial ou com objetivos não autorizados em lei". Se encaixam à previsão "intercepção intencional e ilegítima de dados informáticos [...]", "[...] para, de, ou dentro de um sistema informático, incluindo emissões eletromagnéticas provenientes de um sistema informático que veicule esses dados".

Também não há a punição do agente que fornece um dispositivo concebido para este fim, porém, nesse caso, demonstra-se interessante essa punição, pois a interceptação de comunicações informáticas e telemáticas exige procedimento específico, com invasão dos bancos de dados dos provedores.[7]

Na mesma linha de pesquisa junto à base de dados da ONU, o resultado seguinte se refere à Lei 14.478/2022, que altera o Código Penal, para incluir o crime "Fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros", tipificado junto ao crime de estelionato, sob o n.º 171-A, trata-se, portanto de crime cibernético impróprio, sendo que o elemento cibernético seria "ativos virtuais".

Essa lei também contém previsão de alteração do art. 1º da lei de lavagem de dinheiro (Lei 9.613/1998), para fazer incluir um novo parágrafo de aumento de pena, quando a lavagem de dinheiro ocorre por meio da utilização de ativo virtual, tratando-se novamente de crime cibernético impróprio (elemento "ativo virtual").

---

[7] **A interceptação telemática** é uma ação, com base na Lei n° 9.296/96, **realizada por um provedor de acesso**, **para capturar qualquer tráfego de telecomunicações e fluxo de comunicações em sistemas de informática e telemática** e encaminhá-los ao responsável pela investigação e/ou responsáveis pela interceptação. No resultado da interceptação, o provedor de acesso deve fornecer o conteúdo da comunicação; **remover ou entregar sem codificação ou criptografia**, cujo código-fonte ou chave criptográfica esteja de posse, ou seja, de sua propriedade, ou tenha sido aplicada por ela o conteúdo da comunicação ou a informação relacionada à interceptação (AdNormas, 2022 - grifo próprio).

4 CUMPLICIDADE NOS CRIMES CIBERNÉTICOS

No capítulo atual objetiva-se avaliar a legislação penal brasileira em face das diretrizes previstas na Convenção de Budapeste para criminalização da conduta do cúmplice que auxilia materialmente na prática dos crimes cibernéticos. Para dar suporte à avaliação, e delimitar o escopo da pesquisa, será abordada a diferenciação entre os crimes próprios e impróprios na Convenção de Budapeste, igualmente com auxílio da doutrina, para então serem debatidos em específico os crimes próprios da Convenção, tendo como base o seu próprio texto, com as considerações acerca da ocorrência da cumplicidade nesses delitos.

A necessidade de se penalizar a cumplicidade nos crimes cibernéticos decorre da própria Convenção de Budapeste, que dispõe em seu artigo 11 sobre "Tentativa e cumplicidade":

> Artigo 11º - Tentativa e cumplicidade
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a cumplicidade, quando cometida intencionalmente, na prática de qualquer uma das infracções estabelecidas de acordo com os artigos 2º a 10º da presente Convenção, com a intenção de que essa infracção seja cometida.
> [...] (Conselho da Europa, 2001, art. 11.º).

Além disso, a própria convenção dispõe uma conduta que trata sobre uma espécie de cumplicidade, presente no artigo 6º:

> Artigo 6º - Uso abusivo de dispositivos
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:
> a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:
> i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;
> ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e
> b) A posse de um elemento referido nos alínea a), i. ou ii., com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reuna um certo número desses elementos para que seja determinada a responsabilidade criminal.
> 2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em

> conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.
> 3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, a), ii (Conselho da Europa, 2001, art. 6.º).

Observa-se a descrição da conduta de um eventual cúmplice, que disponibiliza os meios necessários (um dispositivo, ou uma palavra passe) para a prática das condutas descritas nos artigos anteriores (2º a 5º).

