Universidade do Minho
Escola de Direito

Adele Gomes Gottschefsky

Segurança Cibernética no Setor Bancário: Análise da Regulamentação e Práticas de Proteção Contra o Cibercrime

Novembro de 2023

Segurança Cibernética no Setor Bancário: Análise da Regulamentação e Práticas de Proteção Contra o Cibercrime
Adele Gomes Gottschefsky
UMinho | 2023



Universidade do Minho
Escola de Direito

Adele Gomes Gottschefsky

Segurança Cibernética no Setor Bancário: Análise da Regulamentação e Práticas de Proteção Contra o Cibercrime

Dissertação de Mestrado

Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do

Prof. Doutor Pedro Jacob Morais e

do Prof. Doutor Vítor Fonte

Novembro de 2023

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.



Atribuição - Não Comercial - Com partilha Igual
CC BY-NC-SA

https://creativecommons.org/licenses/by-nc-sa/4.0/

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Segurança Cibernética No Setor Bancário: Análise da Regulamentação e Práticas de Proteção Contra o Cibercrime

Resumo

O presente trabalho tem como tema a segurança cibernética em relação ao setor bancário. As entidades bancárias é uma das áreas sensíveis da sociedade relativamente às ameaças cibernéticas. O crescente desenvolvimento da tecnologia fez com que os indivíduos cada vez mais migrassem as suas atividades para o mundo virtual, com o aumento dos utilizadores ocorre o aumento das ameaças. É de extrema relevância compreender o funcionamento desse novo sistema dentro da sociedade, descobrir as vulnerabilidades e os agentes envolvidos. Não são poucas as regulamentações e normas voltadas ao setor bancário para minimizar os efeitos do cibercrime, assim como é importante ter conhecimento da Lei do Cibercrime, criada em Portugal a partir da Convenção de Budapeste, que ocorreu em 23 de Novembro de 2001, e que pune esses atos criminosos. A preocupação da União Europeia sobre o tema não é recente, e diversos organismos foram criados para o combate do cibercrime. Nesse estudo são analisados os ataques que mais afetam os bancos, quem são os agentes do crime, o que a Lei do Cibercrime apresenta de mais importante para esse tema e as medidas tomadas pela União Europeia e por Portugal para minimizar os riscos e combater os ataques.

Palavras-chave: Cibercrime; segurança cibernética; setor bancário; vulnerabilidades.

Cybersecurity in the Banking Sector: Analysis of Regulations and Protection Practices Against Cybercrime

Abstract

This work focuses on cybersecurity in relation to the banking sector. Banking entities are one of the most sensitive sectors of society when faced with cyber threats. The increasing development of technology has caused individuals to increasingly migrate their activities to the virtual world, with the increase in users, an increase in threats. It is extremely important to understand the functioning of this new system within society, discovering the vulnerabilities and the agents involved. There are many regulations and standards external to the sector to minimize the effects of cybercrime, just as it is important to have knowledge of the Cybercrime Law, created in Portugal based on the Budapest Convention, which occurred on November 23, 2001, and which punishes these criminal acts. The European Union's concern on the topic is not new, and several bodies have been created to combat cybercrime. This study analyzes the attacks that most affect banks, who the criminal agents are, what the Cybercrime Law presents as most important for this topic and the measures taken by the European Union and Portugal to minimize risks and combat the attacks.

Palavras-chave: Cybercrime; cyberSecurity; banks sector; vulnerabilities.

Índice Geral

1. Fundamentação teórica

1.1. Conceito de Segurança da Informação.....3

1.2. Diferença entre Segurança Cibernética e Segurança da informação.....6

1.3. Segurança Cibernética no Setor Bancário.....8

1.4. Cibercrime, seus autores e o sistema informático.....14

1.5. Ciberataques.....22

2. Crimes relacionados ao Setor Bancário, análise da regulamentação, e seus efeitos jurídicos

2.1. Crimes cibernéticos que afetam os Bancos e a Lei do Cibercrime.....30

2.2. Políticas de Segurança Cibernética no Setor Bancário.....42

2.3. Regulamentação de Segurança Cibernética aplicada ao Setor Bancário Europeu.....43

3. Aspetos Informáticos na Segurança Cibernética

3.1. Práticas de Segurança adotadas pelas Instituições Bancárias.....56

3.2. Desafios Futuros na Segurança Cibernética no Setor Bancário.....60

4. Conclusões.....66

Bibliografia.....69

Outros Documentos.....79

Introdução

Atualmente a sociedade se encontra cada vez mais vinculada ao uso de dispositivos tecnológicos. Desde os objetos que estão dentro das casas das pessoas (frigoríficos, televisões, máquinas de café), como, por exemplo, nos hospitais, transportes públicos, ginásios e automóveis.

Há alguns anos para uma conta de luz ser paga era necessário se deslocar a um estabelecimento para efetuar o seu pagamento. Hoje toda essa realidade está transformada, e com um simples "clique" a conta é paga através da aplicação do banco.

Entretanto, todo esse rápido desenvolvimento da tecnologia traz consigo a mudança das formas de criminalidade, que passam também a ocorrer no ciberespaço, e que crescem e se desenvolvem com a mesma rapidez que os meios tecnológicos.

O presente estudo irá tratar das formas como esses crimes ocorrem, quais os ciberataques mais utilizados, quem os comete, e como os entes públicos trabalham para minimizar os seus efeitos e punir os criminosos. Ainda, irá se aprofundar no modo que isso ocorre especificamente nas entidades bancárias, que, como será demonstrado nesse trabalho, é um dos setores mais atingidos pelo cibercrime.

Alguns conceitos importantes serão tratados ao longo desta dissertação, como o da segurança da informação e suas diferenças com a cibersegurança, que apesar de serem subtis, são de grande importância para a compreensão teórica do estudo do ciberespaço. Na segurança da informação são tratadas de forma abrangente todas as formas em que é possível proteger a informação, seja com um muro em torno de uma em presa, com mecanismos anti-incêndio, seja com um bom *software* antivírus, por exemplo. Já a cibersegurança vai proteger especificamente o ciberespaço, ou seja, vai se preocupar com o mundo virtual.

Ao ultrapassar tal conceituação, o estudo demonstrará como se dá a segurança cibernética no contexto bancário, que foi o setor pioneiro na preocupação com o tema, uma vez que é o setor mais visado pelos cibercriminosos e que sofre grandes cobranças para estar protegido, especialmente do Banco de Portugal, através de diretrizes e regulamentos feitos por ele para que as instituições financeiras estejam preparadas para lidar com ameaças cibernéticas. O Banco de Portugal exige que os bancos desenvolvam e implementem políticas eficazes no que diz respeito à cibersegurança. Ademais, dissertará sobre que m são esses agentes e suas classificações.

Por outro lado, para se falar de segurança, é importante entender os concretos ataques

que ocorrem e de que forma eles são realizados, o que será debatido por esse trabalho, que também mencionará dois importantes ciberataques que ocasionaram mudanças em relação a cibersegurança, que são o *WannaCry* e o *NotPetya*. Esses ataques ocorridos em 2017 direcionaram de forma mais crítica a atenção da União Europeia ao enfrentamento dos crimes cibernéticos, visto que demonstraram o quão despreparados os entes públicos e privados estavam para essa realidade.

Na tentativa de melhorar as condições da cibersegurança, diversas medidas foram tomadas pelos entes de controlo estatal da União Europeia e seus Estados-Membros, que aqui se tem como enfoque Portugal. Um marco importante foi a Convenção de Budapeste, que, como será analisado neste estudo, acabou por dar surgimento à Lei do Cibercrime, que é um importante instrumento jurídico no combate ao crime cibernético, os artigos da lei mais importantes para a banca (4º, 5º, 6º e 7º) são tratados neste trabalho, e apesar de serem uma evolução para o tema, nem sempre se fazem satisfatórios no combate à criminalidade virtual.

Por fim, se especifica a regulamentação direcionada ao setor da banca no que se trata de segurança cibernética, no qual se elucida as diversas iniciativas regulatórias criadas pelo Banco Central Europeu e as orientações dadas pela Autoridade Bancária Europeia. Desta forma é possível observar o desenvolvimento das diretrizes relacionadas com o tema e sua melhoria após a já mencionada Convenção de Budapeste.

Ademais, se pode perceber os inúmeros esforços das entidades bancárias para proteção do ciberespaço, com a adoção de práticas de segurança esplanadas por este estudo, e todos os desafios que esse setor ainda irá enfrentar para que possa manter a confiança dos seus clientes.

1. Fundamentação Teórica

1.1. Conceito de Segurança da Informação

A segurança da informação é uma ciência que teve seu início há séculos atrás, sua história remonta aos Egípcios, Gregos e Romanos que faziam uso de técnicas de criptografia. Ainda não era denominada da forma que é hoje, porém já era muito utilizada. Conforme o autor Simon Singh[1] foi "a arte do segredo escrito que salvou a Grécia de ser conquistada por Xerxes, rei dos reis, o líder despótico dos persas". Também relata o uso de criptografia por Caio Júlio César, imperador romano, ao se comunicar com seu aliado Cícero: "César descreve como ele enviou uma mensagem a Cícero, que estava sitiado e a beira de se render. Substituiu as letras romanas por letras gregas, tornando a mensagem ininteligível para o inimigo.".

Com o desenvolvimento da sociedade, o uso de técnicas para a segurança da informação continuou permeando momentos históricos importantes, e os métodos foram cada vez mais se aperfeiçoando. Na batalha de *Midway*, que ocorreu durante a Segunda Guerra Mundial entre Estados Unidos da América e o Japão, o serviço de inteligência norte-americano, através do uso da criptografia, desvendou os códigos secretos dos japoneses, o que os levou a saber da estratégia de invasão deles antecipadamente e, assim, os contra-atacou[2]. Ao estudar e interceptar as mensagens no Pacífico, o serviço secreto descobriu o ataque ao atol de *Midway* antes dele ser efetivado[3].

Foi na Segunda Guerra Mundial que a importância da informação e da criptografia se consolidou definitivamente. Nessa época que surgiram as primeiras máquinas de decodificação dado o imenso volume de troca de mensagens. O exército alemão possuía a famosa máquina denominada Enigma [4], que criptografava e descriptografava mensagens, deixando-as praticamente impossíveis de decifrar. Todavia, o matemático Alan Turing cria uma máquina, a Enigma Bombe, capaz de descriptografar as mensagens criadas pela Enigma, e com essa vantagem estratégica, a Alemanha é derrotada.

A informação é um bem precioso, desde os primórdios da sociedade e particularmente após a Segunda Guerra Mundial com a ampla disseminação do uso mundial das redes de

[1] Singh, S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. 1999. "Tradução nossa".
[2] Kahn, D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. 1996.
[3] Hobsbawm, E. J. Era dos extremos: o breve século XX: 1914 - 1991. 2. ed. São Paulo: Companhia das Letras
[4] Enigma foi uma máquina produtora de códigos combinatórios, equipada com rotores eletromecânicos criptográficos. Utilizada tanto para criptografar como para descriptografar códigos de guerra, foi utilizada de diversas maneiras na Europa a partir dos anos 1920. (FERNANDES, Cláudio. "Máquina Enigma"; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/historiag/maquina-enigma.htm. Acesso em 15 de julho de 2023.

computadores. Pode ser conceituada como um conjunto de dados que possuem um significado, e que reduz a incerteza ou que aumenta o conhecimento a respeito de algo[5]. Dalton Luiz Lemos ainda resume a informação como "todo o conjunto de dados devidamente ordenados e organizados de forma a terem significado.".

Para melhor compreensão, os dados são um emaranhado de códigos, decifrados ou não, que com a decodificação passam a ser informação, ou seja, eles são uma base ou fonte de absorção de informações. Antes dos dados serem processados, não são percetíveis aos seres humanos. Dessa forma, compreende-se que a informação é a decodificação dos dados e reconhecimento e elucidação deles, transformando-se em uma mensagem entre indivíduos ou máquinas em um processo comunicativo ou transacional[6].

Conforme Sêmola[7], a informação constitui por si só um ativo, dado o seu valor para a sociedade atual. Não só, ainda elucida que "informação é poder e quanto mais íntegra ela for mais robusta será o seu processo de tomada de decisão e, consequentemente, maiores serão suas chances de sucesso. Tem sido assim há séculos e não há qualquer indício de mudança.". Visualizando a informação como poder, pode-se perceber o porquê da necessidade de protegê-la desde os primórdios. Eis que surge a denominação segurança da informação, que nada mais é do que assegurar a confidencialidade, integridade e disponibilidade da informação. Mas não só, como também garantir o não repúdio e gerenciar os riscos.

Vive-se hoje a sociedade da informação, na qual os seres humanos (sociedade) fazem uso da informação. Uma geração informática e comunicacional, que vivencia avanços tecnológicos velozes e que recebe e dá informação constantemente. Informação essa que, quando entregue, pode causar grandes impactos à população e ao mundo (Com o exemplos mais impactantes tem-se o Brexit e a eleição do Donald Trump[8]). Com quantidades imensas de dados da sociedade cada vez mais disponíveis (apesar dos esforços para Proteção de Dados[9]) e informações cada vez mais acessíveis (sejam verdadeiras ou não) assegurar a informação é tarefa essencial.

---

[5] Lemos II, Dalton Luiz. Tecnologia da informação / Dalton Luiz Lemos II. – 2. ed. – Florianópolis : Publicações do IF-SC, 2011.

[6] Moretti, Cláudio dos Santos. A importância da informação. Revista Gestão de Riscos – 147 ed. – São Paulo, 2020.

[7] Sêmola, Marcos, "Gestão da segurança da informação: uma visão executiva" 2. ed. – Rio de Janeiro: Elsevier, 2014.

[8] Estudos demonstram que tanto o Brexit (saída do Reino Unido da União Europeia) como a eleição do presidente dos Estados Unidos da América, Donald Trump, em 2016, tiveram influência pelo uso de dados pela empresa Cambrigde Analytica, que com a compreensão deles, utilizou-se de informações (falsas e verdadeira) pró e contra as referidas situações para "manipular" parte da população através das redes sociais com uso de tecnologia "bots" que envia mensagens conforme o perfil da pessoa que está a utilizar a rede, e assim, influenciar seu pensamento. (KOZLOWSKA, I. Facebook and Data Privacy in the Age of Cambridge Analytica. Seatlle: Henry M. Jackson School of International Studies; College of Arts and Sciences; University of Washington, 2019.)

[9] "O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, que é o novo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE), estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE.
Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD define novas regras e procedimentos do ponto de vista tecnológico." – Disponível em: https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx. Acedido em 16 de julho de 2023.

A segurança da informação pode ser definida como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. De forma mais ampla, podem os também considerá-la como a prática de gestão de riscos incidentes que impliquem o comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação. Dessa forma, estaríamos falando da definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e controle de ameaças e vulnerabilidades.[10]".

A confidencialidade, um dos pilares fundamentais da segurança da informação, "é a capacidade de garantir que o nível necessário de sigilo seja aplicado em casa junção de dados em processamento[11].", refere-se à proteção das informações contra acessos e divulgações não autorizadas. Dessa forma, impedindo a terceiros de aceder, visualizar dados confidenciais que são armazenados e transmitidos de forma segura.

O objetivo é que principalmente informações sensíveis sejam protegidas e inacessíveis a quem não esteja autorizado a tê-las, seja por proteção de dados pessoais, empresariais, ou qualquer conteúdo que não deva ser acessado por quem não é de direito obtê-los.

Para garantir a confidencialidade podem ser empregues diversas formas de segurança, como o uso de técnicas de criptografia de dados[12], acompanhamento de tráfego de rede[13], controle de acesso rigoroso, classificação de dados[14] e treinamento de pessoal sobre como garantir a segurança dos dados, conceitos que serão amplamente debatidos ao longo desse estudo.

Já a integridade[15] busca garantir a precisão, consistência e confiabilidade das informações, assegurando que não sejam alteradas e permaneçam iguais desde sua criação até seu armazenamento e transmissão. Ela tem por objetivo preservar o conhecimento, garantindo que os dados se mantêm confiáveis e consistentes ao longo do tempo.

Assim como na confidencialidade, também se utiliza a criptografia para proteção da integralidade, assim como assinaturas digitais, *backups* frequentes e remoção de dados

[10] Sêmola,, Marcos, "Gestão da segurança da informação: uma visão executiva" 2. ed. – Rio de Janeiro: Elsevier, 2014.
[11] Machado, Felipe Nery Rodrigues, "Segurança da Informação: Princípios e controle de ameaças." 1ª ed. – São Paulo: Érica, 2014.
[12] A criptografia envolve a conversão de texto simples legível por humanos em texto incompreensível, o que é conhecido como text o cifrado. Essencialmente, isso significa pegar dados legíveis e transformá -los de forma que pareçam aleatórios. A criptografia envolve o uso de uma chave criptográfica, um conj unto de valores matemáticos com os quais tanto o remetente quanto o destinatário concordam. O destinatá rio usa a chave para descriptografar os dados, transforman do-os de volta em texto simples legível.
[13] Software de monitoramento de rede fornece uma maneira conveniente de visualizar a atividade em toda a rede, incluindo quais dispositivos estão conectados quando o usuário não está na rede. Ele também irá alertar sempre que um novo dispositivo se conectar à rede.
[14] A classificação de dados ajuda a aprimorar a informação de segurança e garantir a privacidade de dados permitindo que atribua as permissões de acesso apropriadas e imple mente medidas de proteção apropriadas para diferentes tipos de da dos c o mo identificar reg ularme nte os da dos sensíveis que estão expostos.
[15] Hintzbergen, Jule. Hintzbergen, Kees. Smulders, André. Baars, Hans. "Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002" 3ª. ed. Rio de Janeiro: Brasport, 2018.

duplicados a partir da sua limpeza.

A disponibilidade refere que "toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitem dela para qualquer finalidade[16]", ou seja, tem por objetivo assegurar que as informações estejam sempre acessíveis, sem interrupções não planejadas. Toda vez que uma entidade legítima precise ter acesso elas estarão à disposição.

Além dos três princípios basilares da segurança da informação, ela ainda busca garantir a autenticidade[17], garantindo que a origem dos dados é segura e confiável, e o não repúdio, que permite comprovar a autoria das partes envolvidas e suas transações, que faz uso da assinatura digital com certificação digital, por exemplo, impedindo que uma pessoa ou entidade negue a autoria de algo que assinou.

Dessa forma, a segurança da informação tem como objetivo garantir que esses cinco princípios sejam cumpridos, através de um conjunto de práticas jurídicas, tecnológica e políticas, com o intuito de proteger as informações e sistemas de ameaças, tanto internas como externas.

As práticas mais utilizadas atualmente na sociedade e especialmente nas entidades bancárias são[18] a criptografia, autenticação forte[19] e controlo de acesso[20], o uso de *firewalls*[21], *backups*[22] e recuperação de desastres [23], prevenção de fraudes[24], conscientização e treinamento dos indivíduos e gestão de risco.

1.2. Diferença entre Segurança Cibernética e Segurança da informação

[16] Sêmola, Marcos, "Gestão da segurança da informação: uma visão executiva" 2. ed. – Rio de Janeiro: Elsevier, 2014

[17] Silva, Bruna Patrícia Ribeiro Alves da. "Planeamento e implementação de um sistema de gestão da segurança da informação.". Porto. 2011.

[18] Sêmola, Marcos, "Gestão da segurança da informação: uma visão executiva" 2. ed. – Rio de Janeiro: Elsevier, 2014

[19] Autenticação forte é também conhecida como autenticação de dois fatores, é um recurso de segurança online e sua principal função é proteger os dados. Ela fornece uma camada extra de segurança, ou seja, em vez de ser necessário se autenticar apenas com um *password*, por exemplo, é necessário mais uma forma de autenticação, que pode ser o recebimento de um código através do *sms*, biometria, assinatura digital, entre outras. "O que é autenticação forte? Como funciona e qual sua importância" Disponível em: https://www.linkedin.com/pulse/o-que-%C3%A9-autentica%C3%A7%C3%A3o-forte-como-funciona-e-qual-sua-paulo-oliveira/?originalSubdomain=pt Acedido em: 09.11.2023

[20] O controlo de acesso é um elemento fundamental da segurança que determina quem tem autorização para aceder a determinados dados, aplicações e recursos e em que circunstâncias. Disponível em: https://www.microsoft.com/pt-pt/security/business/security-101/what-is-access-control acedido em: 09.11.2023

[21] Firewalls são programas de software ou dispositivos de hardware que filtram e examinam as informações provenientes da ligação à Internet. Representam a primeira linha de defesa porque podem impedir que um programa malicioso ou atacante tenha acesso à rede e informações antes que qualquer potencial dano seja causado. Disponível em: https://www.mcafee.com/pt-pt/antivirus/firewall.html Acedido em: 09.11.2023

[22] Backup é uma cópia de segurança dos dados que estão guardados em um dispositivo de armazenamento ou sistema para outro ambiente. "O que é um Backup?" Disponível em: https://tecnoblog.net/responde/o-que-e-backup/ Acedido em: 09.11.2023

[23] A recuperação de desastres é o método utilizado por uma organização para recuperar o acesso e a funcionalidade da infraestrutura de TI após um desastre natural ou humano, como falha de equipamentos ou ataques cibernéticos.

[24] A prevenção de fraudes é uma estratégia implementada em diferentes empresas no sentido de detectar ações bancárias ou transações fraudulentas, impedindo que essas ações aconteçam e causem prejuízos financeiros ou afetem a reputação do cliente ou instituição. Disponível em: https://www.ewally.com.br/blog/cuidando-do-seu-dinheiro/prevencao-a-fraude#:~:text=O%20que%20%C3%A9%20preven%C3%A7%C3%A3o%20%C3%A0,reputa%C3%A7%C3%A3o%20do%20cliente%20ou%20institui%C3%A7%C3%A3o. Acedido em: 09.11.2023

Apesar destes conceitos muitas vezes serem confundidos, a diferença entre eles é necessária pois um abrange o outro[25]. A segurança da informação protege toda e qualquer informação, seja ela em formato digital ou não. Utiliza meios para cumprir o seu objetivo que passam por treinamentos de funcionários, no caso de empresas, da conscientização das pessoas quanto ao tratamento dos seus dados, segurança física do ambiente onde se encontram os *hardwares* e *softwares*, como prédios e estabelecimentos empresariais, por exemplo, englobando também os meios tecnológicos. A figura abaixo demonstra a relação entre a segurança da informação, a segurança cibernética, e a segurança da *internet*, do contexto *web* que são as navegações em *world wide web* - *www* (rede mundial de computadores) e de *network* que são todos os componentes de conexão, como, por exemplo, o *router*, os cabos e as empresas de telecomunicações que fornecem a conexão à *internet*[26].

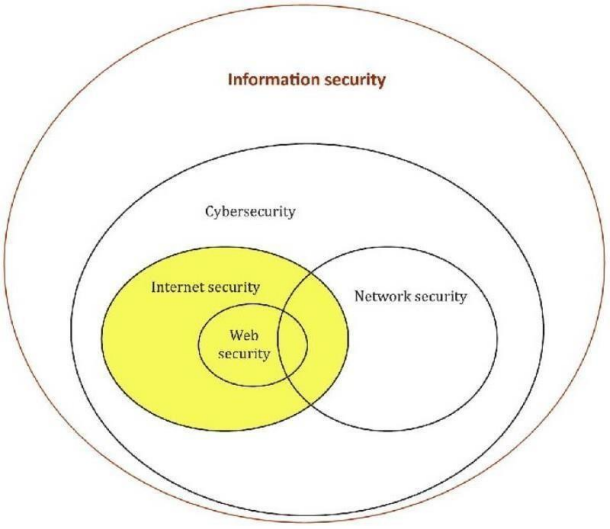


Figura 1 - (Fonte: *ISO/IEC 27032:2023*)[27]

A segurança da informação se preocupa também em proteger esses estabelecimentos de incêndios, de roubos, de empregados mal-intencionados ou não esclarecidos. Já a segurança cibernética[28] é uma parte da segurança da informação, e está focada apenas na proteção de sistemas, redes e dados existentes no ciberespaço frente às ameaças cibernéticas. Busca a proteção das informações que se encontram apenas no espaço cibernético, através de métodos tecnológicos.

[25] Vianna, Eduardo Wallier. Fernandes, Jorge Henrique Cabral. "O gestor da segurança da informação no espaço cibernético governamental: Grandes desafios, novos perfis e procedimentos." Brazilian Journal of Information Science 9.1 - 2015.
[26] Cybersecurity – Guidelines for Internet security - ISO/IEC 27032:2023(E). Disponível em: https://cdn.standards.iteh.ai/samples/76070/be57667fdd0b432490c253ca538c9938/ISO-IEC-27032-2023.pdf Acedido em: 10.09.2023 [27] Norma ISO/IEC 27032:2023: Esta norma fornece diretrizes sobre as estratégias de proteção e sustentabilidade dos processos de negócios no ciberespaço.
[28] da Silva, Michel Bernardo Fernandes. Cibersegurança: Visão Panorâmica Sobre a Segurança da Informação na Internet. Freitas Bastos, 2023.

Conforme Ventre[29], o ciberespaço é definido através de três dimensões "Uma primeira camada é constituída pela arquitetura material, física, *hardware*; ela é feita pelo conjunto de computadores, calculadoras, cabos eletrônicos (*hardw are layer*). Uma segunda camada, média, denominada *software* ou aplicativo, é constituída pelo conjunto de programas, códigos, dados e algoritmos que dão vida ao ciberespaço (*software layer*). E uma terceira camada, informacional, é a do sentido, das informações (*news*), dos conteúdos (*meatware layer*).", o ciberespaço é um novo campo, vasto, aberto[30], um domínio global no ambiente informacional, e os usuários da *internet* o consideram um território, e que ainda é indefinido[31].

Vale ainda esclarecer que *hardware* se refere a parte física, composta por equipamentos, e *software* a parte virtual, contendo programas, informações, sistemas, e assim por diante.

1.3. Segurança Cibernética no Setor Bancário

A cibersegurança tem grande relevância para o setor bancário em razão da magnitude e relevância dos dados por eles tratados, informações sensíveis e valiosas, como dados pessoais e transações financeiras dos seus clientes. O crescimento das atividades bancárias de forma *online* e o constante avanço da tecnologia dentro dessas instituições também os torna alvo principal dos cibercriminosos.

Foi este setor um dos pioneiros a dar maior atenção ao tema, visto sofrer constantes e criativos ataques. Não só por esta razão, como também pelo fato do Banco Central Europeu possuir diversas iniciativas regulatórias das quais os bancos precisam estar em conformidade, visando a proteção das informações de seus usuários e manter a confiança, que é essencial para o tipo de serviço prestado.

A segurança cibernética no setor bancário nada mais é do que um conjunto de medidas estratégicas e tecnológicas utilizadas para proteção dos seus *softwares*, com a consequente proteção dos dados e informações dos seus clientes, para manter os princípios fundamentais da segurança da informação já mencionados, como a integridade, confidencialidade e disponibilidade.

O que vem a ser de grande relevância não é apenas os bens por eles protegidos, e sim a que grandes ameaças estão a ser constantemente submetidos. Assim como os bens físicos dos

[29] Ventre, Daniel. O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras. Dilemas, Rev. Estud. Conflito Controle Soc. – Rio de Janeiro – Edição Especial no 3 – 2019 – pp. 75-96

[30] Levy, Pierre, A Inteligência Colectiva - Por uma Antropologia do Ciberespaço, Loyola, São Paulo, 1998.

[31] Casey, Eoghan. Digital Evidence and Computer Crime, Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet, 3.ª edição, Califórnia: Elsevier, 2011.

indivíduos podem ser acometidos por diversos crimes dispostos no código penal, como roubos, furtos, apropriação ilegítima, entre outros, no mundo informático as ameaças são efetuadas de forma virtual, mas também com o objetivo criminoso.

Assim como um ladrão pode utilizar uma arma para cometer um roubo, u m cibercriminoso pode fazer uso de um *e-mail*, ou de um *site* falso que direciona para outro sítio não esperado pelo usuário. E tudo isso pode se tornar ainda mais perigoso quando realizado dentro de um estabelecimento financeiro.

Em maio de 2022, durante uma conferência organizada pelo Banco de Portugal, a administradora Maria José dos Campos, do banco *Millennium BCP*, afirmou que a maior preocupação dos gestores financeiros hoje é a cibersegurança, e que um ataque cibernético de grande dimensão é uma inevitabilidade atualmente, em Portugal[32].

Ainda afirma a administradora que por ser "quase inevitável", o investimento com foco na proteção e detecção de problemas vêm sendo reforçado. Nessa vertente, e ainda nessa conferência, houve o apoio do diretor Carlos Moura do setor de sistemas e tecnologias do Banco de Portugal, que alertou que a cada 11 segundos uma empresa do mundo é atingida por alguma forma de ciberataque, e que, em média, as empresas demoram 20 dias para se recuperar do ocorrido.

Os principais responsáveis pelas instituições bancárias de Portugal não têm dúvidas de que um grande ciberataque irá se concretizar, o único questionamento que eles têm é quando esse ataque ocorrerá e como se preparar para ele.

Todavia, não é por terem a certeza de que um crime de tamanho considerável irá atentar os bancos que eles já não tenham ocorrido, apenas não houve nenhum que tenha sido irreversível. Com o exemplo disso temos um ciberataque ocorrido em outubro de 2022 contra o já mencionado *Millennium BCP*, que impediu o acesso à página na internet e às aplicações do banco aos seus clientes.

Segundo fontes oficiais do banco, entidades mal-intencionadas dirigiram intensos e não-legítimos pedidos ao *site* e a aplicação, dificultando e impedindo o acesso dos clientes. Esse ataque é denominado como *DoS* (*denial of service*), é um dos mais comuns e é feito enviando um grande número de pedidos ilegítimos ao sistema da entidade atacada, impedindo seu correto funcionamento[33].

[32] Caetano, Edgar. "É "uma inevitabilidade" que haja um grande ataque cibernético a bancos". Disponível em: https://observador.pt/2022/05/02/e-uma-inevitabilidade-que-haja-um-grande-ataque-cibernetico-a-bancos/ . Acedido em 30/07/2023.

[33] Neutel, Hugo. "BCP alvo de ciberataque. Situação já a normalizar, diz banco" Disponível em: https://www.jornaldenegocios.pt/empresas/banca-financas/detalhe/bcp-alvo-de-ciberataque-situacao-ja-a-normalizar-diz-banco Acedido em: 30/07/2023

Ainda mais recente, em junho de 2023, o Banco Europeu de Investimento foi atacado por um grupo de *hackers* russos que reivindicaram o crime. Esse ataque afetou a disponibilidade dos *sites* da organização. Através do *DDoS* (*distributed denial-of-service*) eles interromperam as operações normais do servidor, que ficou indisponível para uso[34].

O caráter crucial da cibersegurança no setor financeiro ainda pode ser destacada tendo atenção às obrigações que estas entidades possuem perante o Banco de Portugal, que é o banco central da república portuguesa[35]. Desde 2019 os bancos devem reportar qualquer incidente de cibersegurança que venham a sofrer, visto que podem comprometer sistemas e dados das entidades supervisionadas.

A instituição aponta que "são considerados incidentes de cibersegurança todos os eventos que tenham um efeito adverso na segurança dos sistemas, aplicações ou redes; que comprometam a informação que estes sistemas, aplicações e redes processam, armazenam ou partilham; e/ou que infrinjam as políticas de segurança de informação e uso dos sistemas, aplicações ou redes das entidades."[36].

Além disso, para maior empenho e eficiência na resposta aos incidentes de segurança, o Banco de Portugal possui uma unidade específica para isso, chamada de *CSIRT-BDP* (*computer security incident response team* - Banco de Portugal), que é o Centro de Resposta a Incidentes de Segurança do Banco de Portugal. Tem como missão "apoiar e proteger o Banco de Portugal – o banco central nacional de Portugal – o seu negócio, interesses e reputação de todos os tipos de ataques mal-intencionados que o possam prejudicar ou comprometer. As atividades do *CSIRT-BDP* são constituídas pela cibervigilância, antecipação, prevenção, deteção e resposta e recuperação.[37]".

Em junho de 2017 ocorreu uma conferência, realizada pelo Banco de Portugal, denominada "Cibersegurança no sistema financeiro: riscos, cooperação e governação", nesse evento foi enaltecida a importância da cibersegurança no setor financeiro, especialmente após dois grandes ataques, o *NotPetya*, que ocorreu em junho de 2017, e o *WannaCry*, em maio de 2017, ambos de escala global. Segundo o administrador Hélder Rosalino[38], apresentador na conferência, esses ataques demonstraram o quanto as entidades públicas e privadas não estão

[34] Geto, Daniel. "Banco Europeu de Investimento alvo de ataque informático DDoS". Disponível em: https://www.menosfios.com/banco-europeu-de-investimento-alvo-de-ataque-informatico-ddos/ Acedido em: 30/07/2023

[35] https://www.bportugal.pt/

[36] Instrução n.o 21/2019 BO n.o 11/2019 Suplemento • 25-11-2019 - Assunto: Reporte de Incidentes de cibersegurança - Banco de Portugal

[37] https://csirt.bportugal.pt/declaracao-de-missao. Acedido em: 31/07/2023

[38] Hélder Rosalino. Administrador. Nasceu em Sintra, em outubro de 1967. É Licenciado e Mestre em Gestão pelo ISCTE e Pós-Graduado em Fiscalidade pelo ISG.

suficientemente preparadas para enfrentar as ciberameaças[39].

Inclusive, elucidou que os ciberataques estão cada vez mais complexos e volumosos, que as redes de cibercrime estão cada vez mais sofisticadas, que não há um devido enquadramento legal, criando um sistema de impunidade, que pelo seu caráter imprevisível é necessária uma vigilância permanente e complexa e que o risco ao funcionamento das organizações está cada vez maior. Concluíram que hoje o mundo vive um momento de elevada com plexidade em termos de cibersegurança e que a ação deve ser imediata.

Relata ainda, a dependência que a sociedade vive em relação às tecnologias e a rápida velocidade que isso ocorreu, e que apesar de trazer consigo inúmeros benefícios, também traz uma série de preocupações. Afirma que é "neste contexto de ameaça quase permanente, sob diferentes facetas, que a cibersegurança assume uma crescente e fundamental importância". Conclui elucidando a importância da segurança cibernética "temos que começar por reconhecer que a cibersegurança tem atualmente um papel fundamental na defesa de alguns dos nossos princípios básicos de cidadania e mesmo na defesa de alguns dos alicerces fundamentais em que está construído o nosso modelo de vida atual. ".

O Banco de Portugal, como vigilante e modelo dos bancos portugueses, não só está atento à importância da cibersegurança no âmbito financeiro, como a considera fundamental na defesa de princípios básicos de cidadania. O risco cibernético pode afetar todos os alicerces dessas entidades, sendo um perigo para as suas reputações, causando a perda da confiança, um dano à marca de valor intangível, perda em custos e tempo para reparar[40].

Com o exemplo disso, tem-se o banco chileno, BancoEstado, o terceiro maior do país, que em 7 de Setembro de 2020 descobriu que sofreu um ataque por *ransomware*, e teve 12 mil dos seus computadores congelados, o que indica grandes falhas no controle de acesso à rede interna, e dessa forma ficou impedido de abrir quase todas as suas agências, de 417, apenas pôde abrir 24[41]. O ataque foi realizado através do *ransomware* denominado "REvil" que já havia feito outras inúmeras vítimas[42], mas nenhuma do porte do banco chileno.

O BancoEstado efetuou todas as medidas que eram determinadas no Chile na época do ataque, ou seja, abriu uma investigação sobre o incidente, e imediatamente comunicou o ocorrido

[39] Rosalino, Hélder. "Cibersegurança no sistema financeiro: riscos, cooperação e governação". 2017. Disponível em: https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20170630.pdf Acedido em: 01/08/2023.

[40] Webinar | Transformação Digital e o papel da Segurança Cibernética SPEEDNET- Direção de Segurança Cibernética Setembro, 2020

[41] Brito, Paulo. "Banco chileno atingido por ransomware: 12 mil computadores congelados". Disponível em: https://www.cisoadvisor.com.br/banco-chileno-atingido-por-ransomware-12-mil-computadores-congelados/ Acedido em: 01/08/2023

[42] Antes do ataque ao BancoEstado, diversos outros já haviam sido realizados e profissionais de cibersegurança já estavam atentos ao desenvolvimento desses ciberataques. https://olhardigital.com.br/2020/10/05/seguranca/resgate-devido-a-ataque-com-sodinokibi-chega-a-us-42-milhoes/

às autoridades. O CSIRT (equipa de resposta a incidentes de segurança da informação) chileno emitiu um comunicado de "Nível de Alerta Cibernética Alta" com uma campanha de prevenção ao *ransomware* direcionada ao setor privado, e solicitava que ficassem atentos aos seus sistemas porque havia probabilidade desse ataque se repetir em outras empresas. Inclusive ativou um nível alto de segurança dado o impacto significativo que esse ataque realizado contra um banco estatal poderia causar no resto da sociedade[43].

Nessa campanha a CSIRT sugeriu a implementação de inúmeras recomendações[44]: aumentar o monitoramento de tráfico, manter os equipamentos atualizados, tanto os sistemas operativos como outros *softwares* instalados, não abrir documentos de fontes desconhecidas, ter cuidado ao abrir documentos e selecionar *links* de *e-mails*, verificar e controlar serviços de área de trabalho remota, efetuar o bloqueio de script ou serviços remotos não permitidos no comunicado, monitorar serviços *SMB*[45] horizontalmente na rede, manter atualizadas as proteções perimetrais das instituições, aumentar os níveis de proteção em computadores que cumprem funções *AntiSpam*, *WebFilter* e antivírus, verificar o funcionamento e, se não for necessário, bloquear ferramentas como *PsExec*[46] e *PowerShell*[47], prestar atenção especial ao tráfego suspeito que tenha conexões com as portas 135TCP/UDP e 445TCP/UDP, verificar periodicamente os indicadores de comprometimento entregues pelo Csirt no Relatórios 2CMV20 e segmentar redes com base nas necessidades de seus ativos, permitindo apenas portas necessárias.

O BancoEstado informou que os fundos dos seus clientes não foram afetados e nem o patrimônio da instituição financeira[48]. E após o fato, em 9 de Setembro de 2020, emitiu um relatório sobre o que aconteceu e os procedimentos realizados[49]. Nele informou que no dia 5 de Setembro recebeu um alerta que uma de suas máquinas tinha sido afetada, sua equipa de cibersegurança analisou e detetou que se tratava de um *ransomware* e que ele havia encriptado

[43] Tavares, Pedro. Banco do Chile sofre ataque ransomware (REvil). 2020. Disponível em: https://seguranca-informatica.pt/banco-do-chile-sofre-ataque-ransomware-revil/ . Acedido em: 09.11.2023

[44] Alerta de Seguridad Cibernética. Disponível em: https://www.csirt.gob.cl/media/2020/09/COMUNICADO-CSIRT-ALERTA-CIBERNETICA.pdf . Acedido em: 09.11.2023 .

[45] SMB (sigla para Server Message Block, ou "bloco de mensagens do servidor") é um protocolo de rede que permite às pessoas se comunicarem com computadores e servidores remotamente para usar os recursos destes dispositivos remotos (compartilhar, abrir ou editar arquivos, por exemplo). "O que é o protocolo SMB? ". Klusaite, Laura. Disponível em: https://nordvpn.com/pt-br/blog/o-que-e-smb/ . Acedido em: 09.11.2023 [46] O PSEXEC é uma ferramenta desenvolvida pela Microsoft que nos permite executar diversos procedimentos remotamente, de forma simples e fácil, utilizando a linha de comando do Windows. "PSEXEC: O que é e como usar?". Dias, Ivo. Disponível em: https://igd753.medium.com/psexec-o-que-%C3%A9-e-como-usar-dd18b8097e81 . Acedido em: 09.11.2023

[47] O PowerShell é uma solução de automatização de tarefas entre plataformas composta por uma shell de linha de comandos, uma linguagem de scripts e uma arquitetura de gestão de configuração. O PowerShell é executado no Windows, Linux e macOS. Disponível em: https://learn.microsoft.com/pt-pt/powershell/scripting/overview?view=powershell-7.3 . Acedido em: 09.11.2023

48 TrendTic. Banco estado: ransomware sodinokibi sería el responsable del cierre de sucursales y csirt del gobierno mantiene "alerta cibernética alta". Disponível em: https://www.trendtic.cl/2020/09/banco-estado-ransomware-sodinokibi-seria-el-responsable-del-cierre-de-sucursales-y-csirt-del-gobierno-mantiene-alerta-cibernetica-alta/ . Acedido em: 09.11.2023

[49] Ciberseguridad en Banco Estado – Senado. Disponível em: https://www.senado.cl/appsenado/index.php?mo=tramitacion&ac=getDocto&iddocto=9955&tipodoc=docto_comision. Acedido em: 09.11.2023

diversos arquivos do banco. Assim executou o protocolo de resposta de incidente de cibersegurança, e ativou o comitê de crises.

Esse comitê efetuou medidas de contenção, a medição de impacto e estabeleceu o plano de recuperação. As medidas de contenção realizadas foram: "O Internet Bank foi desconectado, a maioria dos servidores confidenciais são desligados: transações rápidas e de alto valor, é realizada uma revisão completa de computadores e servidores críticos, a propagação é controlada, é contratado suporte especializado com a Microsoft, que é constituída imediatamente, estão implementadas ferramentas de desinfecção específicas para este vírus e ativação do plano de comunicação interna e externa". Os impactos detetados foram que o vírus afetou plataformas Windows, principalmente canais de serviço em pessoa (Agências Bancárias, Serviestado) e os serviços não afetados foram *Web people*, *Mobile APP*, *ATMs* e "Caixa vizinha". Por fim o plano de recuperação priorizou a restauração da ordem dos serviços, reestabeleceu o trabalho de diferentes equipas e recompôs a continuidade do serviço. Ainda informou que não houve roubo de dados dos clientes. O gasto total do BancoEstado foi de 20 milhões de dólares.

O relatório de Cibersegurança em Portugal [50], emitido pelo Centro Nacional de Cibersegurança[51], com o contributo, entre outras entidades, do Ministério Público, na edição de 2020 constatou que o aumento do número de cibercrimes em Portugal em 2020 foi de 48% em comparação ao ano de 2021[52]. Relata que "considerando os crimes registados pelas autoridades policiais, e observando apenas os crimes estritamente informáticos, verifica-se que estes em 2022 aumentaram 48% face ao ano anterior, de 1496 para 2219. Um crescimento significativo, o maior nesta tipologia desde que há registos. Somando a estes a burla informática/comunicações e a devassa por meio de informática, isto é, contabilizando todos os crimes relacionados com a informática recolhidos pela DGPJ, o aumento é de apenas 1%, de 23 409 em 2021 para 23 651 em 2022.". Também o Relatório Anual de Segurança Interna (RASI) de Portugal [53] demonstra que em 2022 o cibercrime teve um aumento de 48,3% com relação ao ano anterior, sendo a maior parte dos crimes de interceção ilegítima, sabotagem informática e viciação/destruição de dados.

---

[50] Relatório Cibersegurança em Portugal. disponível em: https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf 4ª Riscos e Conflitos - 4ª ed. Acedido em: 01/08/2023.

[51] Através da Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril, é criada a comissão instaladora que tem por objetivo a criação, instalação e operacionalização de um Centro Nacional de Cibersegurança. A 6 de outubro de 2014, é criado o CNCSeg, dentro do Gabinete Nacional de Ciberse gura nça, através do Decreto-Lei n. º 69/ 20 14, de 9 de maio. O CNCS adquire a sua designação atual através do Decreto -Lei n. º 136/2017, de 6 de novembro. Com a publicação da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segura nça do Ciberes paço, é atribuída ao CNCS a competên cia de Autorida de Nacional de Cibersegurança e ao CER T. PT a de ponto de contacto único internacional para reação a ciberincidentes.

[52] ANDRADE, Francisco Pacheco de, FONSECA, Isabel, SILVA, Joana Aguiar e, ABREU, Joana Covelo de, JERÓNIMO, Patrícia, VENÂNCIO, Pedro Dias, e FREITAS, Pedro Miguel, Relatório Cibersegurança em Portugal: Ética & Direito, Braga, JusGov e CNCS, 2020

[53] Relatório Anual de Segura nça Interna (RASI) 2022. Disponível em: https://www.ssi.gov.pt/sites/default/files/2023-07/20230331_pm_RASI_2022.pdf

Um dos crimes que chama a atenção é a fraude por meio de pagamentos eletrónicos, e o que o relatório constata é que na maior parte das vezes isso ocorre por falta de mecanismos de segurança, como a validação multifator que será explicada ao longo deste estudo e, aliado a isso está a inexistência de mecanismos de proteção na transmissão dos dados cliente - servidor e a disponibilização de códigos de acesso/segurança a terceiros.

O crescimento anual do cibercrime é a realidade atual em Portugal e no mundo. Co m ataques cada vez mais incrementados e inesperados, os bancos, hoje, contam com o implemento de métodos de cibersegurança que sejam capazes de conter os *hackers*.

1.4. Cibercrime, seus autores e o sistema informático

Não é possível falar em cibercrime sem antes compreender quem são os seus autores. Eles são o sujeito ativo que comete o crime, o autor da infração penal, que é a pessoa que de forma direta, ou indireta, pratica a conduta descrita pelo tipo legal. A teoria da comparticipação criminosa, que distingue autores e participantes no crime, é uma teoria dos tipos de crime dolosos. A teoria do domínio do facto, hoje absolutamente dominante, diz, segundo o Professor Figueiredo Dias[54], que "Autor é, segundo esta concepção e de forma sintética e conclusiva , quem domina o facto, quem dele é "senhor", quem toma a execução "nas próprias mãos" de tal modo que dele depende decisivamente o *se* e o *como* da realização típica; nesta precisa acepção se podendo afirmar que o autor é a *figura central do acontecimento*".

No ambiente digital a atuação dos criminosos não é diferente do demonstrado, entretanto os sujeitos ativos do crime são conhecidos como *hackers*, que têm definições muito mais complexas do que comumente se conhece. Pode-se destacar entre os cibercriminosos os *hackers* e os *crackers*, sendo que "o primeiro tem o objetivo de invadir sistemas de informação para obtenção de dados, ou simplesmente para testar seus conhecimentos e colocar em prática suas técnicas, enquanto que o segundo, pouco divulgado pela mídia, tem a finalidade de causar prejuízos, seja criando contas bancárias falsas e transferindo dinheiro para elas, como destruindo sistemas, para tirá-los do ar, dentre outras formas de trazer danos às suas vítimas.[55]".

Os *hackers* possuem vasto conhecimento das linguagens de programação, redes de computadores, protocolos, e dessa forma, conseguem facilmente descobrir todos os tipos de

[54] Dias, Jorge de Figueiredo. Direito Penal: parte geral. Tomo I. 1. ed. brasileira. 2. ed. portuguesa. Coimbra: Coimbra Editora . 2007.
[55] Machado, Thiago. Cibercrime e o crime no mundo informático A especial vulnerabilidade das crianças e dos adolescentes. Porto, 2017.

vulnerabilidades presentes nos sistemas informáticos. Sua intenção, diferente do *cracker*, não é necessariamente causar prejuízo para a vítima, e muitas vezes utiliza da sua intervenção para alertá-la sobre suas fragilidades. "Os próprios hackers não vêem suas atitudes como ilícitas ou como capazes de prejudicar terceiros, eles acreditam que estão prestando um serviço à comunidade digital ao vasculhar a Rede em busca de falhas, se é que pode ser considerado dessa forma, pois uma vez invadido um computador o acesso a qualquer tipo de informação poderia ser considerado crime, uma vez tal conduta poderia ser enquadrada como invasão da intimidade, ou poderia estar colocando em risco segredos industriais e governamentais, o que indubitavelmente levaria empresas e governos a sofrerem enormes prejuízos.[56]".

Os *hackers* possuem uma cultura própria, denominada "cultura hacker"[57], e na maioria das vezes realizam seus atos com base nas suas ideologias. Inclusive, no meio informático, ser considerado um *hacker* é um grande elogio.

Já o *cracker*, conhecido equivocadamente na sociedade em geral como *hacker*, também é um indivíduo que possui um vasto conhecimento em sistemas informáticos, porém sua intenção é realizar ataques e ter algum benefício próprio. São considerados os "*hackers* maus", que trilham o caminho do crime no meio digital. A diferença entre os dois tem apenas um condão subjetivo, já que o propósito do *cracker* ao invadir sistemas é obter vantagens financeiras ou causar dano no computador da vítima[58].

Ainda enquadrado na categoria de *hackers*, podem ser divididos em três espécies, os *white hats*, *black hats* e *gray hats*[59]. Os *white hats* buscam vulnerabilidades nos sistemas informáticos com o intuito de protegê-los, normalmente trabalham na área de cibersegurança de empresas para garantir que os dados permaneçam seguros e evitar ataques externos. Os *black hats* são os hackers que invadem sistemas, criam vírus, colapsam redes, entretanto, diferente dos *crackers*, eles não procuram obter benefício próprio, eles querem demonstrar suas aptidões informáticas. Já os *gray hats* variam entre as duas categorias, em alguns momentos apenas mostram as vulnerabilidades existentes nos sistemas e em outros acabam por invadi-los e ter

[56] Inacarato, Flávio. "Hackers, Crackers e nova modalidade de crime virtual – Ransomware, e a Responsabilidade nos Crimes Eletrônicos"

[57] "A cultura hacker tem origens no MIT – Instituto de Tecnologia de Massachussets e em outros laboratórios norte-americanos, como o PARC, da Xerox. Ela se baseia em três pilares: colaboração, conhecimento e liberdade. No código de ética, há algumas regras que devem ser seguidas, como não apagar intencionalmente ou danificar um arquivo em um computador invadido, notificar os administradores de sistemas sobre qualquer brecha encontrada, não invadir para roubar dinheiro ou informações, sempre estar disposto a compartilhar seu conhecimento, métodos, dentre outros." Souza, Franciele. Cultura Hacker. Disponível em: https://edisciplinas.usp.br/mod/glossary/print.php?id=62879&mode=author&hook=ALL&sortkey=FIRSTNAME&sortorder=asc&offset=50 Acedido em: 02/08/2023.

[58] Vianna, Túlio Lima. Hackers: um estudo criminológico da subcultura cyberpunk. Informática e internet: aspectos legais internacionais ed.Rio de Janeiro : esplanada,2001

[59] Quispe, Carlos Alberto Flores. Tipos de Hackers. Universidad Mayor de San Andrés, 2009, 16-18.

atitudes criminosos.

Os crimes cibernéticos são atos realizados normalmente pelos *crackers*, mas também são cometidos por *hackers*, e ofendem "interesses relativos ao uso, à propriedade, à segurança ou à funcionalidade de computadores e equipamentos periféricos (*hardwares*), redes de computadores e programas de com putador (estes denominados *softwares*).". Os atos criminosos, realizados à distância, são "todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede, que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação.[60]".

O conceito de cibercrime, ou crime informático, não é simples, e possui duas vertentes, uma que considera a criminalidade informática em sentido amplo e a outra em sentido estrito. Conforme Pedro Dias Venâncio[61], "na criminalidade informática em sentido amplo, incluímos toda panóplia de atividade criminosa que pode ser levada a cabo por meios informáticos, quer quando a informática é apenas um instrumento para a prática de atos acessórios ou preliminares, quer quando integra os elementos de um determinado tipo legal de crime.", ou seja, em sentido amplo estão incluídos os crimes que apenas são iniciados por meio digital, que tem apenas seus atos preparatório ou acessórios em ambiente digital, como também os crimes que são totalmente cometidos digitalmente.