4.1 Teoria de concurso de pessoas

O termo "concurso de pessoas" foi adotado em nosso ordenamento jurídico como a condição na qual duas, ou mais pessoas, se reúnem para a prática de um crime. O concurso de pessoas pode ser tratado, ainda, como "concurso de agentes", ou "codelinquência". Grande parte dos crimes tipificados são passíveis de serem cometidos por uma, ou mais pessoas, porém, alguns tipos penais, somente podem ser perpetrados por mais de um agente, como é o caso do delito de "associação criminosa", que, pelo nome, facilmente denota-se o motivo (Gonçalves, 2020, p. 166).

Em razão dessas particularidades, podemos classificar os crimes como "unissubjetivos", ou "plurissubjetivos". O nome sugere: os unissubjetivos, ou de concurso *eventual*, são aqueles que podem ser praticados por uma única pessoa, tais como o homicídio e o furto, e consequentemente, os plurissubjetivos são aqueles que devem ser cometidos por duas pessoas ou mais, e também podem ser tratados como crimes de concurso *necessário*, como a "rixa" (Gonçalves, 2020, p. 166).

O concurso de pessoas foi desenvolvido em três teorias: monista, ou unitária; dualista; pluralista. A primeira delas estabelece que todos os envolvidos na conduta serão penalizados por um único crime, enquanto na teoria dualista, se estabelece que haverá dois crimes, sendo um para o autor principal, e um outro para os cúmplices. Já a teoria pluralista, estabelece que, cada agente participante do ato ilícito deverá ser penalizado individualmente, devendo responder por seu próprio crime (Gonçalves, 2020, p. 166).

O Código Penal brasileiro adota a teoria unitária, ou monista, conforme se observa a partir do artigo 29 deste diploma legal[8]. Isso significa, por exemplo, que duas pessoas que praticam um furto, serão penalizadas pelo crime de furto. Existem algumas exceções, e são

[8] Art. 29 - Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade (Brasil, 1940).

observadas no próprio artigo 29, eis que, no seu §2º, encontra-se a tipificação da "cooperação dolosamente distinta", na qual um dos agentes pretende a participação em um crime menos grave, porém o resultado difere daquilo que pretendeu. Cita-se como exemplo, a situação na qual duas pessoas juntam-se a fim de lesionar um terceiro, entretanto, uma delas acaba matando a vítima. Nesse caso, a pessoa que tinha a intenção apenas de machucar, responde pelo crime menos gravoso, que seria a lesão corporal. Essa regra somente é aplicável quando o resultado mais gravoso não era previsível, caso contrário, sendo previsível o resultado mais danoso, a pena do agente que pretendeu o crime menos grave será aumentada em até metade (Gonçalves, 2020, p. 175).

Há ainda outras exceções que podem ser encontradas na parte especial do Código, como é o caso da gestante que consente com a prática do aborto, incidindo no crime previsto no art. 124, enquanto a pessoa que praticou o aborto responderá pelo crime tipificado no art. 126, considerado mais grave (Gonçalves, 2020, p. 175).

Pode-se dizer que existem quatro requisitos para o concurso de agentes: pluralidade de condutas, ou seja, mais de uma ação praticada por duas pessoas ou mais; relevância causal das condutas, que seria a nítida influência de uma determinada ação praticada pelo agente para a consumação do resultado; liame subjetivo, que significa uma identidade de desígnios, ou, uma vontade dos participantes para que o crime seja consumado, não sendo necessário, entretanto, que haja uma prévia combinação entre os agentes, apesar de ser a situação mais comum nesses casos; por fim, é necessária a identidade do crime para todos os indivíduos, isto é, todos os participantes da conduta criminosa respondem pelo mesmo crime, ainda que um deles tenha participado de apenas parte, como por exemplo, num crime de furto, no qual uma das pessoas consegue fugir logo após a prática da conduta, com objetos furtados, enquanto outra acaba sendo presa no local, sem nada levar. Importante salientar que nas exceções antes descritas *não há* o concurso de agentes, respondendo cada pessoa por crime diverso (Gonçalves, 2020, p. 178).