Já a criminalidade em sentido estrito, também nas palavras de Dias Venâncio[62], é "aquela em que o elemento digital surge com o parte integradora do tipo legal ou mesmo como seu objeto de proteção. Ou seja, trata-se não só dos que têm por bem jurídico protegido o próprio acesso ou funcionalidade da sociedade da informação, mas de todos aqueles em que a informática faz parte necessária dos seus elementos típicos.". Os crimes que se enquadram na Lei do Cibercrime são os crimes em sentido estrito que tutelam a confiança nos sistemas informáticos, e estão previstos nela com o fim de reforçar a confiança nos sistemas informáticos, a segurança e o valor jurídico dos atos eletrónicos e os valores gerais comuns a todo ordenamento penal[63]. Esse conceito faz-se de extrema importância a esse estudo, visto serem os crimes constantes na lei do cibercrime relacionados ao presente contexto.

[60] Aras, Vladimir. Crimes de informática.: Uma nova criminalidade. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: https://jus.com.br/artigos/2250. Acesso em: 7 ago. 2023.

[61] Venâncio, Pedro Dias. "Tipos legais de crimes informáticos". "Criminalidade – Novos desafios, ofensas e soluções", Inês Guedes e Marcis Gomes (Coordenadores), PACTOR, Lda, 2021.

[62] Venâncio, Pedro Dias. "Tipos legais de crimes informáticos". Criminalidade – Novos desafios, ofensas e soluções", Inês Guedes e Marcis Gomes (Coordenadores), PACTOR, Lda, 2021.

[63] Venâncio, Pedro Dias. "Tipos legais de crimes informáticos". Criminalidade – Novos desafios, ofensas e soluções", Inês Guedes e Marcis Gomes (Coordenadores), PACTOR, Lda, 2021.

Segundo Guedes[64], o cibercrime pode ser conceituado como "um conjunto de ofensas que partilham uma importante característica, nomeadamente, o facto de serem cometidas através de um computador e de tecnologia eletrónica digital", pode ser praticado contra qualquer pessoa física ou jurídica, individual ou colectiva, pública ou privada, a qualquer momento e circunstância, desde que conectado a um sistema/rede informática ou telemática[65] .

Conforme Sydow[66], os crimes informáticos possuem padrões que estruturam todo o raciocínio jurídico-penal, e que a partir dele existem características com uns a todos os sistemas informáticos que são o alvo dos cibercriminosos, dessa forma mostra-se importante conceituá-los. A Lei do Cibercrime de Portugal conceitua sistema informático como "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;"[67].

As características dos sistemas informáticos importantes para se compreender como ocorrem os crimes informáticos analisadas por Sydow[68] são a interatividade, a mobilidade, a conversabilidade, a conectividade, a ubiquidade, a globalização, a fracionabilidade, a divisibilidade, a intangibilidade, a disponibilidade, a pluralidade, a velocidade e a não territorialidade.

A **interatividade** diz respeito à participação humana, é necessário o comando de um usuário para que qualquer ato ocorra. O utilizador tem o poder de comandar o sistema através de suas ações perante ele[69]. Um computador, atualmente, não possui a capacidade de atuar sem que exista um indivíduo executando-o. Dá como exemplo o "sistema de Internet *banking* que tem como finalidade o controle de contas bancárias, investimentos e outros serviços bancários, exclusivamente. Foi projetada para que seja possível ao indivíduo acessar sua própria conta (ou alguém por ele autorizado) com intenções legais ou ilegais, dependendo somente de seu juízo de valor.", "O sistema de Internet *banking* tem como finalidade o controle de contas bancárias, investimentos e outros serviços bancários, exclusivamente. Foi projetada para que seja possível ao indivíduo acessar sua própria conta (ou alguém por ele autorizado) com intenções legais ou

[64] Guedes, Inês Sousa. Moreira, Samuel. Cardoso, Carla. "Cibercrime: conceptualização, desafios e perceções públicas". Criminali dade – Novos desafios, ofensas e soluções", Inês Guedes e Marcis Gomes (Coordenadores), PACTOR, Lda, 2021.
[65] Dias, Vera Marq ues. "A proble mática da investigaçã o do cibercrime ". DataVenia, revista j urídica digital. Ed. nº 1. 20 12. Dispo nível e m: https://www.datavenia. pt/ficheiros/edicao01/datavenia01_p063-088.pdf Acedido em: 10 de set. 2023.
[66] Sydow, Spencer Toth. "Crimes Informáticos e suas vítimas" . Editora Saraiva, 2000.
[67] Lei n.º 109/200 9, de 15 de Sete mbro - Lei do Cibercri me.
[68] Sydow, Spencer Toth. "Crimes Informáticos e suas vítimas" . Editora Saraiva, 2000.
[69] Sandim, Miguel. Ribeiro, Susana. "Realidade Virtual e Interatividade". Póvoa do Varzim. 2011.

ilegais, dependendo somente de seu juízo de valor."[70]. A interatividade não se limita a somente dois pontos[71], mas de todos para todos[72].

A **mobilidade** demonstra que não é mais possível ligar um IP (*Internet Protocol* - protocolo de rede) a um ambiente físico, visto que, diferentemente de anos atrás, quando um computador não era apto a ser movido com facilidade, hoje temos a possibilidade de transporte dos aparatos informáticos, visto a sua miniaturização. Dessa forma, as ações praticadas dentro das redes podem ser feitas de qualquer lugar, bastando apenas o acesso. Atualmente com o advento do telefone móvel, da internet sem fio, se questiona os espaços públicos e os privados, já que a mobilidade tem causado a privatização do espaço público, já que pode -se estar conectado à *internet* em qualquer sítio na rua[73]. Para Lemos[74] não vivemos apenas a era da conexão, mas também a era da mobilidade.

Já a **conversabilidade** demonstra a capacidade que os equipamentos informáticos, mesmo que possuam diferentes linguagens, têm de interagirem entre si. Independente do modelo, marca, *software*, há condições de "haver troca de informações, e, desta feita, troca de comandos entre aparelhos diferentes, levando-se, pois, a possibilidade de o usuário de um aparelho, em paridade com outro, acesse-o, visualize suas informações e até mesmo controle-o remotamente"[75].

A **conectividade** é a capacidade tecnológica que os aparelhos informáticos possuem de se conectarem uns aos outros. A maioria dos equipamentos modernos têm essa aptidão, e apenas depende da habilidade de conversibilidade, existindo essa característica, eles se conectam facilmente uns aos outros, bastando a vontade dos usuários envolvidos.

A **ubiquidade**, também denominada simultaneidade e onipresença, guarda relação com bens tangíveis. Ou seja, é "a presença desta no cotidiano de cada indivíduo da sociedade, sem que este perceba a atuação daquele."[76], é a capacidade de estar presente em diversos lugares ao mesmo tempo. Essa característica traz grandes debates no âmbito jurídico-penal visto que se a internet está em todo lugar ao mesmo tempo, muitas dúvidas sobre a competência para julgar os crimes informáticos podem surgir.

A **globalização** demonstra a quebra de fronteiras que a rede mundial de computadores

[70] Sydow, Spencer Toth. "Crimes Informáticos e suas vítimas" . Editora Saraiva, 2000.
[71] Ascensão, José de Oliveira. Estudos sobre o Direito da Internet e da Sociedade de Informação. Almedina, 2001.
[72] Castells, Manuel. A Era da Informação: Economia, Sociedade e Cultura, Vol. I A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian, 2005.
[73] Lemos, André. "Cultura da mobilidade." Revista Famecos 2009.
[74] Lemos, André. "Cultura da mobilidade." Revista Famecos 2009.

ocasionou. A globalização faz parte da sociedade há muito tempo, segundo Marques [77] ela tem como um de seus primeiros momentos marcantes os descobrimentos e expansões marítimas europeias, entretanto com a chegada da tecnologia ela se tornou muito mais nítida e se expandiu com grande rapidez.

O conceito de globalização poderia ser facilmente chamado de popularização, visto o crescimento exponencial do acesso à tecnologia e conectividade, que "fez com que as pessoas se aproximassem mesmo que estivessem a milhas de distância, rompendo com os impedimentos geográficos e mudando assim, radicalmente, o panorama da sociedade. Com a presença do telefone, da televisão, da rádio, do computador e da Internet, os nossos hábitos de facto modificaram-se"[78]. Nota-se que "ainda que vivamos num mundo com línguas e culturas particulares para cada soberania, no que se refere à contato ou potencialidade de interação entre hemisférios, países e regiões, a tecnologia retirou o caráter restritivo das fronteiras, garantindo que qualquer episódio ocorrido em qualquer localidade do planeta seja imediatamente conhecido por todos os países conectados, num misto de contaminação e interação."[79].

Já a **fracionabilidade** é um dos pontos fundamentais para se compreender os crimes informáticos, e isso se deve ao fato de que os dados são fracionáveis, podendo ser reduzidos a pedaços de programação. Ou seja, se uma pequena parte de códigos programados, seja uma linha ou um simples caractere, for alterado, removido ou acrescentado, pode levar à completa inutilidade do arquivo, afetando diretamente a sua integridade.

A **divisibilidade** está relacionada à ideia de composição de dados e sua segmentação, e diretamente associada à forma como estes são transferidos na rede mundial de computadores. Diferentemente da fracionabilidade que está associada a segmentação dos dados. Para comunicação das redes há trocas constantes de comandos e de dados, e, nas palavras de Sydow "o fato de a Internet ser difusa faz com que os dados tenham inúmeros caminhos diferentes para atingirem o mesmo destino, todos igualmente viáveis e aptos. Também, uma vez que se trata de transmissão de dados na velocidade da luz, o cumprimento de vias que os dados precisariam trilhar até atingir o destino é praticamente irrelevante." [80]. Ou seja, para que o envio e recebimento seja eficaz, "surge a possibilidade de promover "cortes" nos arquivos com a criação de diversos trechos de programação sem significado sozinhos, mas que, reagrupados com outros trechos

[77] Marques, Daniela Filipa Guerreiro. Os Efeitos da Globalização e Das Novas Tecnologias No Jornal de Letras, Artes e Ideias-Uma Análise Geral. Diss. Universidade de Lisboa (Portugal), 2016.
[78] Marques, Daniela Filipa Guerreiro. Os Efeitos da Globalização e Das Novas Tecnologias No Jornal de Letras, Artes e Ideias-Uma Análise Geral. Diss. Universidade de Lisboa (Portugal), 2016.
[79] Sydow, Spencer Toth. "Crimes Informáticos e suas vítimas". Editora Saraiva, 2000.
[80] Sydow, Spencer Toth. "Crimes Informáticos e suas vítimas". Editora Saraiva, 2000.

adequados referentes ao arquivo fragmentado, voltam a compor o arquivo integral, agora transmitido para outro local da rede".

A **intangibilidade** refere-se ao fato de os dados serem intangíveis, ou seja, não podem ser tocados, não são materiais e nem materializáveis por si só. Conforme Santos [81] as redes são duplamente invisíveis "porque os circuitos, as ondas, o *software*, as senhas, são impercetíveis aos sentidos humanos e também por sua complexidade". Para melhor compreensão da amplitude desse significado, os dados mesmo não sendo palpáveis, são protegidos juridicamente como se fossem um bem móvel, possuindo a mesma proteção jurídica dos direitos autorais. Sydon[82] destaca de forma esclarecedora que "a característica da imaterialidade se mostra bastante peculiar pois leva a uma forte dificuldade de adaptação das regras já existentes atinentes a delitos que violam patrimônio e, portanto, gera uma necessidade de legislação especial".

A **disponibilidade**, já referida e explicada anteriormente como um dos princípios fundamentais da segurança da informação, também é uma das características do sistema informático, que diz respeito ao sistema ter que estar disponível ininterruptamente para que possa ser acessado a qualquer momento que seja necessário.

A **pluralidade** é, nas palavras de Sydon, a "possibilidade de existirem diversos arquivos originais, idênticos, e com as mesmas funcionalidades, pois que bits são imateriais e plurais.", os dados para serem compreendidos pelos humanos precisam ser decodificados, e, dessa forma, um arquivo original pode ser de propriedade de múltiplos usuários.

A **velocidade** é uma característica elementar, visto que a rapidez das conexões cresce a cada ano. Nas palavras de Sydon, "a transferência de dados passa também a ser feita em espaços mais curtos de tempo. Assim, arquivos maliciosos, por terem tamanho diminuto, terminam por ingressar em aparatos alheios em fração de segundo, de maneira praticamente impercetível pelo usuário, dificultando sua proteção e domínio dos acontecimentos dentro da máquina. Outra característica fundamental trazida pela velocidade das conexões e dos processamentos de dados está nos crimes de violação de direitos autorais provenientes de peças audiovisuais, mídias fonográficas e até mesmo programas de computador. Com o advento da velocidade crescente de transferência de dados, mais usuários terminarão por ser incentivados a baixarem um grande número de dados, violando propriedades imateriais dos autores. A velocidade aumenta tanto a possibilidade de baixar (*download*) arquivos legalmente protegidos para as máquinas, quanto

[81] da Costa Santos, Plácida Leopoldina. Vidotti, Silvana. "Quando as webs se encontram: social e semântica -promessa de uma visão realizada.". 2009.
[82] Sydow, Spencer Toth. "Crimes Informáticos e suas vítimas". Editora Saraiva, 2000.

carregar na rede (*upload*) peças protegidas. E quanto maior a velocidade e a capacidade de armazenamento, maior a incidência de tais ações violadoras de bem jurídico.".

Por fim, tem-se a **não-territorialidade**, que é o fato de os sistemas informáticos não estarem fixos em um único local, não há limitação geográfica nos meios computacionais. Conforme Conte[83], território "sob o prisma geográfico, trata-se do espaço físico delimitado por fronteiras", entretanto com os meios digitais não existe tal delimitação, o que altera o que se entende por território, sendo, nesse caso, onde se encontra a informação. Ainda elucida que "a informação na rede, portanto, passa a ser elemento identificador do território no ciberespaço. Assim, essas características faze m com que a Internet tenha uma maior dificuldade em estabelecer um "centro de comando" tal como na versão tradicional de território físico delimitado". Dessa forma, tem-se como característica da rede de com putadores a não-territorialidade.

Todas essas características são de extrema importância para a compreensão da forma como o cibercrime é cometido. Ele difere de modo e lugar da restante criminalidade convencional. Conforme o Relatório "Riscos & Conflitos 2023", do Observatório de Cibersegurança do CNCS, "as ciberameaças a afetar o ciberespaço de interesse nacional em 2022 de modo mais relevante foram o *ransomw are*, a cibersabotagem/indisponibilidade, o *phishing*/*smishing*/*vishing*, a burla online, outras formas de engenharia social e o comprometimento de contas/tentativa de *login*". E "As principais tendências nacionais, no que se refere ao quadro de ameaças no ciberespaço, são a crescente 'profissionalização' do cibercrime, a incerteza resultante da guerra na Ucrânia e algumas ciberameaças específicas, tais como o *ransomware*, o *DDoS*, o *malware* de furto de credenciais e os *smishing*/*vishing*/*spoofing* oportunistas relativamente ao uso massificado do telemóvel.".

Abaixo um "gráfico" do relatório que mostra a cronologia dos ataques no ciberespaço com maior relevância em Portugal no ano de 2022:

[83] Conte, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. Desafios do direito penal no mun do globalizado: a aplicação da lei penal no espaço e os crimes informáticos. 2012.



Figura 2 – (reproduzido por Relatório "Riscos & Conflitos 2023", do Observatório de Cibersegurança do CNCS)

E as ameaças mais utilizadas e seus responsáveis:

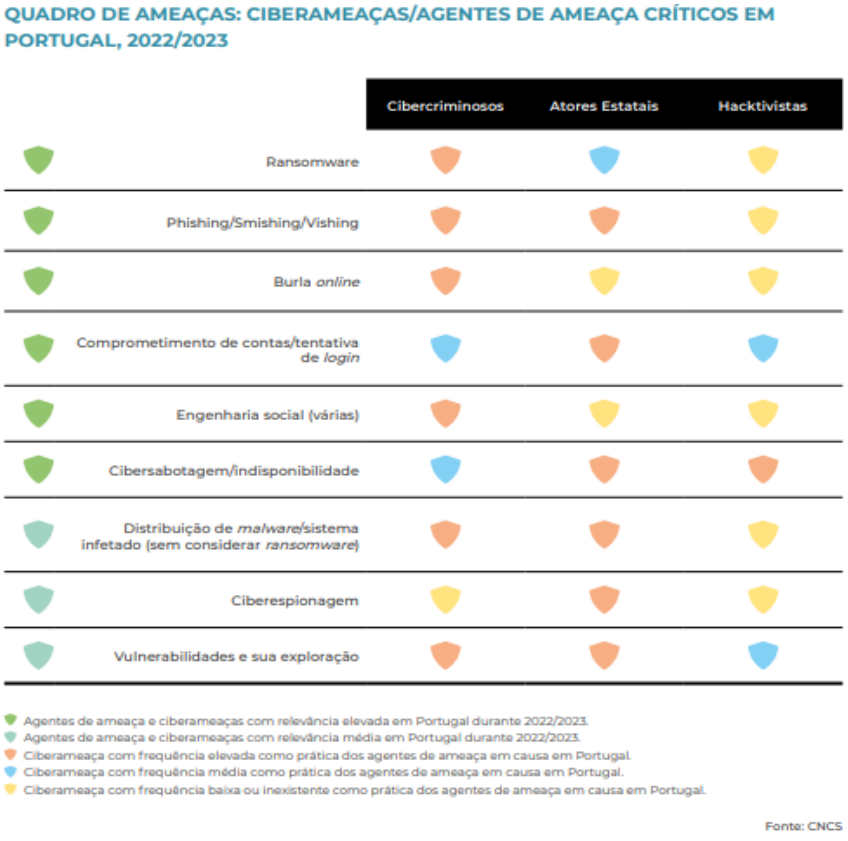


Figura 3 – (reproduzida por Relatório "Riscos & Conflitos 2023", do Observatório de Cibersegurança do CNCS)

1.5. Ciberataques

Muitos ataques são realizados por espécies de *malwares*[84], que é o termo que descreve

[84] Melo, Laerte Peotta, et al. "Análise de malware: Investigaçao de códigos maliciosos através de uma abordagem prática." Sociedade Brasileira de

qualquer programa ou código malicioso. Ou seja, é um programa inserido em um sistema, normalmente de forma encoberta, com a intenção de comprometer um, ou vários, pilares da segurança da informação (confidencialidade, integridade ou disponibilidade). É a ameaça mais significativa à maioria dos sistemas, podendo resultar em amplos prejuízos e perturbações, eventos que demandam extensivos esforços para recuperação. São exemplos de *malware* o *ransomware*, *spyware*, os vírus, *keyloggers*, entre outros.

O *ransonware*[85] faz parte da família dos *malwares* que abrange todos os *softwares* maliciosos, a tradução da palavra já explica muito sobre ele, que se originou da junção da palavra *ranson* que significa resgate e *software* que quer dizer código/programa, ou seja, programa de/para resgate. Nas palavras de Saisse[86], "Tal mecanismo originou as expressões "sequestro" de dados, interpretada como ato de bloquear, inutilizar ou inviabilizar o acesso à dados, e extorsão digital ou criptoviral, ato de solicitar vantagem ilícita/pagamento em troca da liberação dos dados. Essa praga cibernética ganhou grande destaque no cenário internacional rotulada como a ameaça cibernética de maior rentabilidade para a cibercriminalidade". O *ransomware* foi criado com o objetivo de infiltrar-se em sistemas sem a percepção de seu titular. Conforme os ensinamentos de Liska[87], "as duas principais formas de *ransomware* são aquelas que criptografam, ofuscam ou impedem o acesso aos arquivos, e aquelas que restringem o acesso ou bloqueiam os usuários dos sistemas". Após a invasão ao sistema ser efetuada, o cibercriminoso inicia um mecanismo de exibição de imagens/mensagens informando sobre como realizar o resgate dos dados mediante um pagamento. Normalmente os valores são cobrados em bitcoins, devido ao anonimato que essa forma de transação possui.

O *ransomware* se propaga de várias formas[88], incluindo a infiltração via acesso a *websites* suspeitos, que insere o código malicioso mediante a mera visita do usuário. Além disso, esta ameaça pode se ocultar em arquivos dissimulados, como por exemplo, em registos musicais ou de imagens, frequentemente disseminados através de plataformas de redes sociais ou distribuídos via correio eletrônico. Estes arquivos frequentemente são camuflados sob pretextos aparentemente corriqueiros, tais como tópicos de interesse público, questões de ordem financeira, causas sociais, entre outros. Paralelamente, a disseminação do *ransomw are* pode ser executada mediante a exploração de vulnerabilidades em aplicativos instalados em dispositivos móveis ou

Computação (2011).

[85] Liska, Allan; Gallo, Timothy. Ransomw are: defendendo-se da extorsão digital. Novatec Editora, 2019.

[86] Cabral Saisse, R.. Ransomw are: Sequestro de Dados e Extorsão Digital. *Revista Eletrônica Direito & TI*, *1*. 2016.

[87] LiskA, Allan; GALLO, Timothy. Ransomw are: defendendo-se da extorsão digital. Novatec Editora, 2019.

[88] Fornasier, Mateus de Oliveira; Spinato, Tiago Protti; Ribeiro, Fernan da Lencina. Ra nso mw are e ciberseg ura nça: a infor maçã o a meaça da por ataques a dados. R evista Thesis Juris, 2020.

sistemas com putacionais.

Esclarece Seisse[89] que "após a liberação do código no sistema, o *ransomware* opera em "silêncio" sem o conhecimento do usuário até que todos os seus componentes para bloqueio de dados sejam instalados. Uma vez finalizada a instalação, uma mensagem (janela ou *pop-up*) informando sobre o bloqueio dos dados e resgate a ser pago para liberação é exibida. A partir desse instante todos os dados do dispositivo se tornam totalmente inacessíveis.". Inclusive, por ele parecer um arquivo comum, os antivírus normalmente utilizados não o detetam, aumentando consideravelmente seu nível de perigo, chegando a um grau alarmante devido à sua abordagem operacional agressiva.

Um dos maiores ciberataques da história foi de *ransomware* e ficou conhecido como *WannaCry*[90], esse ataque afetou organizações no mundo todo. Iniciou em 12 de maio de 2017 afetando, em primeiro momento, 45 mil máquinas em 11 países, e propagou-se nos cinco dias seguintes para mais de 345 mil computadores em mais de 150 países. Esse vírus teve grande e rápida disseminação pelo fato de não necessitar do contato com o usuário final, através de uma verificação (*scanner)* de porta[91], ele vai à procura de máquinas vulneráveis na rede e utiliza *exploits*[92] para infectar as vítimas. Quando infectado, o *ransomware* criptografa os dados do usuário e lança um aviso informando que este não poderá aceder aos seus arquivos, ou sequer fazer *login* no seu computador[93].

Abaixo a mensagem que foi recebida pelas vítimas do ataque:

[89] Cabral Saisse, R.. Ransomware: Sequestro de Dados e Extorsão Digital. *Revista Eletrônica Direito & TI*. 2016.

[90] Gutsalyuk, Mykhaylo V.; KLYMENKO, Olga A. Combate à criminalidade cibernética e garantias de segurança cibernética na Ucrânia. 2017.

[91] Verificação de porta é um método para determinar quais portas de uma rede estão abertas e podem receber e enviar dados. Esse também é um processo para envio de pacotes a portas específicas em um host e análise de respostas para identificar vulnerabilidades. O objetivo por trás da verificação de porta e rede é identificar a organização dos endereços IP, hosts e portas para determinar corretamente as localizações de servidores abertos e vulneráveis, além de diagnosticar seus níveis de segurança. Disponível em: https://www.avast.com/pt-br/business/resources/what-is-port-scanning#pc Acedido em: 15/08/2023

[92] São programas ou códigos projetados para abusar de vulnerabilidades de software ou hardware e causar efeitos indesejados pelos desenvolvedores ou fabricantes. Para melhor entendimento, pense nas falhas de programas como uma fruta no alto de uma árvore, e no exploit como a escada que você usa para alcançar o alimento. Disponível em: https://canaltech.com.br/seguranca/o-que-e-exploit-203850/ Acedido em: 05/08/2023.

[93] Oliveira, Jéssica. Ransomware - Laboratório de Ataque do WannaCry – Brasília, DF, 30 de novembro de 2018



Figura 4 (reproduzida por https://www.avast.com/pt-br/c-wannacry)

Grandes empresas foram afetadas por este *ransomware*, como *FedEx*, *Honda*, *Nissan*, *Santander* na Espanha e o Serviço Nacional de Saúde (NHS) do Reino Unido, que foi forçado a desviar algumas de suas ambulâncias para hospitais alternativos. O valor inicial do "resgate" dos dados era de US$ 300[94] em *bitcoins*, mas a ferramenta ameaçava aumentar o valor caso o pagamento não fosse feito em até duas horas.

Outro ciberataque já mencionado que também impactou empresas mundialmente foi o *NotPetya*, *ransomware* que fez inúmeras vítimas, e foi noticiado pela primeira vez em 27 de Junhode 2017, o ataque interrompeu por semanas os sistemas de tecnologia da informação da companhia dinamarquesa "MAERSK", a maior empresa armadora mundial no transporte de contentores[95]. Isso decorreu poucas semanas após a disseminação do *WannaCry*[96] e chamou atenção pela forma de propagação dos dois *ransomw ares* que eram muito semelhantes, visto que ambos se alastravam através de compartilhamentos de arquivos abertos na rede interna e, dessa forma, os *malwares* se auto copiava m em novos *hosts*[97]. Entretanto, diferente do *WannaCry*, o *NotPetya* não se limitava a encriptar os dados, a intenção dele era destruir os sistemas que

[94] Teixeira, Cleyson Fernando Araújo. Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos. 2021.
[95] Faria, Duarte Lynce de. "O impacto da cibersegurança no quadro jurídico regulatório da segurança marítima". In Janus.net, e-journal of international relations. Vol. 11, Nº 2Consultado [online] em data da última consulta, DOI: https://doi.org/10.26619/1647-7251.11.2.10.2020.
[96] Graça, Douglas Cordeiro da. Souza, Rodrigo Vieira de. Ransomw ares: uma ameaça crescente. 2020.
[97] Host, hospedeiro ou anfitrião, em informática, é qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários ou outros nós na rede

adentrasse[98].

A identificação do ataque se deu quando um grupo de funcionários da empresa, ao acederem os seus computadores, se depararam com um comportamento inusitado neles. Seus ecrãs mostravam mensagens que anunciavam: "Sistemas de ficheiro em C: em reparação" com um aviso para não desligar o computador, ou "Ooops, os seus ficheiros importantes foram encriptados"[99]. Os cibercriminosos exigir 300 doláres para o resgate, porém a encriptação realizada era impossível de ser desfeita, tornando o pagamento inócuo. Abaixo uma das mensagens que eram recebidas:



Figura 5 – (reproduzida por Kaspersky: New Petya / NotPetya / ExPetr ransomware outbreak)[100]

O prejuízo da empresa foi em torno de 300 milhões de doláres [101]. O *ransomware* se aproveitou de uma vulnerabilidade apresentada no W*indows* que a *Microsoft* resolveu após o ocorrido. Por fim, alega-se ainda hoje que o ataque foi proveniente da Rússia e que, supostamente, tinha como alvo primário a Ucrânia, dada a guerra cibernética vivida pelos dois Estados, entretanto empresas do país acusado também foram afetadas pelo ato. A Ucrânia foi a região mais atingida, com 80% das vítimas mundiais do ataque, diversos dos seus serviços tiveram de ser paralisados, como o metro, energia elétrica, e inclusive o sistema de monitoramento do nível de irradiação de Chernobyl, que teve que ser feito manualmente[102]. A partir daí o *NotPetya* acabou se alastrando

[98] Galoyan, Albert. Segurança cibernética no âmbito das relações internacionais. 2019.
[99] Garcia, Bruno. "Informação e Segurança no Ciberespaço: A influência da globalização na intensificação de riscos e ameaças na última década." Public Sciences & Policies 7.1: 193-212. 2021.
[100] https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/
[101] Novet, Jordan. Shipping company Maersk says June cyberattack could cost it up to $300 million. August, 2017. Disponível em: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html . Acedido em: 09.11.2023. [10]
[2] Perlroth, Nicole. Cyberattack Hits Ukraine Then Spreads Internationally. 2017. Disponível em: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html . Acedido em: 10.11.2023

por 155 países, dentre eles, Estados Unidos da América e o continente asiático[103]. O prejuízo total contabilizado foi em torno de 10 bilhões de dólares[104].

O *phishing* é um dos ataques mais utilizados ao redor do mundo[105] e utiliza a tecnologia e a engenharia social para concretizá-lo. As chances de sucesso do criminoso são muito maiores quando consegue conciliar esses dois métodos estrategicamente [106]. A essência do *phishing*, como sugere o termo em inglês, é a tentativa de obter informações confidenciais e pessoais dos indivíduos[107], realizando uma espécie de "pesca" de dados. Isso inclui elementos como o nome de usuário (*username*), senha (*password*) e outros dados de caráter pessoal. Geralmente, tais informações têm relevância financeira ou bancária, com o objetivo principal de utilizar posteriormente esses dados pessoais obtidos de maneira fraudulenta, em benefício dos perpetradores do golpe, acarretando prejuízos para as vítimas[108].

Na maioria dos casos essa tentativa vem através do correio eletrônico com mensagens falsas[109], na qual a denominação real está muito pouco alterada e faz com que a vítima não se aperceba da diferença. Muitas vezes no corpo do *e-mail* há um *link* no qual, ao pressionar, o usuário é encaminhado para um *site* que irá captar seus dados. Conforme Paulo Teixeira[110] "recorrentemente, as mensagens são enviadas para carteiras de milhares de endereços de *e-mail* que foram previamente recolhidos na *internet* das mais variadas formas. A entrega das mensagens normalmente é realizada por computadores que estão sob o controle dos criminosos e incluem, principalmente, servidores *web* com fragilidades de segurança e em alguns casos computadores pessoais infectados com cavalos de troia (*trojans*) propositadamente desenvolvidos para permitir o envio de e-mails em massa (*spam*). As mensagens comportam ficheiros anexos normalmente com designações apelativas, que o recetor descarrega (*download*), nunca concebendo que é um programa malicioso. Noutras circunstâncias, a mensagem redireciona o recetor para um sítio da internet onde é feito o *download* desse mesmo programa. Pensando a vítima, porque para tal foi

[103] Brito, Paulo. Ataque à Ucrânia pode repetir caos global de 2017. 2022. Disponível em: https://www.cisoadvisor.com.br/ataque-a-ucrania-pode-repetir-caos-global-de-2017/ . Acedido em:10.11.2023

[104] Kaspersky. Top 5 most notorious cyberattacks. 2018. Disponível em: https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/ . Acedido em: 10.11.2023

[105] Neves, Raquel Alexandra Carvalho. Vitimação por phishing: um estudo empírico. 2022.

[106] ALSU WAT, Emad S; AL-Otaibi, Abeer F. ; A study on social engineering attacks: phishing attack. International Journal of Recent Advances in Multidisciplinary Research Vol. 07. 2020.

[107] ALENCAR, Gliner; LIMA, Marcelo de; FIRMO, André. O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 9. , 2013, João Pessoa. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2013. p. 254-259. DOI: https://doi.org/10.5753/sbsi.2013.5694.

[108] Teixeira, Paulo Alexandre Gonçalves. O fenómeno do phishing enquadramento jurídico-penal. 2013. Cam̃es - Repositório Institucional da Universidade Autónoma de Lisboa.

[109] Las-casas, Pedro Henrique B., et al. Uma metodologia para identificação adaptativa e caracterização de phishing. In: Proc. of Brazilian Symposium on Computer Networks and Distributed Systems (SBRC). 2016.

[110] Teixeira, Paulo Alexandre Gonçalves. O fenómeno do phishing enquadramento jurídico-penal. 2013. Cam̃es - Repositório Institucional da Universidade Autónoma de Lisboa.

ardilosamente induzida, que está a atualizar a segurança do seu com putador, acaba por estar a torná-lo mais vulnerável.".

O vírus[111] tipicamente se instala na raiz do sistema operacional, predominantemente em ambientes *Windows*, permanecendo inativo até o momento em que o usuário tenta aceder, por exemplo, a página oficial de seu banco. A partir desse ponto, o vírus entra em ação, substituindo o atalho da página do usuário no navegador *web* por um novo endereço. Nessa fase, o usuário será direcionado para um site que visualmente é idêntico ao site original do banco, inclusive exibindo logotipos institucionais. No entanto, os *banners* presentes na página não passam de imagens estáticas, desprovidas de qualquer funcionalidade real, além de imitar a página autêntica do banco. Isso naturalmente dá uma aparência de legitimidade ao *site* acessado. Uma das capacidades funcionais notáveis desse vírus é seu recurso de *Keylogger*, conforme o próprio nome sugere, esse recurso permite que tudo o que o usuário digita no teclado seja registado e armazenado em um arquivo de texto. Isso inclui informações como o nome de usuário e a senha bancária inseridos pela vítima.

Um ataque de *phishing* famoso na história ocorreu em 2016, na eleição presidencial dos Estados Unidos da América[112], em que concorriam Donald Trump e Hilary Clinton. Nesse crime os *crackers* utilizaram a técnica de *spear phishing* para aceder diferentes contas de *e-mail* da equipe da candidata à presidência. Esse ataque é denominado dessa forma, pois foca em um grupo específico de pessoas para atingir seu objetivo. O criminoso teria feito com que um *e-mail* falso se parecesse com um alerta de segurança do *Google* solicitando que o usuário mudasse a senha de sua conta clicando em um *link* que vinha na mensagem. Dois dias depois, todos os *e-mails* haviam sido copiados. O caso é atribuído à Direção Geral do Estado-Maior General das Forças Armadas da Federação Russa (GRU) pelas empresas privadas *Crow dStrike* (2016) *ThreatConnect* (2016), *Alperovitch* (2016) e pelo Departamento de Justiça dos EUA em uma acusação do Grande Júri de julho de 2018. Os *crackers* realizaram a extração de informações confidenciais da campanha e a liberação de milhares de *e-mails* e documentos. No final de julho de 2016, mais de 20.000 e-mails foram disponibilizados por meio da plataforma *online* do *WikiLeaks*[113].

A engenharia social[114] é o termo utilizado para descrever a estratégia de ataque em que o invasor utiliza a persuasão, frequentemente explorando a inocência ou a confiança do usuário,

[111] Faria, Thiago Stefanini. Técnica phishing: simples, mas eficaz. 2017.
[112] Oliveira, Raquel. Eduardo, Izycki. Propaganda computacional na prática: os casos de Estados Unidos, França e Venezuela. 2021.
[113] WikiLeaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página, postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis.
[114] Mitnick, Kevin e Simon, William L. A Arte de Enganar. São Paulo: Blucher, 2003.

com o objetivo de adquirir informações que possam ser posteriormente empregues para obter acesso não autorizado a sistemas computacionais, dispositivos ou dados confidenciais. Dessa forma, o engenheiro social pode aproveitar-se das pessoas para obter as informações que deseja com ou sem o uso da tecnologia. Mitnick explica que "na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente — os traços sociais necessários para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a praticamente qualquer informação - alvo usando as estratégias e táticas da sua habilidade. Os tecnologistas experientes têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim deixaram de fora a vulnerabilidade mais significativa: o fator humano. Apesar do nosso intelecto, nós humanos — você, eu e todas as outras pessoas — continuamos sendo a ameaça mais séria à segurança do outro". Um caso emblemático de cibercrime com o uso de engenharia social aconteceu com o fabricante japonês de componentes automotivos, *Toyota Boshoku Corporation*. Cibrcriminosos utilizaram de suas habilidades de persuasão, através de *e-mails*, para convencer um executivo do departamento financeiro a alterar os dados da conta bancária da empresa em uma transferência de fundos. O dinheiro perdido foi de 37 milhões de dólares[115].

Os ataques *Denial-of-Service* (DoS) e o *Distributed Denial-of-Service* (DDoS)[116] já mencionados nesse estudo, também fazem parte dos ciberataques mais utilizados atualmente. O *Denial-of-Service* (negação de serviço) tem como objetivo tornar um computador ou uma rede de computadores incapazes de prover o serviço normal. Já o *Distributed Denial-of-Service* (negação distribuída de serviço) emprega um número substancial de computadores para engendrar um ataque *DoS* direcionado a um ou vários alvos. Por meio da aplicação da abordagem Cliente/Servidor, o infrator consegue amplificar de forma considerável a eficácia do ataque *DoS*, ao reunir os recursos de numerosos computadores colaborativos, que agem como plataforma de ataque, muitas vezes sem o conhecimento ou consentimento de seus proprietários. De maneira característica, um *software* mestre de ataque Distribuído de Negação de Serviço (*DDoS*) é implantado em um computador, normalmente após a obtenção indevida de uma senha. O *software* mestre, em um horário predeterminado, estabelece comunicação com os *softwares* agentes, previamente instalados em diversos sistemas na *Internet*. Os agentes, ao receberem a instrução

[115] IP Telecom. Disponível em: https://www.iptelecom.pt/sites/default/files/inline-files/20210524_IPT-Webinar-EngSocial_v1.pdf . Acedido em: 10.11.2023

[116] Neira, Anderson Bergamini; KANTARCI, Burak; NOGUEIRA, Michele. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks, 2023

correspondente, dão início ao ataque. Através da aplicação da arquitetura Cliente/Servidor, o programa mestre tem a capacidade de acionar centenas ou mesmo milhares de programas agentes em questão de segundos.

Outro ataque importante a ser mencionado é a *ciberespionagem* que é uma prática na qual indivíduos, grupos ou entidades, muitas vezes com motivações políticas, econômicas ou militares, utilizam tecnologias e técnicas cibernéticas para obter informações confidenciais ou sensíveis de governos, organizações, empresas ou indivíduos. Essa atividade envolve o acesso não autorizado a sistemas, redes e dispositivos para coletar dados, como segredos comerciais, informações estratégicas, dados pessoais ou dados de inteligência. A ciberespionagem pode ser conduzida por governos, agentes estatais, grupos criminosos ou *crackers* independentes, e as informações obtidas podem ser usadas para ganhos financeiros, vantagens competitivas ou para influenciar cenários políticos.

2. Crimes relacionados ao Setor Bancário, análise da regulamentação, e seus efeitos jurídicos

2.1. Crimes cibernéticos que afetam os Bancos e a Lei do Cibercrime

Em relatório publicado em junho de 2022 sobre cibersegurança em Portugal realizado pelo Centro Nacional de Cibersegurança constatou-se através de análise dos setores e áreas governativas mais atingidos pelos incidentes de cibersegurança que, tal como em anos anteriores, a Banca continua sendo o setor mais afetado por ciberataques, com 13% dos incidentes registados, com uma subida absoluta de 79% relativamente ao ano de 2021.

2020				2021				Ordenação	
RK	Setor e Área Governativa[3]	Nº	%	RK	Setor e Área Governativa	Nº	%	Tendência absoluta %	Lugar RK
1º	Outros	626	36	1º	Outros	1220	39	+ 95	=
2º	Banca	229	13	2º	Banca	411	13	+ 79	=
3º	Infraestruturas Digitais	184	11	3º	Presidência do Conselho de Ministros	270	9	+ 559	+
4º	Prestadores de Serviços de Internet	161	9	4º	Infraestruturas Digitais	266	8	+ 45	-
5º	Educação e Ciência, Tecnologia e Ensino Superior	154	9	5º	Prestadores de Serviços de Internet	187	6	+ 16	-
6º	Transportes	79	5	6º	Administração Interna	181	6	+ 1408	+
7º	Administração Local	41	2	7º	Transportes	133	4	+ 68	-
8º	Presidência do Conselho de Ministros	41	2	8º	Administração Local	120	4	+ 193	-
9º	Energia	30	2	9º	Educação, Ciência, Tecnologia e Ensino Superior	109	3	- 29	-
10º	Saúde	29	2	10º	Saúde	63	2	+ 117	=
11º	Administração Regional	20	1	11º	Energia	31	1	+ 3	-
12º	Defesa Nacional	19	1	12º	Cultura e Turismo	26	1	+ 53	+
13º	Cultura e Turismo	17	1	13º	Finanças	20	1	+ 122	+
14º	Trabalho, Solidariedade e Segurança Social	17	1	14º	Defesa Nacional	19	1	=	-
15º	Negócios Estrangeiros	12	1	15º	Negócios Estrangeiros	18	1	+ 50	=

Figura 5 – (reproduzida por Relatório "Riscos & Conflitos 2023", do Observatório de Cibersegurança do CNCS)

Os ataques/crimes que têm maior taxa de incidência no setor bancário são o roubo de identidade, *phishing*, *vishing*, *malware*, fraude automática em banco *online*, engenharia social, *DOS* e DDoS[117]. No roubo de identidade, os criminosos utilizam dados de outra pessoa, como nome, data de aniversário e endereço, para atividade fraudulenta, e é essa uma das técnicas mais utilizadas, através das máquinas de pessoas físicas que são utilizadores dos bancos *online*, captam os seus dados. Eles utilizam essas informações para abrir novas contas, pedir empréstimos, entre outras atividades bancárias. O *vishing* é uma espécie de *phishing* no qual o cibercriminoso utiliza uma *VOIP* (*voice over IP* - método que permite realizar e receber chamadas através da *internet*) para se fazer passar por um funcionário do banco que precisa confirmar dados bancários por questões de rotina de segurança e, assim, descobrir informações confidenciais do usuário, normalmente o número da vítima é desvendado através de um *e-mail* de *phishing*.

Os atos criminosos cometidos ou potencializados por meio digital, através do uso da *internet* ou de sistemas de computação, podem violar várias categorias de interesses jurídicos, incluindo os direitos das pessoas (como a vida, a honra, a liberdade individual, etc.) e do patrimônio (tanto material quanto imaterial). Em Portugal foi promulgada em 17 de agosto de

[117] K., Dr. U ma mahesw ari, Impacts of Cyber Cri me on Internet Ba nking (Marc h 5, 2021). International Jour nal of En gineering Tec hn ology and Mana ge ment Sciences, Available at SSRN: https://ssr n. co m/a bstract= 39 395 79 or http://dx. doi. org/1 0. 213 9/ssrn. 39 39 579

1991 a Lei 109/91, conhecida como Lei da Criminalidade Informática, que aborda de maneira abrangente os aspetos criminais ocorridos no ambiente digital, assegurando os direitos estabelecidos na Constituição da República Portuguesa (CRP). Esta lei detalha seis categorias de delitos relacionados à informática: a falsidade informática (art. 4º), o prejuízo relacionado a dados ou programas informáticos (art. 5º), a sabotagem informática (art, 6º), o acesso ilegítimo (art. 7º), a intercetação ilícita (art. 8º) e a reprodução indevida de programas protegidos (art. 9º). Posteriormente, com a adesão e subsequente ratificação da Convenção de Budapeste[118], Portugal reviu a sua legislação sobre a criminalidade informática para incorporar todos os requisitos estabelecidos na Convenção. Assim, em 15 de setembro de 2009, foi aprovada a Lei nº 109/2009, também conhecida como a Lei do Cibercrime.

A lei do Cibercrime segue a construção dos tipos incriminadores e obedece à verificaçãode um conjunto de elementos, conforme ensina Figueiredo Dias[119] "os que dizem respeito ao *autor*; os relativos à *conduta*; e os relativos ao *bem jurídico*. Com efeito, todos os tipos incriminadores devem, na sua revelação objectiva, precisar quem pode ser autor do respectivo tipo de crime, qual a conduta em que este se consubstancia; e, na medida possível, dar indicação, explícita ou implícita, mas sempre clara do(s) bem(ns) jurídico(s) tutelado(s)". Ou seja, para constatar a existência de um crime, primeiro é necessário verificar se estão presentes os elementos objetivos do tipo e após devesse constatar a presença do elemento subjetivo do tipo.

Já o tipo subjetivo de ilícito se refere ao dolo, que consiste no conhecimento e vontade de realização do tipo objetivo de ilícito. Sendo punível apenas os factos praticados com dolo, ou, em casos previstos na lei, com negligência[120].

Na falta de previsão específica da punição da negligência nos crimes da Lei do Cibercrime, o preenchimento dos tipos de ilícito dela implica que o ato praticado será decorrente de um dos três tipos de dolo constantes no Art. 14º do Código Penal Português[121]. Esse artigo estabelece o elemento subjetivo deles, que são[122]:

a) Dolo direto intencional ou de primeiro grau (nº 1), em que o agente atua com a

[118] A Convenção de Budapeste, de 21 de novembro de 2001, foi o primeiro trabalho internacional sobre crime no ciberespaço, tendo surgido devido ao novo panorama internacional e aos novos paradigmas enfrentados. Essa Convenção foi criada pelo Conselho da Europa , Estados U nidos, Canadá, Japão e África do Sul. Em j unho de 2021, contam-se 66 países nos quais o tratado está vigente,sendo um deles, Portugal, além de 11 observado res, e co m a estimativa de que 1 58 países o utilizaram co mo orientação para suas legislaçõ es nacionais. (https://www.coe.int/en/web/cybercrime/the-budapest-convention)

[119] Figueiredo Dias, Jorge. Direito Penal, Parte Geral, Tomo I, Coimbra editora, 2004.

[120] Figueiredo Dias, Jorge. Direito Penal, Parte Geral, Tomo I, Coimbra editora, 2004.

[121] Código Penal. DL n.º 48/95, de 15 de Março. Disponível em: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis&so_miolo=

[122] Ventura, André. Noções de Direito Penal. 1ª ed. 2013.

intenção de realizar o facto típico;

b) Dolo direto necessário ou de segundo grau (nº 2), em que o agente aceita a realização dos elementos do tipo objetivo como consequência necessária da sua conduta; e

c) Dolo eventual (nº 3) caracteriza-se pela circunstância de "a realização do tipo objectivo de ilícito ser representada pelo agente apenas "como consequência possível da conduta""[123], ele está disposto a aceitar a realização e o elemento volitivo do dolo do tipo se considera verificado, ou seja, se apresenta num estado de conformação pela realização do resultado previsto como possível.

Aos elementos intelectual e volitivo acresce um elemento emocional que é dado pela consciência da ilicitude[124], ou seja, "uma qualquer posição ou atitude de contrariedade ou indiferença face às proibições ou imposições jurídicas (…) quando o agente revela no facto uma posição ou uma atitude de contrariedade ou indiferença perante o dever-ser jurídico-penal"[125].

Dessa forma, é necessário que a conduta seja praticada com dolo, por uma pessoa singular ou, nos termos do disposto no art. 9º da Lei do Cibercrime, uma pessoa coletiva ou entidades equiparadas. Prescreve que "as pessoas coletivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal". Conforme Duarte Nunes "a previsão da possibilidade de responsabilizar criminalmente os entes coletivos assenta na consciencialização do legislador para a existência de uma criminalidade organizada, empresarial (porque praticada no âmbito das empresas, no interesse em nome destas), económica e transacional".

O artigo 3º da Lei do Cibercrime define o crime de falsidade informática e dispõe:

"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.

[123] Figueiredo Dias, Jorge. Direito Penal, Parte Geral, Tomo I, Coimbra editora, 2017.
[124] Figueiredo Dias, Jorge. Jornadas de Direito Criminal, Fase I, ed. Do Centro de Estudos Judiciários, 1983.
[125] Figueiredo Dias, Jorge. Direito Penal, Parte Geral, Tomo I, Coimbra editora, 2004.

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 núm ero 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."

O elemento objetivo do crime de falsidade informática está previsto no texto legal através dos elementos "quem (…) introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos". Assim, para verificação do tipo objetivo deste ilícito criminal é necessário que exista um resultado, ou seja, os dados informáticos têm de ser alterados com o propósito de desvirtuar a demonstração dos factos que com aqueles dados podem ser comprovados. Já o elemento subjetivo do crime diz respeito a um resultado com a "intenção de provocar engano nas relações jurídicas"[126]. Dessa forma, pode-se perceber que a lei, nesse caso, exige o dolo direto, que poderá ser dolo direto intencional ou dolo direto necessário.

O nº 3 do artigo da falsidade informática determina que é suficiente que o agente utilize um documento gerado a partir de informações digitais e aja com a intenção de prejudicar outra pessoa ou obter um benefício ilegítimo, seja para si próprio ou para terceiros. Não é necessário que o engano resultante tenha impacto nas relações jurídicas, conforme estabelecido no primeiro nº1 desse artigo[127].

[126] Venâncio, Pedro Dias. Lei do Cibercrime - Anotada e Comentada. 1ª ed. 2011.
[127] Ribeiro, Maria da Conceição Fernandes. Cibercrime e prova digital. 2015.

O bem jurídico[128] tutelado pelo crime de falsidade informática é a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório[129] (inclusive a segurança nas transações bancárias), tutelando, também a integridade dos sistemas informáticos, visto que esse crime se assemelha ao crime de falsificação, contante no artigo 256º do Código Penal[130], apenas se diferenciando por efetuar-se digitalmente. Levando-se em consideração a letra da lei que exige a intenção de "provocar engano nas relações jurídicas", seja um terceiro alterando dados do sistema, ou o próprio detentor dos dados que os manipula para enganar outras pessoas, ficando claro que o legislador queria proteger as informações que lá constam, assim como no crime de falsificação[131].

Este delito é um crime público, bastando a notícia da prática do crime (pelas autoridades judiciárias ou policias) ou a denúncia facultativa de qualquer pessoa para que se dê início ao procedimento penal.

Nesse artigo frequentemente são enquadrados os ataques de *phishing*, que normalmente são realizados através de um *e-mail* supostamente enviado pela entidade bancária, no qual a vítima fornece os seus dados em um *site* falso que aparenta ser do banco, assim como o *vishing* que envolve a obtenção de informações sensíveis através de chamadas telefônicas.

Já o artigo 4º que dispõe sobre o dano relativo a programas ou outros dados informáticos estipula que:

"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,

[128] José de Faria Costa explica que o bem jurídico é "o que é fundamental prende-se, não com a específica situação determinada no tipo legal de crime, mas antes com a relação da pessoa com o próprio objecto de valoração", ou seja, é aquilo que norteia a própria criação da norma jurídica. - Noções fundamentais de direito penal - 4ª ed. 2015.

[129] Nunes, Duarte Alberto Rodrigues. O crime de falsidade informática. Revista Julgar. Outubro 2017.

[130] https://w ww. pgdlisboa. pt/leis/lei_mostra_articulado. php? nid= 109&tabela=leis

[131] Nunes, Duarte Alberto Rodrigues. "O crime de falsidade informática". Revista Julgar. Outubro 2017.

programas ou outros dados informáticos destinados a produzir as ações 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 nºs 1, 2 e 4 o procedimento penal depende de queixa."

Os elementos objetivos desse crime estão presentes no nº1 deste artigo, e é constituído pela ação legítima de "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 afetar a capacidade de uso" e com a "ausência de permissão legal ou autorização do proprietário, do titular do direito do sistema ou de parte dele". Não possui dolo específico, basta que de forma ilegítima alguém modifique dados ou programas informáticos de forma a interferir no seu uso original para que preencha a conduta do tipo objetivo do crime[132].