4.2 Diferenciação entre crimes próprios e impróprios na convenção

Como o objetivo do trabalho é investigar a penalização do cúmplice nos crimes cibernéticos próprios, são necessárias algumas considerações acerca dessa classificação. A partir da leitura do Manual de Crimes Informáticos, por Damásio de Jesus e José Antonio Milagre, podemos encontrar a definição de crimes informáticos (cibernéticos) próprios, impróprios, mistos, e mediato ou indireto:

> a) crimes informáticos próprios: em que o **bem jurídico ofendido é a tecnologia da informação em si**. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
> b) crimes informáticos impróprios: em que **a tecnologia da informação é o meio utilizado** para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;
> c) crimes informáticos mistos: são crimes complexos em que, **além da proteção do bem jurídico informático** (inviolabilidade dos dados), **a legislação protege outro bem jurídico**. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;
> d) crime informático mediato ou indireto: trata-se do **delito informático praticado para a ocorrência de um delito não informático** consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, **no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima**. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto) (Jesus, Milagre, 2016 p. 53-54 - grifo próprio).

A distinção é simples, mas necessária, a fim de delimitar os tipos que serão abordados a partir da Convenção de Budapeste, para posterior averiguação da ocorrência do auxílio material pelo cúmplice em cada conduta tipificada.

Os crimes antes analisados dos diferentes países são, em sua maioria, crimes próprios, sendo que encontrava-se, igualmente, na maior parte dos delitos, a tipificação da punição ao cúmplice.

4.3 Crimes próprios previstos na convenção de budapeste

Realizada a diferenciação entre os tipos de crimes cibernéticos, passa-se a abordar cada um em específico, a fim de investigar de que maneira ocorre a penalização do cúmplice a partir de cada conduta.

A Convenção de Budapeste, ou, Convenção Sobre o *Cibercrime*, traz em seus artigos uma variedade de definições, desde os termos utilizados durante toda a elaboração dos seus artigos, como “Sistema informático” e “Dados informáticos”, até a tipificação de crimes próprios e impróprios. Além disso, a Convenção dispõe sobre aspectos processuais e de cooperação internacional.

4.3.1 Acesso ilegítimo

Está assim tipificado o crime de “acesso ilegítimo” na Convenção de Budapeste:

> Artigo 2º - Acesso ilegítimo
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático (Conselho da Europa, 2001, art. 2.º).

Observa-se que o núcleo da conduta reside em "acesso intencional e ilegítimo", que pode ser lido como, o agente que, dolosamente, e sem a permissão, acessa "à totalidade ou a parte de um sistema informático", isto é, a conduta se consuma ainda que o autor acesse apenas parte de um sistema informático, compreendido, por exemplo, como uma pasta de um computador, que esteja ou não protegida - levando-se em conta que a conduta pode ser praticada com, ou sem, a "violação de medidas de segurança" -, bastando que o acesso não tenha sido permitido.

A definição de sistema informático pode ser encontrada no artigo 1º da Convenção:

> Artigo 1º - Definições
> Para os fins da presente Convenção:
> a) "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados; (Conselho da Europa, 2001, art. 1.º).

Os dados informáticos, presentes na conduta de "Acesso ilegítimo" como um fim específico de obtê-los, também são definidos na Convenção:

> b) "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função; (Conselho da Europa, 2001, art. 1.º).

Para os fins da pesquisa: a conduta ora descrita, analisada em conjunto com o disposto no artigo 6º da Convenção - antes descrito -, indica que, seria consumada a cumplicidade mediante a disponibilização de uma senha, ou palavra passe, no caso de o dispositivo informático a ser acessado esteja protegido, sendo necessária a violação de medidas de segurança. A depender do dispositivo a ser acessado - diferente de uma pasta de computador, no exemplo citado -, a disponibilização de uma palavra passe pode ser insuficiente, sendo necessária a fabricação de um outro dispositivo, concebido para mediar esse acesso ilegítimo.

4.3.2 Intercepção ilegítima

O crime de “Intercepção ilegítima” está disposto no artigo seguinte da Convenção (3º):

> Artigo 3º - Intercepção ilegítima
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático (Conselho da Europa, 2001, art. 3.º).

Denota-se um padrão na estruturação dos artigos, a partir da presença do termo “Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, [...]” que se segue com a descrição da conduta específica a ser penalizada.

No caso atual, criminaliza-se “a intercepção intencional e ilegítima”, novamente, dolosamente, e sem autorização, “de dados informáticos” (já descritos), “efectuada por meios técnicos”, mediante a utilização, aparentemente, de um dispositivo concebido para tanto, “em transmissões não públicas”, ou melhor, de particulares, “para, de ou dentro de um sistema informático”, abarcando qualquer possibilidade de transmissão de dados.

Nesse tipo, parece mais claro que a conduta do cúmplice será penalizada mediante a disponibilização do dispositivo concebido para a intercepção, dito de outra forma, interceptação, da transmissão dos dados.

4.3.3 Interferência em dados

Em sequência, encontra-se o crime tipificado no artigo 4º:

> Artigo 4º - Interferência em dados
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.
> 2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves (Conselho da Europa, 2001, art. 4.º).

Mais uma vez se repete a descrição inicial da conduta: o agente que, dolosamente, e sem permissão; para então ser descrita: “danificar, apagar, deteriorar, alterar ou eliminar”, nesse caso, “dados informáticos”, de maneira abrangente.

A partir da análise da conduta descrita, infere-se que o núcleo “danificar” poderia atribuir a característica de crime impróprio ao crime descrito, eis que se encaixaria no crime de “dano” do Código Penal, anteriormente tratado. No entanto, ao serem incluídas as condutas de “apagar” e principalmente “alterar”, se pode classificar mesmo como crime próprio, tendo em vista que não fariam sentido no contexto do crime de dano.

A conduta do cúmplice, nesse caso, seria consumada na medida em que disponibilizaria a palavra passe necessária para que sejam acessados esses dados, no caso, obviamente, de estarem protegidos por alguma medida de segurança. Também se consuma, a conduta do cúmplice, quando eventualmente forneça algum dispositivo que, quando conectado ao sistema que armazena esses dados, acaba ocasionando alguma das condutas específicas (danificar, apagar etc.).

4.3.4 Interferência em sistemas

> Artigo 5º - Interferência em sistemas
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos (Conselho da Europa, 2001, art. 5.º).

O crime de interferência em sistemas é o primeiro da lista que aparece de uma maneira um pouco distinta, com início a partir da “obstrução”, seguida outra vezes pelo significante, sem autorização, e de forma dolosa, “ao funcionamento de um sistema informático”; poderia ser entendido como uma interrupção, ou dificultação do funcionamento desse sistema, mediante a “introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos”.

Denota-se uma junção entre o crime de “interferência em dados” com o de “acesso ilegítimo”, sendo incluída a conduta de “introdução” e “transmissão”. Isto é, uma vez que são tratados os dados (sofrem interferência), para acessar um sistema (daí, o acesso ilegítimo), com o fim específico de obstruir, ou seja, impedir ou atrasar, dificultar, o funcionamento do sistema (e tal fim específico também se encontra previsto no acesso ilegítimo, na parte final: “com a intenção de obter dados informáticos *ou outra intenção ilegítima*”).

Nesse caso, a conduta do cúmplice será a mesma observada nesses crimes que sofrem essa aparente junção, ou seja, mediante uma palavra passe para acessar esse sistema, ou um dispositivo próprio que ele mesmo ocasiona a obstrução, de maneira independente.

4.3.5 Uso abusivo de dispositivos

O tipo a seguir já foi trazido anteriormente, como hipótese para definir de que forma se daria a conduta do cúmplice nos crimes cibernéticos:

> Artigo 6º - Uso abusivo de dispositivos
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:
> a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:
> i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;
> ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e
> b) A posse de um elemento referido nos alínea a), i. ou ii., com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reuna um certo número desses elementos para que seja determinada a responsabilidade criminal.
> 2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.
> 3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, a), ii (Conselho da Europa, 2001, art. 6º).