No nº 2 desse artigo está previsto que a tentativa é punível, ou seja, não é necessário que o crime chegue a se consumar.

A modalidade do crime prevista no nº 3 do artigo 4º tem como elementos objetivos:

a) quem 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 ações não autorizadas no n.º 1;

b) que esse resultado seja realizado de forma ilegítima, ou seja, sem ser o seu proprietário ou sem apresentar permissão ou autorização para o efeito;

Aqui o legislador pretende punir o cibercriminoso que vislumbra a disseminação de *malware* para assim cometer o descrito no nº1. Esse fato é punível mesmo que não produza efeitos, ou seja, o sistema pode não ser prejudicado, o cibercriminoso pode não ter nenhum benefício, o simples fato de espalhar um *malware* já pode ser punido. O crime precisa ser cometido sem permissão ou autorização, dessa forma não é possível criminalizar, por exemplo, os *hackers*

[132] Rodrigues, Benjamim Silva. "Direito Penal – Parte Especial I, Direito Penal Informático-Digital" Coimbra. 2009.

que são contratados por empresas para executar o que está descrito no nº 3, já que fazem isso com autorização para realizar testes de segurança [133]. Ademais, o bem jurídico protegido nesse artigo é a integridade dos dados ou programas informáticos.

Vale referir que os atos ilícitos práticos nos termos dos nºs 1, 2 e 4 deste artigo são crimes semipúblicos o que implica que o procedimento penal depende de queixa. No tocante aos atos ilícitos praticados nos nºs 3 e 5 a lei classifica como crime público[134].

Os ataques de *DoS* e *DDos* se enquadram claramente nesse artigo, visto que o seu objetivo de sobrecarregar os servidores ou deixá-los inativos se enquadra diretamente com o tipo penal em questão.

O artigo 5º descreve o crime de sabotagem informática e dispõe o que se segue:

"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

[133] Verdelho, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes. 2010.
[134] Ribeiro, Maria da Conceição Fernandes. Cibercrime e prova digital. 2015.

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."

Os elementos objetivos constitutivos do crime de sabotagem, na modalidade prevista no n.º 1 do artigo 5.º, são "quem sem permissão legal ou sem para tanto estar autorizado (…), entravar, impedir, ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento ou impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático". Não se exige especial intenção, apenas que o criminoso interfira no sistema informático. O elemento subjetivo desse crime apenas dispõe que ele atue intencionalmente e racionalmente na prática do ato, sem necessidade de especial motivação, e desde que não seja autorizado a atuar.

No seu n.º 2, pune-se igualmente, "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 ações não autorizadas descritas no número anterior". Aqui pretende-se punir a difusão de *malwares* que permitem a criação de redes ilegais para controle nocivo das delas[135] como a disseminação de vírus, *worms*[136], cavalo de Tróia[137], entre outros.

Faz-se importante referir que a conduta prevista no n.º 2 do artigo 5.º que consistente em "introduzir" em sistema informático (…) já está punida pelo n.º 1 do mesmo artigo, considerando a doutrina que a sua inserção no n.º 2 se deve a erro do legislador[138].

A Lei do Cibercrime, no elemento subjetivo do crime, deixou de exigir dolo específico (intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância)[139], pelo que bastará a prática do ato delituoso em qualquer uma das vertentes

[135] Verdelho, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes. 2010.

[136] "Verme (Worms): é um código mal intencionado autopropagável de um computador para outro, por meio da rede. A ação nociva pode ocorrer pelo consumo de recursos da rede ou do sistema local, podendo causar um ataque de negação de serviço. Alguns vermes podem ser executados, espalhando-se sem que o usuário perceba, enquanto outros precisam que o usuário execute o verme, para que este se espalhe. Além de se replicar, o verme pode entregar u ma carga", vale mencionar que o *malware* w orms se propaga mais rapidame nte que os outros tipos de *malwares*. - Damatto, Felipe César; Rall, Ricardo. "Estudo dos possíveis motivos do aumento de incidentes de *malwares* nas empresas." tekhne e logos, 2011.

[137] "É um programa que parece ser útil ou inofensivo, porém tem códigos ocultos criados para explorar ou danificar o sistema no qual foi executado. Geralmente os cavalos de tróia chegam através de mensagens de e -mail. U m cavalo de tróia pode interromper o trabalho do usuário, operações normais do sistema, podem abrir uma porta dos fundos no sistema para que um hacker invada o sistema, roube dados ou altere configurações". - Damatto, Felipe César; Rall, Ricardo. "Estudo dos possíveis motivos do aumento de incidentes de *malwares* nas empresas." tekhne e logos, 2011.

[138] Dias Venâncio, Pedro, Lei do Cibercrime Anotada e Comentada, Coimbra Editora, 2011.

[139] Dias Venâncio, Pedro, Lei do Cibercrime Anotada e Comentada, Coimbra Editora, 2011.

do dolo.

Relativamente ao bem jurídico tutelado pelo crime de sabotagem informática é a segurança dos sistemas e comunicações eletrónicas em seu normal funcionamento[140], ou seja, a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos. E é um crime classificado como crime público.

Com o exemplo de enquadramento nesse artigo tem-se a situação em que o *ransomware* criptografa os dados de um banco, incluindo registos de transações e informações de contas de clientes e exigem um pagamento em criptomoedas para descriptografar os dados e evitar a perda das informações.

Já o artigo 6º da lei estabelece o crime de acesso ilegítimo e determina que:

"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 outr a 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 ações 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

[140] Simas, Diana Viveiros. O cibercrime. Dissertação de Mestrado, Universidade Lusófona de Humanidades e Tecnologias., Direito, Lisboa. 2014.

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 nºs 2 e 3.

7 - Nos casos previstos nos nºs 1, 4 e 6 o procedimento penal depende de queixa."

O tipo objetivo do crime de acesso ilegítimo previsto é determinado por "qualquer acesso a um sistema informático" e a "ausência de permissão legal ou ausência de autorização do respetivo proprietário, ou por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático" ou seja, para o cometimento do crime basta que o criminoso adentre em todo ou em parte de um sistema informático (*harware*, componentes, dados armazenados no sistema instalado, diretorias, dados de tráfego e dados relativos ao conteúdo) sem autorização para isso[141].

Enaltecendo que a intenção de causar um prejuízo não integra qualquer dos elementos do tipo deste crime, o crime cons uma-se com a concretização, por qualquer modo, de acesso a sistemas informáticos. Conforme Pedro Simões Dias[142] "es se é um crime informático técnico que tem verdadeira expressão quando praticado através de uma infraestrutura técnica. Neste sentido, é um crime volátil, praticado à distância". Se enquadram nesse artigo os casos em que alguém obtém acesso não autorizado a uma conta bancária *online*, por exemplo, usando credenciais roubadas.

As penas serão mais graves se tiver havido violação de regras de segurança, se tiver por objeto um qualquer meio eletrónico de pagamento, se se tomar conhecimento de segredo comercial ou industrial, ou de dados confidenciais, e ainda se o benefício ou vantagem patrimonial forem de valor consideravelmente elevado (n.º 3, n.º 4 e n.º 5 do artigo 6.º da Lei do Cibercrime).

[141] Verdelho, Pedro. "A nova Lei do Cibercri me", Lei n.º 10 9/2 00 9. 2010.
[142] Dias, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito, in Direito da Sociedade da Informação, vol. VIII. Coimbra Editora, 2009.

Quanto ao elemento subjetivo do crime em questão apenas se exige o dolo genérico, como resulta da expressão "sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele", não exigindo atualmente e ao contrário de versões anteriores desta norma jurídica, qualquer intenção específica, por exemplo a de causar prejuízo ou a de obter qualquer benefício ilegítimo.

Relativamente ao bem jurídico tutelado pelo crime de acesso ilegítimo, não é o património, nem a vida privada do lesado, mas sim a segurança dos sistemas informáticos[143].

Por fim, os atos ilícitos práticos nos termos dos nºs 1, 4 e 6 deste artigo, são crimes semipúblicos. E no que concerne aos ilícitos dos nºs 2, 3 e 5 a lei classifica como crime público.

Os crimes elencados acima são os mais relevantes para as entidades bancárias, pois são os que possuem grande incidência nesse âmbito. Entretanto a lei possui mais dois artigos, menos importantes para esse estudo, mas que merecem ser referidos: o artigo 7º que tipifica a intercetação ilegítima que se caracteriza pelo ato de intercetar comunicações eletrônicas, como *e-mails* ou mensagens, sem consentimento, com a finalidade de divulgação dessas informações; e o artigo 8º que expõe a reprodução ilegítima de programa protegido que ocorre quando há reprodução não autorizada de programas de computador protegidos por direitos autorais, violando os direitos de propriedade intelectual. No contexto bancário, isso pode ocorrer quando alguém copia e distribui um *software* bancário protegido sem a devida autorização. Também pode envolver a manipulação de programas de computador usados para realizar transações financeiras.

A Lei do Cibercrime é uma lei inovadora e supriu uma lacuna no ordenamento jurídico português frente a esse tema, entretanto, apesar de ter sido uma grande evolução em matéria de crime cibernético, ainda precisa se desenvolver muito[144]. A lei possui uma grande abrangência quanto as infrações que são punidas, o que dá a ela importante relevância, e, apesar da natureza complexa e instável que esses crimes possuem, a lei conseguiu ampliar e agilizar as formas de investigação, permitindo maior eficácia na sua implementação e punibilidade dos fatos criminosos.

Ainda assim as medidas não são suficientes para o combate do crime cibernético. Uma das dificuldades latentes dessa lei é a punição dos cibercriminosos, visto que para isso acontecer

[143] Dias, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito, in Direito da Sociedade da Informação, vol. VIII. Coimbra Editora, 2009.
[144] Cancela, Alberto Gil Lima. A prova digital: os meios de obtenção de prova na lei do cibercrime. Diss. Universidade de Coimbra (Portugal), 2016.

é necessário que haja a cooperação entre os países, já que nesse novo formato de crimes não existem fronteiras definidas, eles são transnacionais[145]. A dimensão transfronteiriça dos crimes cibernéticos dificulta a prevenção, a investigação, a repressão e a cooperação das autoridades competentes. A existência de divergências e lacunas entre as legislações nacionais, limitações técnicas e operacionais, conflitos de jurisdição e soberania, questões de direitos humanos e privacidade, e a constante evolução das tecnologias e das modalidades criminosas não conseguem ser ultrapassadas por essa lei. Os criminosos podem estar em qualquer parte do mundo, assim como as suas vítimas. Dessa forma, a resposta a esses crimes precisa ser internacional, dinâmica, rápida e conjunta, a União Europeia vem buscando harmonizar as medidas[146] tomadas pelos estados-membros, entretanto elas não têm tido a harmonia necessária para eficácia desse combate.

2.2. Políticas de Segurança Cibernética no Setor Bancário

Para evitar a ocorrência de cibercrime diversas medidas tiveram que ser tomadas por parte das entidades governamentais e do setor bancário. A política de segurança implica um conjunto de diretrizes que devem ser adotadas pelos utilizadores das instalações de uma organização. Ela deve, portanto, ser apresentada de maneira clara e precisa, estabelecendo as esferas de responsabilidade dos usuários, da equipa de administração de sistemas e redes, bem como da direção. Além disso, viabiliza a incorporação de ferramentas e métodos de segurança, técnicas de auditoria e estabelece uma base para procedimentos legais em caso de incidentes[147]. Existem duas políticas de segurança utilizadas pelas empresas que objetivam evitar as ameaças. A primeira denomina-se política de segurança física, que como já foi descrito, diz respeito à segurança da informação, que versa sobre a implementação de meios físicos seguros para acomodar os sistemas e equipamentos informáticos. É importante evitar a ocorrência de ataques físico, que podem ocasionar o roubo ou o dano de máquinas, instalação de *malwares*, ou, inclusive, deixar aberta uma porta de acesso remoto.

A política de segurança física tem a intenção de proteger os sistemas contra essas ameaças internas ou externas que podem comprometer a integridade, confidencialidade ou

[145] AGUILAR, Amanda Albuquerque. Responsabilidade civil dos bancos nos casos de danos e fraudes causados por hackers. Manaus: UEA, 2017.

[146] Como exemplo dessas medidas tem-se a Diretiva NIS; a criação do centro europeu especializado em cibercriminalidade (EC3 EU), no quadro da Euro pol, que aj uda os estados- me mbros a investigare m os cibercrimes e a des ma ntelar redes crimin osos; a ENIS A, Agência Euro peia de Cibersegurança;

[147] Estrada, Manuel Martin Pino . Internet Banking no Brasil, na A mérica Latina e na Euro pa. Dispo nível em http://www.publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161. Acedido em 10/8/2023

disponibilidade deles[148]. Dentre as medidas que elas executam estão o cuidado com o local em que se encontram os *hardwares*, para que não sejam de fácil acesso, realização do controlo do acesso das pessoas, mantendo uma vigilância ativa e permanente, utilização sistemas de proteção contra catástrofes naturais e combate à falta de energia elétrica, com sistemas subsidiários no caso de falha na eletricidade.

O controlo do acesso consiste em restringir que indivíduos acedam a locais físicos sem autorização. Esse controlo pode ser realizado de diversas formas como através de fechaduras seguras nas portas, cartões para acesso, senhas, biometria ou reconhecimento facial. Impedindo, dessa forma, que pessoas não autorizadas tenham acesso aos recursos informáticos [149]. Já a vigilância ativa é feita com a monitoria constante dos espaços físicos onde se encontram os equipamentos informáticos, através do uso de câmeras, sensores de presença, alarmes ou guardas de segurança, podendo utilizá-los de forma combinada. Essas medidas devem ser constantemente verificadas para garantir que estão em pleno funcionamento.

A segunda denomina-se política de segurança lógica que abrange a proteção dos bancos de dados contra ameaças de *software* malicioso, levando em consideração o armazenamento e a preservação dos arquivos, a gestão de riscos e outros elementos pertinentes. Para implementar tais políticas, empregam-se métodos como certificação digital, criptografia e *firewall* (será melhor explicado a seguir)[150]. Ou seja, a política de segurança lógica consiste em proteger o ambiente tecnológico, diferentemente da política de segurança física, que busca resguardar o estabelecimento.

As políticas físicas de cibersegurança desempenham um papel vital na segurança cibernética, atuando em conjunto com as medidas lógicas para proteger sistemas e aplicações informáticas. Uma política física de cibersegurança eficaz tem o poder de evitar ou reduzir os efeitos de incidentes como incêndios, inundações, cortes de energia, ataques terroristas, espionagem industrial ou um simples funcionário mal-intencionado.

As políticas físicas e lógicas de cibersegurança são complementares e devem ser aplicadas de forma integrada.

2.3. Regulamentação de Segurança Cibernética aplicada ao Setor Bancário Europeu

148 Integrity Newsletter Cibersegurança. A importância da Segurança Física. 2022. Disponível em: https://w ww.i ntegrity. pt/pt/newsletters/2022/segura nca - fisica.html#:~:text=A%20estrutura%20de%20seguran%C3%A7a%20f%C3%ADsica%20%C3%A9%20composta%20por, melhorado%20e%20mantido.%201.%20Defini%C3%A7%C3%A3o%20de%20Seguran%C3%A7a%20F%C3%ADsica . Acedido em: 10.11.2023.

149 Matos, Pedro Carvalhais de Abreu. Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas. 2018.

150 Leite, Monteiro Luciano. Políticas de segurança física e lógica de tecnologia da informação em redes de computadores e seus ativos. 2018.

Estar em conformidade com as leis e os regulamentos é um dos principais objetivos de um programa de segurança da informação. Existem inúmeras regulamentações voltadas para a cibersegurança, em diversos níveis de governança, desde exigência internacionais, nacionais, estaduais e locais.

A regulamentação voltada à cibersegurança para os bancos cresceu rapidamente visto a grande relevância de manter a segurança neste setor [151]. O Banco Central Europeu criou diversas iniciativas regulatórias e a Autoridade Bancária Europeia comunicou orientações a serem cumpridas por eles, fazendo com que eles adotassem medidas de controle mais cedo que a maioria dos setores[152].

A Convenção de Budapeste que deu origem à Lei de Cibercrime em Portugal, já mencionada neste estudo, originou uma série de diretrizes relacionadas ao tema, visto que a União Europeia (UE) foi encorajada a tomar certas medidas. Em 2004 surgiu a Agência Europeia para a Segurança das Redes e da Informação (ENISA)[153], que foi reforçada após a Convenção de Budapeste, ela desempenha um papel fundamental na coordenação e fortalecimento das capacidades de cibersegurança da UE. A criação dela se deu devido ao aumento de ciberataques que causaram dano económico substancial que causou a consequente diminuição da confiança no mercado[154]. A sua missão é alcançar um elevado nível comum de cibersegurança em toda a Europa[155]. Conforme o *site* da União Europeia explica, "A ENISA trabalha com organizações e empresas para aumentar a confiança na economia digital, reforçar a resiliência das infraestruturas da UE e, em última análise, manter os cidadãos da UE seguros no plano digital. Fá-lo através da partilha de conhecimentos, do desenvolvimento do pessoal e das estruturas, bem como da sensibilização. O Regulamento Cibersegurança da UE reforçou o trabalho da agência[156]". Seu trabalho abrange desde a sensibilização sobre ameaças cibernéticas até a análise de riscos e a coordenação de respostas a incidentes.

Outra importante função da ENISA é realizar *ciber* exercícios/treinamentos a cada dois

[151] Khatri, Prem. The importance of cyber security in banking. 2019. Disponível em: https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/ . Acedido em: 25.09.2023.

[152] Fernandes, Filipe S.. Cibersegurança é tema na gestão de topo. 2020. Disponível em: https://www.jornaldenegocios.pt/negocios-iniciativas/banca-do-futuro/detalhe/cibersegurança-e-tema-na-gestao-de-topo . Acedido em: 25.09.2023.

[153] Leite, Ana Marta Xavier Ferreira. A problemática da cibersegurança e os seus desafios. CEDIS Working Papers. Direito, Segurança e Democracia. ISSN 2184-0776. Nº 49. 2016.

[154] Christou, George. The collective securitisation of cyberspace in the European Union. West European Politics. 2019.

[155] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pt

[156] Agência da União Europeia para a Cibersegurança (ENISA) Disponível em: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pt . Acedido em: 20.09.2023.

anos em setores críticos da sociedade em relação à cibersegurança, são denominados *Cyber Europe programme*. Esses exercícios simulam um cenário de crise, ou seja, um ciberataque, e os envolvidos devem o analisar e o repelir. Participam dele tanto entidades do setor público como do privado, assim como profissionais especializados em tecnologia da informação, como em desenvolvimento. Após a realização do treinamento a ENISA emite um relatório com a descrição de como ele se desenvolveu e o que foi concluído. Esses testes permitem que as entidades e profissionais se aprimorem baseados em uma simulação da realidade, descobrindo suas falhas e seus acertos.

O *e-banking* (banco virtual) foi o cenário sensível escolhido em 2012 para o treinamento. Nele foi utilizado um ataque de *DDoS*, já explicado ao longo desse estudo, a serviços eletrónicos públicos. Mais de quinhentas pessoas de trezentas e trinta e nove entidades participaram no evento, incluindo 25 países, dentre eles Portugal, e institutos da União Europeia. As recomendações da ENISA foram que esse setor deve continuar se desenvolvendo e que mais testes devem ser realizados[157].

Em 2019 surgiu o regulamento nº 2019/881 do Parlamento Europeu e do Conselho de 17 de abril que atualizou o funcionamento da ENISA e regulamentou a certificação da cibersegurança das tecnologias da informação e comunicação, também revogou o Regulamento da UE nº 526/2013 sobre cibersegurança. Essa atualização melhorou a tarefa de consciencializar a UE da relevância da cibersegurança e transformou a ENISA numa agência permanente[158]. Segundo o relatório de ética e direito[159], esse é um dos três[160] atores mais importantes em matéria de cibersegurança na União Europeia e tem como atribuições "a contribuição para a elaboração e a execução da política e do Direito da União em matéria de cibersegurança; a prestação de assistência para reforço das capacidades dos Estados Membros e das instituições e organismos da UE; o apoio à cooperação operacional entre Estados Membros, instituições da UE e outras partes interessadas; o apoio à elaboração e execução da política da União em matéria de certificação da cibersegurança dos produtos, serviços e processos de TIC; a produção de conhecimento e informação; a organização de campanhas de sensibilização e educação; a contribuição para a agenda estratégica da investigação e inovação ao nível da UE no domínio da

[157] Relatório da ENISA. https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme/cyber-europe-2012 . 2012.
[158] Serrano, Inês Isabel Baião. Cibersegurança na União Europeia: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos. MS thesis. Universidade de Évora, 2022.
[159] CNCS. (2020b). Ética & Direito. Observatório de Cibersegurança. 1-138. Disponível em https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriocibersegurancа-cncs.pdf. Acedido em 11/08/2023.
[160] Agência da União Europeia para a Cibersegurança (ENISA), a equipa de resposta a emergências informáticas (CERT.EU) e o Centro Europeu da Cibercriminalidade (EC3)

cibersegurança; a contribuição para os esforços de cooperação da União com países terceiros e organizações internacionais.".

Em 2012 foi instituída permanentemente a Equipa de Resposta a Emergências Informáticas da UE (CERT.UE), que, conforme demonstra o site da União Europeia[161] "é composta por uma equipa de peritos em segurança informática das instituições e organismos da UE. A equipa recolhe, gere, analisa e partilha informações com as instituições, organismos e agências da UE sobre ameaças, vulnerabilidades e incidentes relacionados com infraestruturas de TIC não classificadas. Coordena ainda as respostas a incidentes a nível institucional e interinstitucional, por exemplo, prestando ou coordenando a prestação de assistência operacional especializada.". Ela tem como objetivo prevenir, detectar, atenuar e responder a ciberataques.

O terceiro agente considerado mais importante é o Centro Europeu de Cibercriminalidade (EC3)[162] que foi criado em 2013 pela UE e é uma unidade de combate à cibercriminalidade que faz parte da Europol (serviço Europeu de polícia) e desempenha um papel crucial no bloqueio das operações das organizações criminosas dedicadas à cibercriminalidade[163]. Suas principais funções são, conforme o ato de sua criação, ser o ponto de convergência europeu das informações sobre a cibercriminalidade, deve também recolher informações de uma ampla variedade de fontes, identificar tendências e ameaças e melhorar os serviços de informação. Além disso tem a função de congregar conhecimentos especializados para apoiar o reforço das capacidades nos Estados - Membros: centrado sobretudo na formação de agentes da polícia e titulares do poder judiciário . Deve realizar o apoio operacional aos Estados-Membros, incentivar a criação de equipas de investigação conjunta para fazer face a questões específicas de cibercriminalidade e o intercâmbio de informações operacionais nas investigações em curso. Deverão, além disso, partilhar conhecimentos técnicos de armazenamento e cifragem (codificação de mensagens ou dados para impedir o acesso autorizado), bem como outros instrumentos e instalações *online*; ser o interlocutor coletivo dos investigadores europeus de cibercrimes a nível das autoridades policiais e do poder judicial nas discussões com o setor das TIC e outras empresas do setor privado, bem como com a com unidade dos investigadores, as associações de utilizadores e as organizações da sociedade civil[164].

No ano de 2016 surge uma importante Diretiva, especialmente para o setor bancário,

[161] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/computer-emergency-response-team-eu-institutions-bodies-and-agencies-cert-eu_pt

[162] Dunn, Myriam. A Resilient Europe for an Open, Safe and Secure Cyberspace UI Occassional Papers. Suécia. Nº 23. 2013.

[163] Barbosa, Maria Luís. As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal. JANUS.NET, e-journal of International Relations. Vol. 11, Nº.1. 2020.

[164] https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:230806_1

denominada Diretiva de Segurança das Redes e da Informação (*Network and Information Security* – NIS/SRI - 2016/1148) relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia. Sua criação proveio da incapacidade que a União Europeia tinha de garantir o nível de segurança pretendido[165], visto que tem como objetivo criar um espaço de liberdade, segurança e justiça. É a primeira legislação a nível europeu sobre segurança cibernética[166] e tem como função concentrar-se no reforço das autoridades cibernéticas a nível nacional, trazendo maior coordenação entre elas e introduzindo requisitos de segurança para setores privados essenciais, denominando-os de fornecedores de serviços essenciais, que são entidades consideradas parte integrante da infraestrutura essencial da União Europeia, e dentre elas estão as entidades bancárias[167]. Os Estados-Membros foram obrigados a transpô-las no prazo de 21 meses. A Diretiva impõe que qualquer legislação nacional sobre o tema deve observar, obrigatoriamente, dois requisitos: assegurar uma segurança cibernética de alto nível para as infraestruturas críticas do país e estabelecer um mecanismo de cooperação eficaz entre os Estados-Membros da UE para promover este objetivo. A Diretiva se propõe a criar uma ferramenta de resposta aos incidentes que possam prejudicar os serviços essenciais para o bom funcionamento da sociedade[168].

Conforme o *site* da União Europeia, o objetivo que a Diretiva propõe é realizar "um vasto conjunto de medidas para reforçar o nível de segurança das redes e sistemas de informação (cibersegurança) com vista a proteger serviços vitais para a sociedade e economia da União Europeia (UE). A Diretiva visa assegurar que os países da UE estejam devidamente preparados e prontos para fazer face e reagir a ciberataques através da designação de autoridades competentes; da criação de equipas de resposta a incidentes de segurança informática (CSIRT); e da adoção de estratégias nacionais de cibersegurança. Cria ainda um grupo de cooperação para facilitar a cooperação estratégica e técnica ao nível da UE. Introduz, por último, a obrigação para os operadores de serviços essenciais e os prestadores de serviços digitais de tomar as medidas de segurança apropriadas e notificar as autoridades nacionais competentes de qualquer incidente grave.".