A partir da leitura em conjunto ao artigo 11 da Convenção, que trata da necessidade de penalizar a cumplicidade, com as particularidade de cada país signatário, denota-se que o conteúdo revela essa punição ao cúmplice, eis que descreve justamente aquilo que foi observado na tipificação da legislação dos países estudados, ou seja, a punição ao agente que disponibiliza (de variadas formas) um dispositivo concebido para a prática das condutas que são descritas, nesse caso, especificamente aquelas dos artigos 2º a 5º.

Diferente do que se encontra nas legislações analisadas, vê-se a tipificação, como conduta a ser penalizada, da *posse* desses dispositivos, ou palavras-passe, código, dados. São exceptuadas, com sabedoria, os usos eventuais desses dispositivos para outros fins, além da prática dos crimes previstos.

Essa exceção manifesta a expressão de agentes conhecidos na temática cibernética como “Hackers”, sendo “pesquisadores de segurança da informação” (Damásio, Jesus, 2016 p. 16) , em comparação aos “Crackers”, que “exploram as intimidades dos sistemas e também

dos processos desenvolvidos sobre a tecnologia da informação para a prática de delitos" (Damásio, Jesus, 2016, p. 16). De outro modo, caso não houvesse a exceção, impossibilitaria o desenvolvimento de métodos para a proteção dos sistemas.

Por fim, encontra-se a descrição do n.º "3", reservando aos países a possibilidade de não penalizar os agentes que produzem, ou obtêm, uma palavra-passe, código de acesso etc. concebido para ser utilizado em cometimento das condutas criminosas. Essa exceção aparenta ser um complemento à anterior, possibilitando aos hackers essa investigação/pesquisa. Por óbvio, os países não poderiam optar por permitir qualquer forma de disponibilização dessas ferramentas, de modo que os Hackers devem obtê-las por seus próprios meios.

5 CONCLUSÃO

Por meio do estudo presente foi possível perceber que a Sociedade de Risco, atual estágio no qual nos encontramos, ou que estamos transicionando para, nos termos de Ulrich Beck, traz consigo variados riscos que aumentam na medida em que são desenvolvidas novas técnicas, e dentre eles, são destacados os crimes cibernéticos.

Esses novos tipos delitivos apresentam relação com a Sociedade de Risco pois os efeitos dos riscos em geral, são observados também nos crimes cibernéticos, sendo estes um novo tipo de risco em si mesmos: a distribuição dos crimes é desigual e abrangente por toda a sociedade, e se observa imprevisão quanto aos possíveis efeitos que acontecem pelo avanço desenfreado das técnicas, que acabam gerando novas práticas que precisam ser tipificadas nos ordenamentos jurídicos.

A partir da pesquisa sobre os crimes cibernéticos, observou-se que o bem jurídico tutelado nessas condutas pode ser considerado abrangente, sendo considerada, em última análise, a informação - ou dados, porém, os sistemas informáticos, e a sua incolumidade, bem como, os dispositivos informáticos, e a privacidade dos indivíduos em alguns tipos penais.

Nesse sentido, foi observado que a Constituição Federal de 1988 também apresenta importantes contribuições à definição de bem jurídico penal, com a presença de limitações aos legisladores pátrios, e princípios que devem ser observados na elaboração das leis.

Com a delimitação sobre os crimes cibernéticos e os bens jurídicos que são protegidos pelas condutas típicas, foi realizada a pesquisa das legislações que foram editadas em diferentes países do mundo, com auxílio da base de dados disponibilizada pela Organização das Nações Unidas (ONU), com o objetivo de investigar de que modo o cúmplice que auxilia materialmente à consumação dos crimes cibernéticos é penalizado nesses países.

Primeiramente, foi relacionada a legislação de Portugal, por apresentar semelhanças ao ordenamento pátrio, para então serem descritas as leis promulgadas nos Estados Unidos da América, tendo em vista que o país é conhecido por apresentar um forte combate aos cibercriminosos, e tal circunstância foi verificada.

Para apresentar uma comparação efetiva, buscou-se trazer para a discussão a legislação brasileira produzida no âmbito dos crimes cibernéticos, consideradas pela ONU, sendo colacionados os crimes próprios previstos na legislação, com a investigação em específico sobre os cúmplices, tal como realizado nas legislações dos países anteriores.

A esse respeito, por meio da pesquisa doutrinária, foram trazidos os conceitos pertinentes ao concurso de pessoas, além da delimitação de crimes cibernéticos próprios e impróprios, considerando que o foco da pesquisa é com relação aos primeiros.

Na pesquisa sobre o concurso de pessoas foi observado que o Brasil adota, de maneira geral, a teoria unitária, apesar de constar pelo ordenamento algumas exceções à essa adoção.

Após realizadas as considerações sobre as legislações produzidas pelo mundo, e no Brasil, buscou-se trazer as disposições da Convenção de Budapeste, no que concerne à parte destacada pelo seu artigo 6º, "Uso abusivo de dispositivos", em conjunto com o artigo 11º, que trata sobre a necessidade de se penalizar a cumplicidade nos crimes cibernéticos, com relação aos crimes definidos nos artigos 2º a 5º, que tratam de condutas próprias.

Como resultado, foi observado que a Convenção de Budapeste adota a teoria dualista, ou pluralista, ao prever o artigo 6º, que descreve a conduta do cúmplice que auxilia materialmente o autor do crime cibernético, ao disponibilizar, um dispositivo, ou palavra-passe concebido para praticar as condutas descritas. Ou seja, diferentemente do que se observa nas legislações pesquisadas, a Convenção de Budapeste apresenta uma conduta única para o cúmplice, devendo ele ser punido nos moldes descritos no artigo 6º da Convenção.

Em contrapartida, nos países em que se observou a edição de leis que punem os cibercriminosos, a conduta do cúmplice é punida como acessória ao cometimento da conduta principal, com disposições no seguinte sentido: "nas mesmas penas incorre o agente que auxilia materialmente", sendo aplicável, portanto, o mesmo crime, diferente do que ocorre na Convenção. Também se observou que nem mesmo há punição ao cúmplice em determinadas situações, como é o caso do Brasil, ao prever o art. 266 do Código Penal, que trata da "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", sendo que não se encontram condutas acessórias.

Sendo assim, observou-se que a criminalização da conduta do cúmplice que auxilia materialmente na prática dos crimes cibernéticos ocorre de maneira bastante semelhante nos países analisados, com a descrição de condutas anexas aos artigos principais, adotando-se a teoria unitária, em comparação à Convenção de Budapeste, que prevê um tipo específico para criminalizar o cúmplice, adotando-se a teoria dualista, ou pluralista. Além disso, na Convenção de Budapeste se encontra prevista a conduta de *possuir* um dispositivo, palavra passe, ou outros dados informáticos concebidos para o fim específico de praticar as condutas descritas nos artigos 2º a 5º da Convenção, porém, nos países analisados, não se observa tal previsão.

REFERÊNCIAS

BECK, Ulrich, 1944 - **Sociedade de risco: rumo a uma outra modernidade**/ Ulrich Beck; tradução de Sebastião Nascimento; inclui uma entrevista inédita com o autor - São Paulo: Editora 34, 2011 (2ª edição).

BRASIL. [Código Penal (1940)]. **CÓDIGO PENAL**. Rio de Janeiro, 31 de Dezembro de 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 13 set. 2023.

BRASIL. [LEI Nº 9.296 (1996)]. **LEI Nº 9.296, DE 24 DE JULHO DE 1996**. Brasília, 24 de julho de 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 15 nov. 2023.