[165] Gonçalves, Paula Filipa Trilho. Os Novos Desafios à cibersegurança na União Europeia em tempos de pandemia Covid19: De que forma a pandemia Covid19 veio alterar a cibersegurança na União Europeia, no período compreendido entre Março 2020 -Março 2021. 2022.

[166] Pereira, João Pedro Carvalhosa. A nova tecnologia 5G e a cibersegurança –Perceção dos impactos nas organizações e dos desafios para os auditores. 2022.

[167] Transposição da Diretiva Relativa à Segurança das Redes e da Informação (SRI) da UE disponível em: https://www.digitaleurope.org/resources/transposicao-da-diretiva-relativa-a-seguranca-das-redes-e-da-informacao-sri-da-ue/ Acedido em: 13/08/2023

[168] Hermenegildo França, Gabriella. Cibersegurança na União Europeia e os desafios para a sua eficácia perspetivas, panorama estratégico e instrumentos jurídicos. 2020

Ainda prevê que os Estados-Membros devem "designar uma ou mais autoridades nacionais competentes e CSIRT, assim como identificar um ponto de contacto único (se houver mais de uma autoridade nacional); e identificar os operadores de serviços essenciais de setores críticos, como o da energia, transportes, financeiro, bancário, da saúde, da água e das infraestruturas digitais, em que um ciberataque seria suscetível de perturbar um serviço essencial." Essa identificação dos serviços essenciais deve ser revisada a cada dois anos e se necessário a lista dos operadores de serviços essenciais identificados deve ser atualizada.

Ademais, a Diretiva é muito específica quando se refere a setores da banca, que, por ser parte essencial para esse estudo, passa a ser transcrita[169]:

"A regulamentação e a supervisão nos setores da banca e das infraestruturas dos mercados financeiros estão bastante harmonizadas a nível da União por via do direito primário e do direito derivado da União e das normas elaboradas em conjunto com as autoridades europeias de supervisão. No quadro da União Bancária, a aplicação e supervisão desses requisitos é assegurada pelo Mecanismo Único de Supervisão. Nos Estados-Membros que não fazem parte da União Bancária, tal aplicação e supervisão são asseguradas pelas entidades reguladoras bancárias competentes em cada um deles. Noutras áreas da regulamentação do setor financeiro, o Sistema Europeu de Supervisão Financeira também assegura um elevado grau de uniformização e convergência das práticas de supervisão. A Autoridade Europeia dos Valores Mobiliários e dos Mercados desempenha também um papel de supervisão direta de determinadas entidades, a saber, as agências de notação de risco e os repositórios de transações.".

No que diz respeito a Portugal, tem-se o já mencionado Banco de Portugal que regula, fiscaliza e sanciona a conduta das instituições de crédito, das sociedades financeiras, das instituições de pagamento, das instituições de moeda eletrónica e dos intermediários de crédito na comercialização de produtos e serviços bancários de retalho[170].

A Diretiva continua descrevendo que "o risco operacional constitui uma parte essencial da regulamentação e supervisão prudenciais nos setores da banca e das infraestruturas dos mercados financeiros. Abrange todas as operações, incluindo a segurança, integridade e resiliência das redes e dos sistemas de informação. Os requisitos relativos a esses sistemas, que frequentemente extravasam os requisitos previstos na presente diretiva, são estabelecidos numa série de atos jurídicos da União, inclusive nas regras aplicáveis ao acesso à atividade das

[169] DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L1148Acedida em: 12/08/2023

[170] https://www.bportugal.pt/page/missao-e-funcoes

instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento e nas regras relativas aos requisitos prudenciais aplicáveis às instituições de crédito e às empresas de investimento, que incluem requisitos relativos ao risco operacional; nas regras aplicáveis aos mercados de instrumentos financeiros, que incluem requisitos relativos à avaliação dos riscos das empresas de investimento e dos mercados regulamentados; nas regras aplicáveis aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações, que incluem requisitos relativos ao risco operacional das contrapartes centrais e dos repositórios de transações; e, nas regras aplicáveis à melhoria do sistema de liquidação de valores mobiliários na União e às centrais de depósito de títulos, que incluem requisitos relativos ao risco operacional. Além disso, os requisitos de notificação de incidentes, que fazem parte das práticas normais de supervisão no setor financeiro, são frequentemente incluídos nos manuais de supervisão. Os Estados-Membros deverão considerar essas regras e esses requisitos na sua aplicação da *lex specialis*."

A Diretiva é clara ao especificar determinadas medidas que devem ser observadas pelo setor bancário. E os inclui taxativamente na lista de operadores de serviços essenciais (OSE)[171]:

"Operador de serviços essenciais – OSE (Anexo II, Diretiva SRI): 1. Energia: a) Eletricidade, b) Petróleo, c) Gás; 2. Transportes: a) Transporte aéreo, b) Transporte ferroviário, c) Transporte marítimo e por vias navegáveis interiores, d) Transporte rodoviário; 3. Setor bancário; 4. Infraestruturas do mercado financeiro; 5. Setor da saúde: Instalações de prestação de cuidados de saúde (nomeadamente hospitais e clínicas privadas); 6. Fornecimento e distribuição de água potável; 7. Infraestruturas digitais: Pontos de troca de tráfego, Prestadores de serviços de DNS, Registos de nomes de domínio de topo."

Os operadores de serviços essenciais devem notificar as autoridades quando houver um incidente grave de segurança que, como a própria diretiva descreve, é "um evento com um efeito adverso real na segurança das redes e dos sistemas de informação". A Diretiva ainda exemplifica o que um evento grave é aquele que causa um efeito perturbador, e para a sua qualificação deve-se ter em consideração diversos fatores como o número de utilizadores que dependem desse serviço para fins privados ou profissionais, podendo essa utilização ser direta, indireta ou por intermediação. Deve-se considerar o tempo que pode decorrer até que a descontinuidade comece a ter um impacto negativo e a distribuição geográfica, no que se refere à zona afetada pelo

[171] Volchkova, Ekaterina. Sistema de gestão integrada de privacidade e segurança da informação : alinhamento com o regulamento geral sobre a proteção de dados. 2018.

incidente. Também deve levar-se em consideração a quota de mercado da entidade, e a importância da entidade para a manutenção de um nível suficiente do serviço, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço. E ainda prevê que para o setor bancário deve-se observar também fatores específicos como a sua importância sistémica com base nos ativos totais ou no rácio ativos totais/PIB.

A Diretiva determina que cada Estado-Membro irá adotar uma estratégia nacional de segurança das redes e dos sistemas de informação que defina os objetivos estratégicos e as medidas políticas e regulamentares adequadas para alcançar e manter um elevado nível de segurança das redes e dos sistemas de informação e que eles podem solicitar a assistência da ENISA para elaborar as suas estratégias nacionais. Cada Estado-Membro deve ter pelo menos uma Equipa de resposta a incidentes de segurança informática (CSIRT)[172].

Transpondo a Diretiva para o contexto do trabalho, ela impõe que os Estados-Membros assegurem que os operadores de serviços essenciais, no caso, as entidades bancárias, tomem "medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes". Devem também assegurar que esses serviços tomem as medidas adequadas para evitar incidentes e para reduzir ao mínimo o seu impacto, para que a continuidade da prestação de serviço seja garantida. Os bancos devem notificar as autoridades competentes caso haja algum incidente com impacto importante na continuidade do serviço por si prestados, e isso deve ocorrer sem demora injustificada. Caso o impacto do incidente afete outros Estados-Membros a autoridade competente ou a CSIRT deve informá-los. Ainda especifica que "após consultar o operador de serviços essenciais notificante, a autoridade competente ou a CSIRT podem informar o público sobre incidentes específicos, caso seja necessário sensibilizá-lo para evitar um incidente ou para tratar um incidente em curso".

Em 2020 a Diretiva é atualizada e assim surge a SRI2 que tem como objetivo garantir um eleva do nível comum de cibersegurança na União[173]. Ela fomenta a cooperação entre os Estados Membros, e estabelece que eles adotem estratégias nacionais de cibersegurança.

A Diretiva 2016/1148, a SRI, é transposta para o ordenamento português[174] através do

[172] Barros, Gabriel Osório. A Cibersegurança em Portugal. Gabinete de Estratégia e Estudos. 2018.
[173] Gonçalves, Paula Filipa Trilho. Os Novos Desafios à cibersegurança na União Europeia em tempos de pandemia Covid19: De que forma a pandemia Covid19 veio alterar a cibersegurança na União Europeia, no período compreendido entre Março 2020-Março 2021. Diss. 2022.
[174] Gouveia, Jorge Bacelar. Direito do Ciberespaço e Segurança Cibernética. Revista Jurídica Portucalense. 2021.

Regime Jurídico da Segurança do Ciberespaço, Lei n.º 46/2018, de 13 de Agosto[175]. A lei define os princípios, as regras, os órgãos e as medidas para a proteção do ciberespaço nacional, bem como as obrigações e os deveres dos operadores de serviços essenciais e dos prestadores de serviços digitais[176]. Inclusive, no seu artigo 9º, estabelece as competências da Equipa de Resposta a incidentes de Segurança Informática Nacional (CERT.PT) que são: Exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática setoriais existentes; monitorizar os incidentes com implicações a nível nacional; ativar mecanismos de alerta rápido; intervir na reação, análise e mitigação de incidentes; proceder à análise dinâmica dos riscos; assegurar a cooperação com entidades públicas e privadas; promover a adoção e a utilização de práticas comuns ou normalizadas; participar nos fora nacionais de cooperação de equipas de resposta a incidentes de segurança informática; assegurar a representação nacional nos fora internacionais de cooperação de equipas de resposta a incidentes de segurança informática; e participar em eventos de treino nacionais e internacionais[177].

O Relatório de Cibersegurança em Portugal esclarece que "em Portugal, a Autoridade Nacional de Cibersegurança é o Centro Nacional de Cibersegurança, que faz parte do Gabinete Nacional de Segurança. Outros atores importantes incluem o Conselho Superior de Segurança do Ciberespaço, a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T), o Gabinete Cibercrime da Procuradoria-Geral da República, a Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT) e a Comissão Nacional de Proteção de Dados".

A Lei n.º 46/2018 prevê que a missão do Centro Nacional de Cibersegurança é[178] "garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços

[175] Pinto, Filipa Couto Astorga Batista. Enquadramento técnico-jurídico da segurança do ciberespaço. Diss. 2019.
[176] Teixeira, Maria Emília, Reis, Lara. A transformação digital na banca e a crescente relevância da resiliência operacional. Revista Electrónica de Direito. 2022
[177] Lei n.º 46/2018. Regime Jurídico da Segurança do Ciberespaço. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
[178] Lei n.º 46/2018. Regime Jurídico da Segurança do Ciberespaço. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384

essenciais e dos prestadores de serviços digitais".

Ademais, afigura-se de extrema importância a Estratégia Nacional de Segurança do Ciberespaço (ENCS), adotada em 2015 e atualizada em 2019[179], que é uma orientação holística para Portugal que tem o intuito de implementar uma visão global e caminhos a serem seguidos para a proteção e segurança das infraestruturas tecnológicas nacionais e dos serviços vitais de informação[180]. A coordenação dessa estratégia é da responsabilidade do Centro Nacional de Cibersegurança. A estratégia possui cinco pilares basilares, conforme Luís Borges Gouveia[181] "Subsidiariedade: a proteção do ciberespaço é responsabilidade primária dos utilizadores que o utilizam e dos proprietários das infraestruturas tecnológicas que compõe este domínio de interação. Com pete ao Estado apenas intervir, em última instância, a título subsidiário, auxílio e reforço para garantir a eficácia e as necessidades da segurança do ciberespaço; Co mple mentaridade: todas as partes interessadas no ciberespaço repartem entre si a responsabilidade da segurança deste ambiente. Todos devem contribuir e apoiar -se mutuamente com base nas suas capacidades em prol do bem comum; Cooperação: face à ausência de fronteiras e delimitações no ciberespaço torna-se mais eficaz a sua segurança com a agregação de esforços entre todos os intervenientes nacionais e internacionais reforçadas por uma cultura de confiança global; Proporcionalidade: os recursos e as ações necessárias à segurança do ciberespaço devem ser os apropriados e ajustados face aos riscos identificados para cada situação; Sensibilização: a tomada de consciência por parte dos utilizadores, dos possíveis riscos existentes no ciberespaço, é fundam ental para uma melhor avaliação das ações necessárias à sua prevenção e proteção".

Os três objetivos estratégicos são maximizar a resiliência, promover a inovação e gerar e garantir recursos[182]. Para atingir esses objetivos foram determinados seis eixos de intervenção: O eixo um diz respeito a estrutura de segurança do ciberespaço, que tem como objetivo garantir a segurança e a resiliência do ciberespaço nacional, protegendo os interesses nacionais e os direitose liberdades fundamentais dos cidadãos.

Esse eixo assegura a envolvência de recursos, conhecimentos e competências necessárias

[179] Estratégia Naci onal de Segura nça do Ci berespaço 2019-2023. Disponível em: https://www. cncs. gov. pt/docs/cncs-ensc-2019-2023.pdf . Acedido em: 29.09.2023.

[180] Gouveia, Luís Borges. Estratégia Nacional de Segurança do Ciberespaço. Tecnologia, redes e sociedade. 2017.

[181] Gouveia, Luís Borges. Estratégia Nacional de Segurança do Ciberespaço. Tecnologia, redes e sociedade. 2017.

[182] Obj etivo estratégico 1 - Maximizar a resiliência: Fortalecer e garantir a resiliência digital nacional potenciando a inclusão e a colaboração em rede de forma a salvaguardar a segurança do ciberespaço de interesse nacional face às ameaças que possam compr ometer ou provocar a disrupção das redes e sistemas de informação essenciais à sociedade. Obj etivo estratégico 2 - Promover a inovação: Fomentar e potenciar a capacidade nacional de inovação afirmando o ciberespaço como um domínio de desenvolvimento económ ico, social, cultural e de prosperidad e. Objetivo estratégico 3 - Gerar e garantir recursos: Contribuir para obter e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço.

para lidar com a complexidade e a abrangência dos desafios da segurança do ciberespaço, que tem como órgão consultivo do primeiro-ministro o Conselho Superior de Segurança no Ciberespaço, possui representantes de todas as partes interessadas e assegura a coordenação político-estratégica para a segurança do ciberespaço.

Algumas das ações previstas no eixo um são o reforço da capacidade de prevenção, deteção, resposta e recuperação face a incidentes e ameaças no ciberespaço , a promoção da cooperação entre as entidades públicas e privadas responsáveis pela segurança do ciberespaço, incluindo os operadores de serviços essenciais e os prestadores de serviços digitais, o desenvolvimento e implementação de mecanismos de partilha de informação e boas práticas sobre segurança do ciberespaço e a sensibilização e capacitação dos utilizadores do ciberespaço para a adoção de comportamentos seguros e responsáveis[183].

O eixo dois é a prevenção, educação e sensibilização, dos cidadãos, das organizações e do Estado, sobre os riscos e oportunidades do ciberespaço[184]. Algumas das medidas previstas por esse eixo são o desenvolvimento e implementação de um plano nacional de sensibilização para a segurança do ciberespaço, dirigido a diferentes públicos-alvo, como crianças, jovens, idosos, profissionais, empresas e entidades públicas; a criação de conteúdos educativos e informativos sobre a segurança do ciberespaço, utilizando diversos meios e canais de comunicação, como redes sociais, plataformas digitais, campanhas de publicidade, eventos e iniciativas de divulgação, o reforço.

Prevê também a formação e a qualificação dos recursos humanos na área da segurança do ciberespaço, tanto no setor público como no setor privado, incentivando a certificação de competências e a criação de oportunidades de carreira; o estimulo da participação da sociedade civil na promoção da segurança do ciberespaço, envolvendo associações, organizações não governamentais, academias, centros de investigação e outros atores relevantes; a proteção do ciberespaço e das infraestruturas; resposta às ameaças e combate ao cibercrime; Investigação, desenvolvimento e inovação; e Cooperação nacional e internacional.

Co m relação a esse eixo foi criado um progra ma de formação avançada em cibersegurança para a administração pública e o setor privado desenvolvido pelo Centro Nacional de Cibersegurança no âmbito do Plano de Recuperação e Resiliência, denominado *C-Academy*[185]. O programa pretende qualificar e requalificar recursos humanos de acordo com o referencial de

[183] Gouveia, Luis Borges, and Raul Morgado. "Estratégia Nacional de Segurança do Ciberespaço." * TRS Relatório Interno 2017.10/2017. 2017.
[184] Estratégia Nacional de Segura nça do Ciberespaç o 2019- 20 23
[185] Portaria n.º 163/ 20 23 - Diário da Re pú blica, 2.ª série – 202 3. Disponível e m: https://files. dre. pt/2s/20 23/ 04/ 06 80 000 00/ 00 01 800 01 9. pdf . Acedido e m: 10. 11. 2023

competências de cibersegurança; disponibilizar conteúdos e formações alinhados com o Quadro Nacional de Referência para a Cibersegurança (QNRCS); convergir com os Digital *Innovation HUBs*; alcançar uma distribuição geográfica que permita abranger todo o território nacional; abranger pelo menos 9800 formandos até ao primeiro trimestre de 2026 em parceira com as Instituições de Ensino. A formação se encontra distribuída por todo o território português[186].

O terceiro eixo é a proteção do ciberespaço e das infraestruturas, que tem como principais medidas "Avaliar o estado da arte no que concerne à segurança do ciberespaço e da capacidade de atuação dos organismos que administrem infraestruturas críticas e serviços vitais de informação, bem como prover melhorias contínuas de atuação; desenvolver a capacidade de deteção de ataques e implementar as contramedidas necessárias de modo a garantir a continuidade normal das operações; os proprietários de infraestruturas críticas devem incluir medidas de segurança do ciberespaço, baseadas na gestão do risco, nos seus planos de proteção. Devem igualmente, incluir nos seus planos de segurança medidas a adotar suster ameaças oriundas do ciberespaço; fomentar e incentivar o uso de políticas e normas de segurança para assegurar um elevado nível de proteção; os operadores de infraestruturas críticas devem constituir um conjunto mínimo de recursos humanos e técnicos adstritos à função da segurança do ciberespaço; atualizar a legislação nacional para fazer face às evoluções tecnológicas e às boas práticas para a proteção do ciberespaço"[187].

O eixo quatro consiste na resposta às ameaças e combate ao cibercrime, esse eixo pretende desenvolver e consolidar a capacidade de ciberdefesa, avaliar as necessidades de revisão e atualização da legislação, promover, ao nível setorial e do tecido empresarial, a criação de fóruns de partilha de informação operacional e técnica, de resposta coordenada a incidentes de segurança. A estratégia, nesse eixo, refere a importância de uma observação atenta e permanente para a prevenção e investigação dos cibercrimes. Também a essencialidade de as instituições desenvolverem um permanente esforço de apetrechamento que lhe permita cumprir com a função de vigilância ativa do seu ciberespaço[188].

Já o eixo cinco diz respeito a investigação, desenvolvimento e inovação, através do qual se pretende o fortalecimento, apoio e promoção do potencial nacional de investigação, desenvolvimento e inovação de processos e tecnologias de vanguarda para a cibersegurança, com base nas capacidades individuais e coletivas do setor público e privado, da academia e da

[186] C-Academy. CNCS. Disponível em: https://cncs.gov.pt/pt/c-academy/ . Acedido em: 10.09.2023

[187] Gouveia, Luis Borges, and Raul Morgado. "Estratégia Nacional de Segurança do Ciberespaço." * TRS Relatório Interno 2017.10/2017. 2017.

indústria. Também busca fomentar a produção científica, estimular e potenciar através de financiamento adequado as capacidades científicas, técnicas e industriais do país, com especial ênfase nos domínios críticos e nas tecnologias emergentes, dando prioridade ao desenvolvimento de tecnologias para a cibersegurança e à resposta às necessidades identificadas de inovação. Promover o desenvolvimento de produtos, sistemas e serviços tecnológicos. Esse eixo busca incentivar todo o tipo de inovação aliada à cibersegurança.

Por fim, o eixo seis trata da cooperação nacional e internacional, demonstra que no mundo globalizado em que vivemos a cooperação entre as nações se faz essencial para a proteção do ciberespaço e que o desenvolvimento da confiança mútua deve ser um dos alicerces. Tem com o medidas "Contribuir para a regulação e universalização do ciberespaço promovendo o respeito do direito internacional aplicável, a partilha transparente da sua governação entre todos os atores, a respetiva acessibilidade universal e a disseminação de boas práticas de utilização; aprofundar a participação nacional nos órgãos, organismos e agências relevantes, nomeadamente, da Organização das Nações Unidas, da União Europeia e da Organização do Tratado do Atlântico Norte. Deve também aprofundar a participação nacional na Organização para a Segurança e Cooperação na Europa, designadamente, no esforço de redução do risco de tensões entre Estados, no âmbito da segurança do ciberespaço; participar nos exercícios de cibersegurança e de ciberdefesa reforçando e aumentando o nível de maturidade para a proteção do ciberespaço, onde a partilha de informação e conhecimento constitui um fator fundamental; Integrar organismos internacionais de cibersegurança e de ciberdefesa tendo em vista a cooperação internacional e a afirmação de Portugal neste domínio; aprofundar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças; aprofundar a articulação entre o Centro Nacional de Cibersegurança e a ANACOM - Autoridade Nacional de Com unicações, bem como entre aquele e as entidades que compõem o Sistema de Certificação Eletrónica do Estado no âmbito das respetivas atribuições; desenvolver o quadro internacional da ciberdiplomacia em que Portugal se deverá inserir, identificando iniciativas prioritárias, nomeadamente, as organizações internacionais ou intergovernamentais de intercâmbio de boas práticas a que deverá aderir"[189].

Portugal, através da estratégia nacional de segurança do ciberespaço que constitui marco fundamental para o futuro da segurança do ciberespaço no contexto nacional, da transposição da

Diretiva SRI através da Lei 46/2018, do Centro Nacional de Cibersegurança (CNCS) que é a autoridade nacional responsável pela promoção e coordenação da cibersegurança em Portugal, vem realizando um trabalho árduo de prevenção e resposta aos cibercrimes, aplicando de maneira célere e adequada as orientações da União Europeia, que busca não só fomentar a presença de empresas tecnológicas com um ciberespaço seguro, mas também se coloca como precursora da defesa da população frente às ciberameaças, servindo de exemplo para todos os países que não se preocupam apenas com o crescimento económico, mas também com o bem -estar dos seus cidadãos.

3. Aspetos Informáticos na Segurança Cibernética

3.1. Práticas de Segurança adotadas pelas Instituições Bancárias

Além da adequação aos diplomas já mencionados, as entidades bancárias adotam estratégias de cibersegurança para proteção contra o cibercrime, essas são feitas de forma que mitigue os riscos existentes, já que não é possível estar completamente protegido, e não se faz coerente ou minimamente sensato não ter proteção nenhuma[190].

Um dos elementos primordiais para uma boa cibersegurança é a implementação de uma estratégia da empresa para a execução de políticas de segurança cibernética. Essa estratégia é um conjunto de etapas e instruções que definem quais os objetivos a serem atingidos, os riscos existentes e a atual situação que a empresa se encontra nesse quesito[191].

A utilização de boas práticas de segurança é uma forma de minimizar os riscos de sofrer um ciberataque bem-sucedido e que prejudique o funcionamento do banco, e elas devem ser inovadoras, visto que o ambiente da tecnologia está em constante mudança. Normalmente essa atribuição é dividida em diversos setores, com responsabilidades diferentes para cada um deles[192].

Uma dessas medidas é a autenticação multifator, que é utilizada na maioria das entidades financeiras[193]. A autenticação é uma maneira de o utilizador aceder a um recurso informático comprovando a sua identidade através de uma forma pré-concebida no sistema, a forma mais usual é o uso de uma palavra-passe, podendo ser reconhecimento facial, ocular, leitura da digital,

[190] Silva, Pedro Miguel Lopes Martins da. Gestão de cibersegurança em organizações financeiras. MS thesis. 2018.
[191] Faria, Nelson Correia. *Estratégia de cibersegurança.* Diss. 2022.
[192] Faria, Nelson Correia. Estratégia de Cibersegurança. 2022.
[193] Equipe Totvs. Autenticação multifator: O que é e como implementar. 2023. Disponível em: https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/autenticacao-multifator/ Acedido em: 17.09.2023.

entre outras. Quando é exigida pelo sistema apenas uma prova de identidade, chama -se autenticação simples. Entretanto, para maior segurança, as entidades bancárias normalmente exigem a autenticação multifator, nesse caso são exigidas diversas provas de verificação da identidade, uma por cada fator de autenticação.

Conforme Élton Carpinteiro[194], "O uso de múltiplos fatores de autenticação para provar a identidade de alguém é baseado na premissa de que uma pessoa não autorizada provavelmente não será capaz de fornecer todos os fatores necessários para o acesso. Assim, se numa tentativa de autenticação pelo menos um dos componentes estiver em falta, ou se for incorreto, a identidade do utilizador não é estabelecida com um grau de certeza suficiente e o acesso ao recurso informático permanece bloqueado". Essas provas de identificação podem ser classificadas em quatro fatores[195]:

Something you know (fator de conhecimento): que é algo que o usuário sabe previamente (senha, *personal identification number - PIN*). Esse meio de identificação possui baixo custo e é de simples implementação.

Something you have (fator de posse): que é algum objeto que o usuário possui *(cartões eletronicos*, chaves físicas, comumente chamados de *token*).

Somthing you are (fator inerente): que é algo que a pessoa possui fisicamente (retina, impressão digital, ADN, padrão de voz).

Someplace you are (fator de localização): que é através de sua localização geográfica ou endereço de *IP*.

A autenticação multifator utiliza mais de um tipo de identificação, podendo ser os dois do mesmo grupo de fatores ou de grupos diferentes, como por exemplo realizar um levantamento de dinheiro em um *ATM (Automated Teller Machine)* no qual é necessário o uso de um *token* físico (o cartão bancário) e um código *PIN*, que é a combinação de um fator de conhecimento com o fator de posse[196]. Quem define isso é o administrador do sistema após analisar o que é seguro o bastante para a rede em questão.

Dentre as formas de autenticação existem também os protocolos dos quais decorre a permissão do acesso ao sistema. Um modelo muito interessante e que vem crescendo e começando a ser comum em empresas é o acesso via *Single Sing-On (SSO)*. O ambiente *SSO* permite que o usuário se autentique apenas uma vez por sessão, não tendo a necessidade de

[194] Pastilha, Élton Carpinteiro. Autenticação fido2 em dispositivos android. 2022.
[195] William Kennedy and Aspen Olmsted. Three factor authentication. In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). 2017. Disponível em: http://www.icitst.org/Proceedings/ICITST-2017-Proceedings.pdf . Acedido em: 01.10.2023.
[196] Saldanha, Ana Beatriz Martins. Gestão de Dados em Cidades Inteligentes. 2022.

voltar a se identificar após adentrar o sistema. Depois de *"logar"* fica permitido o acesso a todos os recursos da rede[197]. Uma boa maneira de manter o *SSO* mais seguro é unir ele e a autenticação multifator[198].

Após a autenticação ser realizada com sucesso ocorre a autorização, que é controlo e acesso, que faz a mediação do serviço, que determina se o pedido deve ser aceito ou negado[199].

A autenticação multifator é um conjunto de autenticações e o usuário deve acertar todas as formas de prova da sua identidade, errando uma elas, já não será possível adentrar ao sistema. O processo funciona com o envio das credenciais pelo usuário, o servidor verifica se elas estão corretas. Ao realizar a verificação o servidor envia uma autorização de autenticação ao usuário, que passa a ter o acesso ao sistema permitido[200].

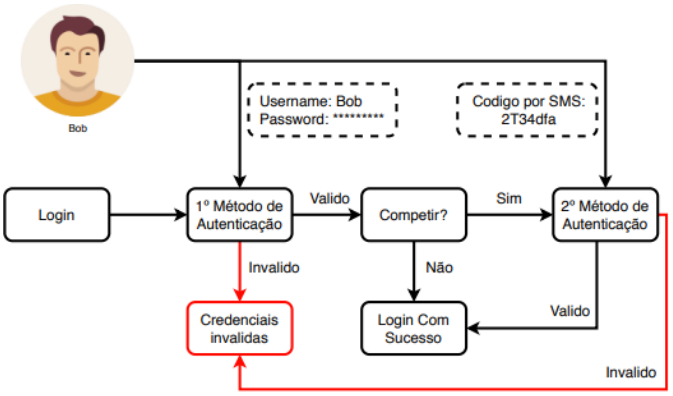


Figura 6 – (reproduzida por Pastilha, Élton Carpinteiro)

O controlo criptográfico é outro meio de segurança amplamente utilizado no setor bancários e empresarial. Como já mencionado anteriormente, existem relatos que esse método já era utilizado pelos romanos, e vem se aprimorando desde então. Com a criptografia, as mensagens ficam acessíveis apenas a quem tem autorização para visualizá-las[201].

A criptografia, além de manter a informação confidencial, garante a integridade e a autenticidade dela[202]. Esse método deve ser forte, como por exemplo a criptografia *AES (Advanced Encryption Standard)*, que é simétrica, altamente confiável e compatível com diversos sistemas

[197] Mesquita, Tiago António Cabanelas. Soluções Single Sign On em software de uso livre. 2010.
[198] Jorge, Bruno Tiago Correia. Segurança e privacidade numa infraestrutura de VoIP. 2017.
[199] Saldanha, Ana Beatriz Martins. Gestão de Dados em Cidades Inteligentes. 2022.
[200] Pastilha, Élton Carpinteiro. Autenticação fido2 em dispositivos android. Diss. 2022.
[201] de Moraes, Alexandre Fernandes. Cibersegurança e a nova geração de Firewalls. Saraiva Educação SA, 2021.
[202] Ferreira, Haroldo. Cibersegurança. Editora Senac São Paulo, 2021.

operacionais[203].

A criptografia por chave simétrica funciona com os participantes compartilhando a mesma chave de acesso, ou seja, essa chave é usada para codificar e para descodificar os dados[204]. O modelo em questão, o *AES*, é um dos mais seguros na atualidade, sendo utilizado, inclusive, pelo governo dos Estados Unidos da América. Conforme Augusto Arcanjo "Sua criptografia é um bloco de 128 bits, mas a chave também pode ser aplicada em 192 e 256 bits, dificultando muito a quebra dessa chave em um ataque cibercriminoso tradicional".

Outro método essencial utilizado pelos bancos é o uso de *framework* de *cibersecurity*. *Frameworks* (traduzido é estrutura) são uma série de procedimentos, análises e boas praticas que são adotadas na implementação da segurança da informação[205]. Os dois mais utilizados no mundo são a ISO 27000 e a NIST *Cybersecurity Framework*. A primeira possui uma série de edições com normas direcionadas a diversos temas. O significado de ISO é *International Organization for Standardization* (Organização Internacional de Padronização), e são sistemas internacionais de padrões industriais publicados por essa organização. As normas voltadas à cibersegurança são a ISO 27001 e a ISO 27002 e descrevem o método de gestão da segurança da informação, elas fornecem um quadro de atuação e são mais voltadas à proteção de dados[206]. Essa normatização torna a empresa capaz de avaliar os riscos à segurança da informação e implementar políticas e procedimentos para gerir esses riscos.

A ISO 27001 fornece uma estrutura para orientar organizações, de qualquer tamanho, a proteger sistematicamente e de forma econômica os seus dados, por meio de um processo denominado Sistema de Gerenciamento de Segurança da Informação (SGSI)[207]. Nas palavras de Pedro Magalhães "Um SGSI já implementado rege-se pelas políticas, procedimentos, processos e fluxos de trabalho que são escolhidos para ajudar a proteger a segurança dos dados de uma organização. Assim que as políticas forem definidas pela organização, elas devem ser implementadas e geridas em toda a organização para obter os seus benefícios. A organização tem no seu poder governar as políticas com o ciclo PD CA (Planear, Executar, Verificar e Agir), revendo regularmente os procedimentos e ajustando-os conforme necessário". A principal filosofia dessa

[203] O sistema operacional é um software, ou conjunto de softwares, cuja função é administrar e gerenciar os recursos de um sistema, desde componentes de hardware e sistemas de arquivos a programas de terceiros, estabelecendo a interface entre o computador e o usuário.
[204] KUROSE, James - Redes de Computadores e a Internet uma abordagem top-down-Pearson. 2013.
[205] Virgilio, Flávio. Frameworks paa Segurança da Informação. 2022.
[206] Miranda, Cláudio Zumpichiatte. Auditoria de Segurança da Informação nos Órgãos da Administração Pública: Maturidade, Compliance e Boas Práticas. .Distrito Federal. 2017.
[207] Magalhães, Pedro M. "Requisitos e recomendações para o desenvolvimento e operação de um SGSI–Abordagem com ISO 27001/27002."

ISO é realizar a gestão de riscos, descobrindo onde eles estão, e assim tratá -los através da implementação de controlos de segurança.

Já a segunda, o NIST (*National Institute of Standards and Technology*), é um órgão de defesa do governo dos Estados Unidos da América, que emitiu um conjunto de boas práticas para cibersegurança, denominado NIST *Cybersecurity Framework*, e se tornou um padrão de referência por todo o mundo, sendo muito utilizado por grandes empresas [208] . Ele é um guia para ajudar a lidar com a segurança da informação nas dimensões físicas, cibernéticas e em relação a pessoas. Ele pode ser usado na área de tecnologia da informação, nos sistemas de controlo industrial, nos sistemas ciber-físicos ou em dispositivos relacionados à *internet* das coisas, com o objetivo de reduzir e gerenciar os riscos de segurança em cada uma dessas áreas ou na estrutura inteira. O guia complementa o processo de gerenciamento de segurança e potencializa os métodos de proteção já utilizados pela empresa [209].

Ademais, fazem uso de *firewalls*, que é uma ferramente indispensável para qualquer empresa. O *firewall* "nada mais é do que um ativo colocado em uma localização estratégica dentro da topologia de rede, por onde todo tráfego, obrigatoriamente, deve passar para poder chegar em determinado destino. Sua função é realizar a segurança de toda comunicação entre as redes existentes, como a passagem de determinados tráfegos, portas, determinar o que pode entrar e sair em termos de pacotes e informações de rede, quem pode aceder determinada rede, permitindo assim um controle maior sobre o ambiente"[210]. É uma combinação de *hardware* e *software* que controla a entrada e a saída dos pacotes na rede, permitindo que alguns passem e bloqueando outros, dependendo se são seguros ou não. O nome *firewall* remete, na sua tradução, à muro de fogo, que ao se fazer uma analogia consegue-se visualizar o funcionamento dele.

Esses métodos de cibersegurança, combinados com a adequação aos regulamentos tornam os bancos mais seguros e confiáveis, e com mais possibilidade de diminuir a taxa de ataques cibernéticos que possam ser prejudiciais ao seu funcionamento.

3.2. Desafios Futuros na Segurança Cibernética no Setor Bancário

O maior desafio das entidades bancárias atualmente é utilizar métodos inovadores que tenham baixo custo para a sua segurança. Com a chegada de novas formas de empresas

[208] Pinto, Walker Douglas Garcia. Cibersegurança. Seminário de tecnologia gestão e educação. 2020.
[209] Paschoal, Dener Aparecido Caldeira; Pereira, Guilherme Fontes. Segurança da informação na indústria 4.0: framework NIST. 2019.
[100] Fachinelli, Mateus. Ahlert, Edson Moacir. Firewall de próxima geração-fortinet. *Revista Destaques Acadêmicos*. 2019.

financeiras (bancos digitais, *fintechs*[211]), os bancos precisam se modernizar e estar atualizados tecnologicamente para que não percam os seus usuários. Porém, com o crescimento do uso dos meios digitais, aumenta a insegurança perante os cibercrimes, e assim, deve aumentar a atençãoà cibersegurança, a tendo como prioridade, e implementar meios cada vez mais modernos para sua proteção e, dessa forma, proteção dos seus clientes[212].

Uma nova tecnologia que vem surgindo e que os novos modelos de empresa já se apresentam ao mercado a utilizando é a *cloud technology* (tecnologia na nuvem), e hoje os bancos aceleram o seu processo de migração para essa nova forma de gestão[213]. Além de todos benefícios que a tecnologia *cloud* apresenta[214], é uma forma de aumentar a segurança cibernética das redes.

A tecnologia na nuvem elimina a necessidade de qualquer servidor local. Nas palavras de Flávio Sousa[215] "a nuvem é uma metáfora para a Internet ou infraestrutura de comunicação entre os componentes arquiteturais, baseada em uma abstração que oculta à complexidade de infraestrutura ... Para utilizarem os serviços, os usuários necessitam apenas ter em suas máquinas um sistema operacional, um navegador e acesso à *Internet*. Todos os recursos computacionais estão disponíveis na nuvem e as máquinas dos usuários não necessitam ter altos recursos computacionais, diminuindo o custo na aquisição de máquinas. Todo *hardware* pode ser utilizado para realizar alguma tarefa que seja adequada ao seu poder de processamento. Novos recursos de *hardware* podem ser adicionados a fim de aumentar o poder de processamento e cooperar com os recursos existentes". Abaixo uma demonstração de como funciona essa tecnologia:

[211] O termo fintech surgiu da combinação das palavras em inglês *financial* (finanças) e *technology* (tecnologia). Esse nome, por si só, resume bem a ideia: fintech é toda empresa que oferece serviços financeiros que se diferenciam pelas facilidades proporcionadas pela tecnologia e, com efeito, pela internet. A tecnologia é aplicada, essencialmente, para trazer conveniência por meio da inovação: empresas do ramo utilizam recursos tecnológicos amplamente disseminados para criar metodologias, processos e ferramentas que facilitam o acesso a serviços financeiros. (Disponível em: https://www.infowester.com/fintech.php Acedido em: 25.09.2023).

[212] Garcia, Paulo. "Que tendências estão a moldar o futuro da banca?". Disponível em: https://observador.pt/opiniao/que-tendencias-estao-a-moldar-o-futuro-da-banca/ Acedido em: 25.09.2023

[213] Setor bancário acelera adoção da cloud. Disponível em: https://www.itinsight.pt/news/digital/setor-bancario-acelera-adocao-da-cloud.

[214] Conforme estudo da Accenture realizado este ano, 2023, a *cloud* traz para os bancos maior velocidade e agilidade, e novos recursos que lhes permitem aumentar a receita, além de maior segurança. Disponível em: https://bankingblog.accenture.com/banking-cloud-altimeter-magazine/volume-4-bank-cloud-mainframe-migration.

[215] Sousa, Flávio. Moreira, Leonardo. Machado, Javam. Computação em nuvem: Conceitos, tecnologias, aplicações e desafios. II Escola Regional de Computação Ceará, Maranhão e Piauí (ERCEMAPI). 2009.

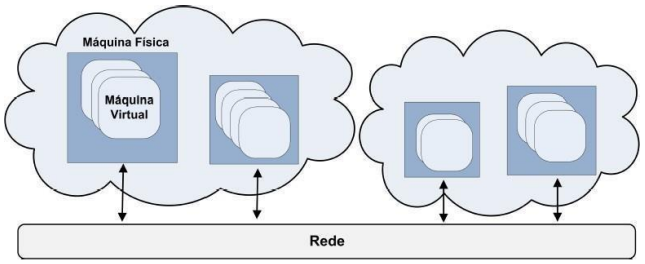


Figura 7 – (reproduzida por Emanuel F. Coutinho, Flávio R. C. Sousa, Danielo G. Gomes e José N. de Souza[216])

Esse modelo de computação traz facilidade de acesso, baixo custo e garantia de disponibilidade e escalabilidade. Para a segurança cibernética a nuvem se faz uma opção de extrema relevância, já que essa proteção vem como prioridade. Não há ambiente físico, o que já diminui uma possibilidade de fragilidade da informação (por exemplo, um incêndio não afetaria minimamente os dados da empresa), os *backups* são feitos constantemente, os dados não se perdem pois não há uma rede interna privada que pode ser atingida[217]. Essa segurança é feita por meio de inteligência artificial que permitem antecipar avisos e alertas, permitindo a ação mais célere dos utilizadores.

Outra forma muito utilizada por fintechs e que agora está finalmente ganhando as atenções das entidades bancárias é a tecnologia *blockchain* ("o protocolo de confiança"). Essa tecnologia aumenta os níveis de confiabilidade entre os dispositivos de uma rede e reduz os riscos de adulteração de dados, garantindo, assim, a integridade da informação[218].

A *blockchain* possui um armazenamento onde periodicamente são registradas todas as informações das transações nela realizadas, esses registros são públicos, compartilhados e universais, ou seja, qualquer um que tem acesso à essa rede, tem como verificá-los. É impossível que haja repetição de registros. Além de não poderem ser repetidos, depois de registrados, jamais poderão ser alterados ou excluídos, caso aconteça algum erro no procedimento, ele só poderá ser corrigido com nova transação.

A *blockchain* é formada por uma série de blocos, e cresce constantemente à medida que

[216] Coutinho, Emanuel & Sousa, Flávio & Gomes, Danielo & Souza, Jose. (2013). Elasticidade em Computação na Nuvem: Uma Abordagem Sistemática.

[217] Dias, Carlos Luís Soares. "Computação em nuvem." 2013.

[218] Fernandes, Filipe S. Cibersegurança no setor financeiro: os perigos e consequências dos ataques cibernéticos em instituições financeiras. 2020. Disponível em: https://www.jornaldenegocios.pt/negocios-iniciativas/banca-do-futuro/detalhe/ciberseguranca-e-tema-na-gestao-de-topo .

novos blocos são acrescentados (à medida que se fazem as transações). Assim, essa tecnologia busca a descentralização como forma de segurança, foi desenvolvida como uma rede par-a-par, ou seja, todos os participantes da rede são iguais, não existindo um nó centralizador. Todos os participantes dessa rede trabalham para que ela continue e siga segura, todos são espécies de vigilantes dela[219]. Nas palavras de Daniel Drescher "de maneira simplificada a *Blockchain* é uma estrutura de dados que armazena transações de forma ordenada e ligada ao bloco anterior, servindo como um sistema de registros distribuído. Essa estrutura é dividida em duas partes: cabeçalho e transações, e armazena informações detalhadas a respeito das transações que contém. Assim é possível associar uma transação ao seu endereço de origem e destino. Cada bloco possui uma identificação única gerada a partir de um resumo criptográfico (...) Por esse motivo, essa estrutura recebeu o nome de "corrente de blocos" ou *Blockchain*".

Estudos confirmam que a *blockchain* é a melhor forma de proteger a "tríade da CIA", ou seja, os pilares da cibersegurança, confidencialidade, integridade e autenticidade[220]. A *blockchain* garante uma melhor criptografia, visto que consegue analisar a integridade dos dados de forma célere, e eliminar a necessidade de senhas, que, por ser responsabilidade do usuário, é uma fragilidade na cibersegurança. Ademais, por ser uma rede compartilhada, permite uma constante vigilância das possíveis ameaças, anomalias e organismos não familiares sem necessitar de um controlo central. Inclusive, seu modo de funcionamento evita ataques *DDos* já mencionado anteriormente[221].

Vale mencionar que a *blockchain* juntamente com a cibersegurança estão em constante evolução e transformação. Por fim, cabe destacar os seus benefícios para a *cybersecurity* que são a proteção e o processamento de dados (dados nela gravados são imutáveis, dessa forma são mais seguros e íntegros), transferência segura de informação, eliminação de um ponto vulnerável (o ser humano), transparência e rastreabilidade dos dados (as transações são digitalmente assinadas e com hora certa registada), confidencialidade do usuário (a confidencialidade dos usuários da rede é extremamente alta devido à uma chave pública criptografada que autentica os usuários) e aumento da confiança (algo essencial para os bancos).

As entidades bancárias necessitam olhar para as tecnologias emergentes como algo a ser

[219] Drescher, Daniel. *Blockchain Básico: uma introdução não técnica em 25 passos.* Novatec Editora, 2018.
[220] Revoredo, Tatiana. Segurança cibernética de blockchains e protocolos de consenso: Como blockchain supera as adversidades da cibersegurança?. 2021. Disponível em: https://mittechreview.com.br/seguranca-cibernetica-de-blockchains-e-protocolos-de-consenso/. Acedido em: 27.09.2023.
[221] Camilo, Evandro. Blockchain: uma nova forma de pensar em cybersecurity. Report • Cyber Tech. 2021

implementado imediatamente, para sua segurança e manutenção no mercado financeiro. Entretanto, não basta o uso das tecnologias sem a devida aplicação delas.

Apesar da atenção dedicada pelos bancos à cibersegurança, não se faz suficiente seus mecanismos de defesa, um dos problemas que gera grandes danos e que não tem a atenção necessária é o fator humano, que já é uma vulnerabilidade, e com o crescimento da tecnologia trará ainda mais prejuízo se não for gerido imediatamente[222]. As pessoas não se preparam e não são preparadas para utilizar os meios informáticos de forma adequada, essa falta de instrução somada à atual dependência às redes representa essa grande vulnerabilidade[223].

A maioria dos erros humanos são causados por falta de treinamento adequado, no caso das entidades bancárias, tanto dos seus trabalhadores quanto dos seus clientes, quando não são causados por funcionários mal-intencionados. Dessa forma, eles se tornam uma porta aberta para o acesso aos dados que os cibercriminosos estão em busca[224]. Em um estudo realizado pela *Ponemon Institute*[225] concluiu que o custo médio das violações sofridas através de um cibercrime em uma grande empresa pode gerar o custo de 3,86 milhões de dólares[226], esse prejuízo poderia ser consideravelmente minimizado caso as companhias investissem em um treinamento de segurança cibernética de qualidade aos seus funcionários e usuários.

Outra grande falha dos bancos tradicionais é não investir devidamente em profissionais especializados em cibersegurança. Esses trabalhadores que tratam especificamente de tornar a empresa cumpridora das regulamentações voltadas à segurança cibernética[227], e como se pôde constatar ao longo desse estudo, não são poucas, e são de extrema relevância para a manutenção dos princípios e pilares do tema. E não só, como também são eles os responsáveis por estarem atualizados sobre as atuais ameaças, as técnicas de defesa, sendo necessária a constante atenção às rápidas mudanças que ocorrem nesta área. Mesmo com as melhores tecnologias, não tendo

---

[222] Owaida, Amer. Segurança cibernética no setor financeiro: riscos e desafios. 2021. Disponível em: https://www.welivesecurity.com/br/2021/03/26/seguranca-cibernetica-no-setor-financeiro-riscos-e-desafios/ . Acedido em: 10.10.2023.

[223] Winnefeld, J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. Harvard Business Review, 86–95. Disponível em: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-hepentagon?fbclid=IwAR2zPlzFapkpG9k3pogjhRs5E0oYmOoKheERpwxAbPKUVtKCHUK-KkK97Rk . Acedido em: 10.10.2023

[224] Siota, Wendel. O Custo do Erro Humano para a Cibersegurança. 2022. Disponível em: . Acedido em: 11.10.2023.

[225] "O Instituto Ponemon foi criado em 2002 pelo Dr. Larry Ponemon e Susan Jayson. É uma organização de dicada a dois princípios: estudar questões de segurança e privacidade da informação e educar as pessoas sobre esses resultados e suas implicações. É uma organização independente dedicada ao estudo objetivo e à coleta de dados para apresentá-los sem preconceitos ou agendas. Por outras palavras, o Instituto Ponemon estuda questões de segurança cibernética e privacidade e depois preserva fielmente os dados adquiridos nesses estudos." (tradução nossa). Disponível em: https://noknok.com/what-is-the-ponemon-institute/ .

[226] Irwin, Luke. The cost of a cyber attack in 2021. 2021. Disponível em: https://www.itgovernance.co.uk/blog/the-cost-of-a-cyber-attack . Acedido em: 14.10.2023.

[227] Martinelli, Cláudio. Profissionais de cibersegurança nunca foram tão necessários e o futuro é ainda mais promissor. 2020. Disponível em: .

uma equipa adequada, não será possível manter uma segurança adequada[228].

Esses profissionais são escassos no mercado de trabalho, e uma grande solução que os bancos poderiam implementar para estarem um passo à frente na cibersegurança é investir em treinamento para trabalhadores internos de tecnologia da informação com o intuito de criar uma excelente equipa ness e setor. Conforme a empresa norte americana *cybersecurity ventures* [229], que realiza pesquisas sobre cibersegurança, constatou que os cargos de cibersegurança por preencher atingirão os 3,5 milhões este ano, 2023, mundialmente[230].

Os bancos devem aumentar seus investimentos na segurança cibernética, especialmente no treinamento de seus trabalhadores e cliente, e em bons profissionais especializados na área, O futuro está em garantir da melhor forma possível a cibersegurança e, assim, manter a confiança dos seus clientes e se desenvolver juntamente com o mundo digital que está cada vez mais presente no dia a dia da população mundial.

[228] Entrevista com Pedro Rodrigues, Ciso do Banco de Portugal. Revista IT Security – 14 de outubro de 2023.
[229] https://cybersecurityventures.com/our-company/
[230] Analysis. Como colmatar a falta de profissionais de TI com uma solução SASE. 2023.

Conclusão

Como já mencionado ao longo deste trabalho, nas últimas duas décadas houve uma imensa evolução na tecnologia. Essa nova realidade mudou a vida das pessoas. E vem mudando a forma como a sociedade funciona.

Atualmente um criminoso pode não ser mais reconhecido na rua, ele não tem rosto, apenas um *IP*. As fronteiras já conhecidas estão tomando outras proporções, as competências territoriais tão debatidas e definidas no âmbito jurídico começam a ser revistas [231]. Não é mais possível ver o direito da mesma forma quando se fala de tecnologia, é preciso compreender a realidade virtual, como ela funciona, como os agentes do crime agem e quem eles são.

Este estudo analisou os crimes que mais ocorrem dentro do setor bancário que, como pode se ver ao longo dele, é uma das áreas mais vulneráveis e que presta um serviço essencial à sociedade. É constatado ao longo deste trabalho que a engenharia social é um dos ataques mais utilizadas pelos cibercriminosos visto que o fator humano é o mais frágil de todo esse sistema. O *phishing* nem sempre possui uma grande tecnologia por trás, e sim um indivíduo que através de burla se aproveita da ingenuidade, curiosidade e/ou fragilidade do ser hum ano. Mas é claro, às vezes existem tecnologias avançadas dentro deles que rapidamente se espalham por máquinas pelo mundo inteiro, como foi possível ver com o *WannaCry* e o *Notpetya*, *malwares* muito bem desenvolvidos, com uma capacidade de disseminação extremamente veloz.

A Convenção de Budapeste foi um importante marco quando se fala em cibersegurança, logo após, e em consequência disso, surge a inovadora Lei do Cibercrime em Portugal, que passa a tratar especificamente dos crimes informáticos, e que preenche lacunas no ordenamento jurídico que se encontravam latentes, com o intuito de resolver a impunidade dos crimes cibernéticos. A análise dos artigos da referida lei foi realizada tendo em consideração o setor bancário e os crimes que mais o atingem, para depois analisar a regulamentação sobre cibersegurança que são de extrema relevância para a prevenção dos ataques, assim como para conter cenários de crise, quando os ataques são realizados. Entretanto a Lei do Cibercrime não consegue resolver um dos grandes problemas do combate à cibercriminalidade, que é a forma transnacional que o cibercrime se concretiza. Para isso será necessário um esforço conjunto das nações.