CONSELHO DA EUROPA. [Convenção sobre o cibercrime (2001)]. **CONVENÇÃO SOBRE O CIBERCRIME**. Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em 13 set. 2023.

DANTAS, Tiago. "**Pirataria**"; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/curiosidades/pirataria.htm. Acesso em 12 nov. de 2023.

Editoria Segurança Pública. Polícia Civil alerta a população sobre as modalidades do golpe do pix. **Agência Estadual de Notícias**. Paraná. 30 ago. 2023. Disponível em: https://www.aen.pr.gov.br/Noticia/Policia-Civil-alerta-populacao-sobre-modalidades-do-golpe-do-pix. Acesso em: 15 nov. 2023

ESTADOS UNIDOS DA AMÉRICA. [Title 18-CRIMES AND CRIMINAL PROCEDURE. PART I-CRIMES. CHAPTER 47-FRAUD AND FALSE STATEMENTS (1986)]. **Fraud and related activity in connection with computers**. From. Disponível em: https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim). Acesso em: 15 nov. 2023.

GONÇALVES, Victor Eduardo Rios. **Curso de Direito Penal**: Parte Geral: arts. 1º a 120. 4. ed. São Paulo: Saraiva Educação, 2020. p. 166-167; 175-178.

TELEMÁTICA: O que é e para que serve?. **Engenharia híbrida**. 9 set. 2022. Disponível em: https://www.engenhariahibrida.com.br/post/telematica-o-que-e-para-que-serve. Acesso em: 15 nov. 2023.

FULLER, Greice Patricia; TATEOKI, Victor Augusto. Os dados pessoais como bem jurídico a ser penalmente tutelado na sociedade da informação. **Revista Em Tempo**, [S.l.], v. 22, n. 1, p. 110 - 124, fev. 2023. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3264. Acesso em: 10 set. 2023.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. 1.ª Edição. São Paulo: Saraiva, 2016.

PORTUGAL. [Código Penal (1995)]. **Código Penal - CP. Decreto-Lei n.º 48/95**. Em vigor Diário da República n.º 63/1995, Série I-A de 1995-03-15. Versão à data de 4-9-2023. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675-106555901. Acesso em: 12 nov. 2023.

PORTUGAL. [Lei do Cibercrime (2009)].**Lei do Cibercrime. Lei n.º 109/2009**. Em vigor. Diário da República n.º 179/2009, Série I de 2009-09-15. Versão à data de 24-11-2021. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2009-128879174. Acesso em: 12 nov. 2023.

PORTUGAL. [Código da Propriedade Industrial - CPI (2018)]. **Código da Propriedade Industrial - CPI. Decreto-Lei n.º 110/2018**. Em vigor. Diário da República n.º 237/2018, Série I de 2018-12-10. Versão à data de 29-1-2021. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/2018-117279941. Acesso em: 12 nov. 2023.

AS ORIENTAÇÕES normativas para a interceptação telemática de ordem judicial. **Revista AdNormas**. 13 dez 2022. Disponível em: https://www.revistaadnormas.com.br/2022/12/13/as-orientacoes-normativas-para-a-interceptacao-telematica-de-ordem-judicial. Acesso em: 15 nov. 2023.

SMANIO, Gianpaolo Poggio. O bem jurídico e a Constituição Federal. **Sedep**. Campo Grande. In: Doutrina Adcoas, v. 7, n. 21, p. 423-426, 1. quinz. nov. 2004. Disponível em: https://www.sedep.com.br/artigos/o-bem-juridico-e-a-constituicao-federal/. Acesso em nov. 2023.

TEIXEIRA, Pedro S. Bairros ricos concentram crimes digitais na capital paulista, mostram dados inéditos. Secretaria estadual não divulga dados sobre golpes na internet; boletins de ocorrência foram obtidos via LAI. **Folha de S. Paulo**. São Paulo. 26. out. 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/10/bairros-ricos-concentram-crimes-digitais-na-capital-paulista-mostram-dados-ineditos.shtml. Acesso em: 15 nov. 2023.