[231] Verdelho, Pedro. Phishing e outras formas de defraudação nas redes de comunicação. In Direito da Sociedade da Informação – Vol. VIII, Associação Portuguesa do Direito Intelectual. Coimbra Editora, 2009

Um grande exemplo do despreparo mundial ao enfrentamento do cibercrime é o ataque *NotPetya*, que culminou numa série de medidas com o intuito de melhorar a proteção e a resposta a essas situações. As providências que vêm sendo tomadas não parecem ser suficientes para evitar outro grande ato criminoso com o esse. Os cibercriminosos desenvolvem formas cada vez mais criativas de ataque, e a prevenção contra crimes iguais aos que já se passaram não será o bastante, pois o próximo provavelmente será de maior dimensão. Isso já é alvo de debate entre os profissionais de cibersegurança, que concluem que o que poderá vir terá proporções catastróficas. O cumprimento das Diretivas e regulamentos emitidas pela União Europeia e por Portugal, se fazem essenciais para uma melhor proteção das entidades bancárias, assim como mantém a confiabilidade, característica tão importante para esse setor. Como exemplo neste estudo foi visto o ataque ao BancoEstado, que parou por dias o funcionamento dele. A existência de uma simples vulnerabilidade em uma rede de computadores permitiu aos cibercriminosos adentrar todo ciberespaço da entidade, o que provavelmente teria sido evitado com uma simples atualização do sistema.

A União Europeia criou diversas entidades para auxiliar os Estados-Membros a se prevenir e a conter os ciberataques, e a partir daí Portugal criou o seu próprio organismo. A Diretiva SRI ganhou forte destaque, pois orientou os Estados -Membros a criarem uma Estratégia Nacional de Segurança das Redes e dos Sistemas de Informação para a definição de objetivos estratégicos e medidas políticas e regulamentares para atingir um elevado nível de segurança das redes e dos sistemas de informação, ela auxilia, fornecendo um plano estruturado, coordenado e abrangente para enfrentar ameaças cibernéticas, promovendo a segurança, estabilidade e confiança em questões de cibersegurança.

Além das orientações e normas estatais que os bancos devem seguir, eles utilizam boas práticas de conduta, como explicado, as mais utilizadas no mundo são as ISO's e a NIST. O uso dessas orientações ajuda os bancos a estabelecerem uma base sólida para a proteção dos dados financeiros e a realizar uma gestão eficaz dos riscos de cibersegurança. Dessa forma, se protege melhor a tríade CIA (confidencialidade, integridade e disponibilidade), mantendo os princípios fundamentais que a sociedade espera de um banco.

Os ciberataques evoluem rapidamente, os *crackers* nem sempre são indivíduos amadores que estão se aventurando no crime cibernético, e sim especialistas em tecnologia da informação e que usam seus vastos conhecimentos para obter benefícios próprios. Dessa forma, une-se ao fator de risco, o elemento surpresa, as entidades bancárias, assim como qualquer organização do

mundo, nem sempre sabem o que irá se apresentar nesses ataques. É importante que estejam sempre atentos às vulnerabilidades dos seus sistemas, e também dos seus trabalhadores e usuários. Manuel Castells, ilustre sociólogo espanhol, disse em entrevista [232] que "um país educado com internet progride; um país sem educação usa a internet para fazer "estupidez"", utilizando esse pensamento para a realidade deste trabalho, uma equipa sem uma preparação eficaz é uma porta aberta para o cibercrime, assim como usuários sem literacia digital realmente adequada.

A sociedade está a dar os primeiros passos para conviver com o fenómeno da tecnologia, as entidades bancárias estão um passo a frente, contudo ainda há muito caminho a ser percorrido. Os bancos devem manter uma postura de vigilância constante, devem estar atualizados em relação às ameaças emergentes e continuar aprimorando suas medidas de segurança cibernética, para que quando ocorram novos cibercrimes eles estejam preparados para minimizar os seus efeitos e proteger os seus usuários. A União Europeia e Portugal vêm fazendo um ótimo trabalho de cooperação com os bancos, o que é fundamental para a rapidez e eficácia das respostas às ameaças cibernéticas.

[232] https://gauchazh.clicrbs.com.br/geral/noticia/2015/05/manuel-castells-um-pais-educado-com-internet-progride-um-pais-sem-educacao-usa-a-internet-para-fazer-estupidez-4762 171 .html

Bibliografia

AGUILAR, Amanda Albuquerque. Responsabilidade civil dos bancos nos casos de danos e fraudes causados por hackers. Manaus: UEA, 2017.

ALENCAR, Gliner; LIMA, Marcelo de; FIRMO, André. O Efeito da Conscientização de Usuários no Meio Corporativo no Com bate à Engenharia Social e Phishing. In: SIMPÓSIO BRASILEIRO DE SISTEMAS DE INFORMAÇÃO (SBSI), 9. , 2013, João Pessoa. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2013. p. 254-259. DOI: https://doi.org/10.5753/sbsi.2013.5694.

ALSUWAT, Emad S; AL-Otaibi, Abeer F.; *A study on social engineering attacks: phishing attack. International Journal of Recent Advances in Multidisciplinary Research* Vol. 07. 2020.

ANDRADE, Francisco Pacheco de, FONSECA, Isabel, SILVA, Joana Aguiar e, ABREU, Joana Covelo de, JERÓNIMO, Patrícia, VENÂNCIO, Pedro Dias, e FREITAS, Pedro Miguel, Relatório Cibersegurança em Portugal: Ética & Direito, Braga, JusGov e CNCS, 2020

Aras, Vladimir. Crimes de informática.: Uma nova criminalidade. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51. 2001. Disponível em: https://jus.com.br/artigos/2250. Acesso em: 7 ago. 2023.

ASCENSÃO, José de Oliveira. Estudos sobre o Direito da Internet e da Sociedade de Informação. Almedina, 2001.

BARBOSA, Maria Luís. As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal. JANUS.NET, e-journal of International Relations. Vol. 11, Nº.1. 2020.

BARROS, Gabriel Osório. A Cibersegurança em Portugal. Gabinete de Estratégia e Estudos. 2018.

BRITO, Paulo. Banco chileno atingido por ransomware: 12 mil computadores congelados. Disponível em: https://www.cisoadvisor.com.br/banco-chileno-atingido-por-ransomware-12- mil-computadores-congelados/ Acedido em: 01/08/2023

BRITO, Paulo. Ataque à Ucrânia pode repetir caos global de 2017. 2022. Disponível em: https://www.cisoadvisor.com.br/ataque-a-ucrania-pode-repetir-caos-global-de-2017/. Acedido em:10.11.2023

CAETANO, Edgar. É "uma inevitabilidade" que haja um grande ataque cibernético a bancos. Disponível em: https://observador.pt/2022/05/02/e-uma-inevitabilidade-que-haja-um-

grande-ataque-cibernetico-a-bancos/ . Acedido em 30/07/2023.

CASTELLS, Manuel. A Era da Informação: Economia, Sociedade e Cultura, Vol. I A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian, 2005.

CAMILO, Evandro. Blockchain: uma nova forma de pensar em cybersecurity. Report • Cyber Tech. 2021. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report2 -distrito.pdf Acedido em: 27.09.2023

CANCELA, Alberto Gil Lima. A prova digital: os meios de obtenção de prova na lei do cibercrime. Diss. Universidade de Coimbra (Portugal), 2016.

CASEY, Eoghan. Digital Evidence and Computer Crime, Digital Evidence and Computer Crime – Forensic Science, Computers and the Internet, 3.ª edição, Califórnia: Elsevier, 2011.

CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. Desafios do direito penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos. 2012.

COUTINHO, Emanuel. Sousa, Flávio. Gomes, Danielo. Souza, Jose. (2013). Elasticidade em Computação na Nuvem: Uma Abordagem Sistemática.

CHRISTOU, George. The collective securitisation of cyberspace in the European Union. West European Politics. 2019.

DAMATTO, Felipe César; Rall, Ricardo. "Estudo dos possíveis motivos do aumento de incidentes de malwares nas empresas." tekhne e logos, 2011.

DIAS, Carlos Luís Soares. Com putação em nuvem. 2013.

DIAS, Jorge de Figueiredo. Direito Penal: parte geral. Tomo I. 1. ed. brasileira. 2. ed. portuguesa. Coimbra: Coimbra Editora. 2007.

DIAS, Pedro Simões / MARQUES, J. A. Garcia / MARTINS, A. G. Lourenço, Cyberlaw em Portugal. O Direito das Tecnologias da Informação e Comunicação, Centro Atlântico, Lisboa, 2004;

DIAS, Pedro Simões, O "Hacking" enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito, in Direito da Sociedade da

Informação, vol. VIII. Coimbra Editora, 2009.

DIAS, Vera Marques. "A problemática da investigação do cibercrime". DataVenia, revista jurídica digital. Ed. nº 1. 2012. Disponível em: https://www.datavenia.pt/ficheiros/edicao01/datavenia01_p063 -088.pdf Acedido em: 10 de set. 2023.

DRESCHER, Daniel. Blockchain Básico: uma introdução não técnica em 25 passos. Novatec Editora, 2018.

DUNN, Myriam. A Resilient Europe for an Open, Safe and Secure Cyberspace. UI Occassional Papers. Suécia. N° 23. 2013.

ESTRADA, Manuel Martin Pino. Internet Banking no Brasil, na América Latina e na Europa. Disponível em http://www.publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161. Acedido em 10/8/2023

FACHINELLI, Mateus. Ahlert, Edson Moacir. Firewall de próxima geração-fortinet. Revista Destaques Acadêmicos. 2019.

FARIA, Duarte Lynce de. "O impacto da cibersegurança no quadro jurídico regulatório da segurança marítima". In Janus.net, e-journal of international relations. Vol. 11, Nº 2Consultado [online] em data da última consulta, DOI: https://doi.org/10.26619/1647-7251.11.2.10. 2020.

FARIA, Nelson Correia. Estratégia de cibersegurança. Diss. 2022.

FARIA, Thiago Stefanini. Técnica phishing: simples, mas eficaz. 2017.

FERNANDES, Cláudio. "Máquina Enigma"; Brasil Escola. 2023.

Fernandes, Filipe S. Cibersegurança no setor financeiro: os perigos e consequências dos ataques cibernéticos em instituições financeiras. 2020. Disponível em: https://www.jornaldenegocios.pt/negocios-iniciativas/banca-do-futuro/detalhe/ciberseguranca-e-tema-na-gestao-de-topo . Acedido em: 27.09.2023.

FERNANDES, Filipe S.. Cibersegurança é tema na gestão de topo. 2020. Disponível em: https://www.jornaldenegocios.pt/negocios-iniciativas/banca-do-futuro/detalhe/ciberseguranca-e-tema-na-gestao-de-topo . Acedido em: 25.09.2023.

FERREIRA, Haroldo. Cibersegurança. Editora Senac São Paulo, 2021.

FORNASIER, Mateus de Oliveira; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista Thesis Juris, 2020.

GALOYAN, Albert. Segurança cibernética no âmbito das relações internacionais. 2019.

GARCIA, Bruno. Informação e Segurança no Ciberespaço: A influência da globalização na intensificação de riscos e ameaças na última década. Public Sciences & Policies 7.1: 193 -212. 2021.

GARCIA, Paulo. Que tendências estão a moldar o futuro da banca?. Disponível em: https://observador.pt/opiniao/que-tendencias-estao-a-moldar-o-futuro-da-banca/ Acedido em: 25.09.2023

GETO, Daniel. "Banco Europeu de Investimento alvo de ataque informático DDoS". Disponível em: https://www.menosfios.com/banco-europeu-de-investimento-alvo-de-ataque-informatico-ddos/ Acedido em: 30/07/2023

GONÇALVE S, Paula Filipa Trilho. Os Novos Desafios à cibersegurança na União Europeia em tempos de pandemia Covid19: De que forma a pandemia Covid19 veio alterar a cibersegurança na União Europeia, no período compreendido entre Março 2020-Março 2021. 2022.

GOUVEIA, Jorge Bacelar. Direito do Ciberespaço e Segurança Cibernética. Revista Jurídica Portucalense. 2021.

GOUVEIA, Luís Borges. Estratégia Nacional de Segurança do Ciberespaço. Tecnologia, redes e sociedade. 2017.

GRAÇA, Douglas Cordeiro da. Souza, Rodrigo Vieira de. Ransom wares: uma ameaça crescente. 2020.

GUEDES, Inês Sousa. Cibercriminalidade: novos desafios, ofensas e soluções. Lisboa: Pactor, 2021.

GUTSALYUK, Mykhaylo V.; KLYMENKO, Olga A. Combate à criminalidade cibernética e garantias de segurança cibernética na Ucrânia. 2017.

HERMENEGILDO, Gabriella França. Cibersegurança na União Europeia e os Desafios para a sua Eficácia: Perspetivas, Panorama Estratégico e Instrumentos Jurídicos. Faculdade de Direito

da Universidade do Porto, Porto, 2020.

HINTZBERGEN, Jule. HINTZBERGEN, Kees. SMULDERS, André. BAARS, Hans. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 3ª. ed. Rio de Janeiro: Brasport, 2018.

HOBSBAWM, E. J. Era dos extremos: o breve século XX: 1914 - 1991. 2. ed. São Paulo: Companhia das Letras

INACARATO, Flávio. Hackers, Crackers e nova modalidade de crime virtual – Ransom ware, e a Responsabilidade nos Crimes Eletrônicos. 2017.

IRWIN, Luke. The cost of a cyber attack in 2021. 2021. Disponível em: https://www.itgovernance.co.uk/blog/the-cost-of-a-cyber-attack . Acedido em: 14.10.2023.

K., Umamaheswari, Impacts of Cyber Crime on Internet Banking (March 5, 2021). International Journal of Engineering Technology and Management Sciences, Disponível: https://ssrn.com/abstract=3939579 or http://dx.doi.org/10.2139/ssrn.3939579

KAHN, D. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.1996.

KENNEDY, William. Olmsted, Aspen. Three factor authentication. In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). 2017. Disponível em: http://www.icitst.org/Proceedings/ICITST-2017-Proceedings.pdf . Acedido em: 01.10.2023.

KHATRI, Prem. The importance of cyber security in banking. 2019. Disponível em: https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/ . Acedido em: 25.09.2023.

KOZLOW SKA, I. Facebook and Data Privacy in the Age of Cambridge Analytica. Seatlle: Henry M. Jackson School of International Studies; College of Arts and Sciences; University of Washington, 2019.

KUROSE, James e Ross Keith; redes de computadores e a internet: Uma abordagem Top-down. 5ta. Brasil: Pearson, 2010.

LAS-CASAS, Pedro Henrique B., et al. Uma metodologia para identificação adaptativa e caracterização de phishing. In: Proc. of Brazilian Symposium on Computer Networks and Distributed Systems (SBRC). 2016.

LEITE, Ana Marta Xavier Ferreira. A problemática da cibersegurança e os seus desafios. CEDIS

Working Papers. Direito, Segurança e Democracia. ISSN 2184-0776. Nº 49. 2016.

LEITE, Monteiro Luciano. Políticas de segurança física e lógica de tecnologia da informação em redes de computadores e seus ativos. 2018.

LEMOS, André. Cultura da mobilidade. Revista Famecos. 2009.

LEMOS II, Dalton Luiz. Tecnologia da informação / Dalton Luiz Lemos II. – 2. ed. – Florianópolis : Publicações do IF-SC, 2011.

LEVY, Pierre, A Inteligência Colectiva - Por uma Antropologia do Ciberespaço, Loyola, São Paulo, 1998.

LISKA, Allan; GALLO, Timothy. Ransomware: defendendo -se da extorsão digital. Novatec Editora, 2019.

MACHADO, Felipe Nery Rodrigues, Segurança da Informação: Princípios e controle de ameaças. 1ª ed. – São Paulo: Érica, 2014.

MACHADO, Thiago. Cibercrime e o crime no mundo informático A especial vulnerabilidade das crianças e dos adolescentes. Porto, 2017.

MAGALHÃES, Pedro M. Requisitos e recomendações para o desenvolvimento e operação de um SGSI–Abordagem com ISO 27001/27002. 2021.

MARTINELLI, Cláudio. Profissionais de cibersegurança nunca foram tão necessários e o futuro é ainda mais promissor. 2020. Disponível em: . Acedido em: 19.10.2023.

MARQUES, Daniela Filipa Guerreiro. Os Efeitos da Globalização e Das Novas Tecnologias No Jornal de Letras, Artes e Ideias-Uma Análise Geral. Diss. Universidade de Lisboa (Portugal), 2016.

MATOS, Pedro Carvalhais de Abreu. Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas. 2018.

MELO, Laerte Peotta, et al. "Análise de malware: Investigaçao de códigos maliciosos através de uma abordagem prática." Sociedade Brasileira de Computação (2011).

MESQUITA, Tiago António Cabanelas. Soluções Single Sign On em software de uso livre. 2010.

MILLION, August. The NotPetya fallout continues, with global transport and logistics conglomerate Maersk reporting up to $300 million in losses following a June cyber attack. 2017. Disponível em: https://www.digitalguardian.com/blog/cost-malware-infection-maersk-300-
million#:~:text=The%20NotPetya%20fallout%20continues%2C%20with,compromise%20by%20t he %20NotPetya%20malware.

MIRANDA, Cláudio Zumpichiatte. Auditoria de Segurança da Informação nos Órgãos da Administração Pública: Maturidade, Com pliance e Boas Práticas. .Distrito Federal. 2017.

MITNICK, Kevin e Simon, William L. A Arte de Enganar. São Paulo: Blucher, 2003.

MORAES, Alexandre Fernandes de. Cibersegurança e a nova geração de Firewalls. Saraiva Educação SA, 2021.

MORETTI, Cláudio dos Santos. A importância da informação. Revista Gestão de Riscos – 147 ed. – São Paulo, 2020.

NEIRA, Anderson Bergamini; KANTARCI, Burak; NOGUEIRA, Michele. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Com puter Networks, 2023

NEVES, Raquel Alexandra Carvalho. Vitimação por phishing: um estudo empírico. 2022.

NEUTEL, Hugo. "BCP alvo de ciberataque. Situação já a normalizar, diz banco" Disponível em: https://www.jornaldenegocios.pt/empresas/banca---financas/detalhe/bcp-alvo-de-ciberataque-situacao-ja-a-normalizar-diz-banco Acedido em: 30/07/2023

NOVET, Jordan. Shipping company Maersk says June cyberattack could cost it up to $300

NUNES, Duarte Alberto Rodrigues. O crime de falsidade informática. Revista Julgar. Outubro 2017.

OLIVEIRA, Jéssica. Ransomware - Laboratório de Ataque do WannaCry – Brasília, DF, 30 de novembro de 2018

OLIVEIRA, Raquel. Eduardo, Izycki. Propaganda computacional na prática: os casos de Estados Unidos, França e Venezuela. 2021.

OWAIDA, Amer. Segurança cibernética no setor financeiro: riscos e desafios. 2021. Disponível em: https://www.welivesecurity.com/br/2021/03/26/seguranca -cibernetica-no-setor-

financeiro-riscos-e-desafios/ . Acedido em: 10.10.2023.

PASCHOAL, Dener Aparecido Caldeira; Pereira, Guilherme Fontes. Segurança da informação na indústria 4.0: framework NIST. 2019.

PASTILHA, Élton Carpinteiro. Autenticação fido2 em dispositivos android. 2022.

PEREIRA, Daniel. A Onipresença da Internet versus a Privacidade Individual: Uma batalha injusta. Novembro de 2019.

PEREIRA, João Pedro Carvalhosa. A nova tecnologia 5G e a cibersegurança–Perceção dos impactos nas organizações e dos desafios para os auditores. 2022.

PERLROTH, Nicole. Cyberattack Hits Ukraine Then Spreads Internationally. 2017. Disponível em: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html . Acedido em: 10.11.2023

PINTO, Filipa Couto Astorga Batista. Enquadramento técnico-jurídico da segurança do ciberespaço. Diss. 2019.

PINTO, Walker Douglas Garcia. Cibersegurança. Seminário de tecnologia gestão e educação. 2020.

QUISPE, Carlos Alberto Flores. Tipos de Hackers. Universidad Mayor de San Andrés, 2009.

REVOREDO, Tatiana. Segurança cibernética de blockchains e protocolos de consenso: Como blockchain supera as adversidades da cibersegurança?. 2021. Disponível em: https://mittechreview.com.br/seguranca-cibernetica-de-blockchains-e-protocolos-de-consenso/. Acedido em: 27.09.2023.

RIBEIRO, Maria da Conceição Fernandes. Cibercrime e prova digital. 2015.

RODRIGUES, Benjamim Silva. "Direito Penal – Parte Especial I, Direito Penal Informático-Digital" Coimbra. 2009.

ROSALINO, Hélder. "Cibersegurança no sistema financeiro: riscos, cooperação e governação". 2017.

SALDANH A, Ana Beatriz Martins. Gestão de Dados em Cidades Inteligentes. 2022.

SANDIM, Miguel. Ribeiro, Susana. Realidade Virtual e Interatividade. Póvoa do Varzim. 2011.

SANTOS, Plácida Leopoldina da Costa. Vidotti, Silvana. "Quando as webs se encontram: social e semântica-promessa de uma visão realizada.". 2009.

SÊMOLA, Marcos, "Gestão da segurança da informação: uma visão executiva" 2. ed. – Rio de Janeiro: Elsevier, 2014.

SERRANO, Inês Isabel Baião. Cibersegurança na União Europeia: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos. MS thesis. Universidade de Évora, 2022.

SILVA, Bruna Patrícia Ribeiro Alves da. Planeamento e implementação de um sistema de gestão da segurança da informação. Porto. 2011.

SILVA, Michel Bernardo Fernandes da. Cibersegurança: Visão Panorâmica Sobre a Segurança da Informação na Internet. Freitas Bastos, 2023.

SILVA, Pedro Miguel Lopes Martins da. Gestão de cibersegurança em organizações financeiras. MS thesis. 2018.

SIMAS, Diana Viveiros. O cibercrime. Dissertação de Mestrado, Universidade Lusófona de Humanidades e Tecnologias., Direito, Lisboa. 2014.

SINGH, S. The Code Book: The Science of Secrecy from Ancient Egypt to Quantu m Cryptography. 1999.

SIOTA, Wendel. O Custo do Erro Humano para a Cibersegurança. 2022. Disponível em: . Acedido em: 11.10.2023.

SOUSA, Flávio. Moreira, Leonardo. Machado, Javam. Computação em nuvem: Conceitos, tecnologias, aplicações e desafios. II Escola Regional de Com putação Ceará, Maranhão e Piauí (ERCEMAPI). 2009.

TAVARES, Pedro. Banco do Chile sofre ataque ransomware (REvil). 2020. Disponível em: https://seguranca-informatica.pt/banco-do-chile-sofre-ataque-ransomware-revil/ . Acedido em: 09.11.2023

TEIXEIRA, Cleyson Fernando Araújo. Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos. 2021.

TEIXEIRA, Maria Emília. Reis, Lara. A transformação digital na banca e a crescente relevância da resiliência operacional. Revista Electrónica de Direito. 2022

TEIXEIRA, Paulo Alexandre Gonçalves. O fenómeno do phishing enquadramento jurídico -penal. Camões - Repositório Institucional da Universidade Autónoma de Lisboa. 2013.

VENÂNCIO, Pedro Dias. Lei do Cibercrime - Anotada e Comentada. 1ª ed. 2011.

VENÂNCIO, Pedro Dias. "Tipos legais de crimes informáticos". "Criminalidade – Novos desafios, ofensas e soluções", Inês Guedes e Marcis Gomes (Coordenadores), PACTOR, Lda, 2021.

VENTRE, Daniel. O dilema da fronteira virtual: Quando os Estados se tornam construtores de ciberfronteiras. Dilemas, Rev. Estud. Conflito Controle Soc. – Rio de Janeiro – Edição Especial no 3 –2019

VENTURA, André. Noções de Direito Penal. 1ª ed. 2013.

VERDELHO, Pedro, "Phishing e outras formas de defraudação nas redes de comunicação", in Direito da Sociedade de Informação, Vol. VIII, Coimbra, 2009.

VERDELHO, Pedro. A nova Lei do Cibercrime, Lei n.º 109/2009. 2010.

VERDELHO, Pedro, Lei n.º 109/2009, de 15 de Setembro, in Comentário das leis penais extravagantes. 2010.

VIANNA, Eduardo Wallier. FERNANDES, Jorge Henrique Cabral. "O gestor da segurança da informação no espaço cibernético governamental: Grandes desafios, novos perfis e procedimentos." Brazilian Journal of Information Science 9.1 - 2015.

VIANNA, Túlio Lima. Hackers: um estudo criminológico da subcultura cyberpunk. Informática e internet: aspectos legais internacionais. ed. Rio de Janeiro : esplanada, 2001.

VIRGILIO, Flávio. Frameworks para Segurança da Informação. 2022.

VOLCHKOVA, Ekaterina. Sistema de gestão integrada de privacidade e segurança da informação : alinhamento com o regulamento geral sobre a proteção de dados. 2018.

WINNEFELD, J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. Harvard Business Review, 86–95. Disponível em: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-hepentagon?fbclid=IwAR2zPlzFapkpG9k3pogjhRs5E0oYmOoKheERpwxAbPKUVtKCHUK-KkK97Rk . Acedido em: 10.10.2023

Outros Documentos

Instrução nº 21/2019 - BO nº 11/2019 Suplemento • 2019/11/25. Banco de Portugal.

Ordem dos Psicólogos Portugueses (2021). Contributo Científico OPP – Projecto de Decreto-Lei sobre o Regime da Segurança do Ciberespaço e Obrigações de Certificação da Cibersegurança. Lisboa.