Universidade do Minho
Escola de Direito

Jean Carlos Jara De Freitas

A Proteção dos Dados Pessoais de Pagamento Utilizados no Comércio Eletrónico, em Portugal

Outubro 2018

A Proteção dos Dados Pessoais de Pagamento Utilizados no Comércio Eletrónico, em Portugal

Jean Carlos Jara De Freitas

UMinho | 2018

Universidade do Minho
Escola de Direito

Jean Carlos Jara De Freitas

A Proteção dos Dados Pessoais de Pagamento Utilizados no Comércio Eletrónico, em Portugal

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação da
Professora Doutora
Teresa Alexandra Coelho Moreira
e do
Professor Doutor
Vítor Francisco Mendes Freitas Gomes Fonte

Outubro 2018

DECLARAÇÃO

Nome

_____JEAN CARLOS JARA DE FREITAS_____

Endereço eletrónico: ___jeanjara@yahoo.com_____ Telefone: __+593 984721788 / _____

Número do Bilhete de Identidade: ___31079568_____

Título dissertação■ / tese □

A Proteção dos Dados Pessoais de Pagamento Utilizados no Comércio Eletrónico, em Portugal.

Orientador(es):

Professora Doutora Teresa Alexandra Coelho Moreira e o Professor Doutor Vítor Francisco Mendes Freitas Gomes Fonte_____

_____ Ano de conclusão: __2018_____

Designação do Mestrado ou do Ramo de Conhecimento do Doutoramento:

_____Mestrado em Direito e Informática_____

É AUTORIZADA A REPRODUÇÃO INTEGRAL DESTA TESE/TRABALHO APENAS PARA EFEITOS DE INVESTIGAÇÃO, MEDIANTE DECLARAÇÃO ESCRITA DO INTERESSADO, QUE A TAL SE COMPROMETE;

Universidade do Minho, _18__/_10__/__2018____

Assinatura: _____

AGRADECIMENTOS

Agradeço a Deus, por estar ao meu lado dando-me força e coragem para alcançar este objetivo.

A minha mãe, família e amigos pelo incentivo e por acreditar em mim nos momentos em que me dedicava a esta tarefa.

As minhas amigas e colegas Katy Fernandes e Bárbara Barbosa, a quem dedico a minha mais sentida gratidão, pelo aporte, colaboração e por todo o incondicional apoio demonstrado.

A minha sincera e profunda gratidão aos Professores Doutora Teresa Alexandra Coelho Moreira e Doutor Vítor Francisco Mendes Freitas Gomes Fonte, os quais me receberam e me levaram sem reservas ao longo desta jornada, com interesse e disponibilidade, brindando as suas sabedorias e valiosos contributos em todo este processo.

À célebre Universidade do Minho, o Coordenador do Mestrado de Direito e Informática, Professor Doutor Francisco António Carneiro Pacheco de Andrade e o Corpo Docente por ter contribuído à realização deste Mestrado.

À memória dos meus queridos avôs.

RESUMO

A dissertação Intitulada A PROTEÇÃO DOS DADOS PESSOAIS DE PAGAMENTO UTILIZADOS NO COMÉRCIO ELETRÓNICO, EM PORTUGAL, visa dilucidar aspetos essenciais a serem considerados para proteger os dados pessoais de pagamento à distância nas operações de comércio eletrónico (B2C), com o fim de evitar o seu uso não autorizado, assim como os crimes informáticos a eles relacionados, observando com precisão os aspetos técnicos e legais que contribuem à privacidade e a validez legal das transações comerciais pelos médios eletrónicos.

Desta forma, a presente pesquisa pretende encontrar repostas por um lado, nas atuais ferramentas tecnológicas que permitam brindar segurança no uso dos sistemas informáticos durante as operações do comércio eletrónico, assim como, estudar, avaliar e provir o entorno legal, considerando o ordenamento jurídico das Comunicações Eletrónicas, a Proteção dos Dados Pessoais, a Assinatura Eletrónica, o Comércio Eletrónico, a Identificação Eletrónica e os Serviços de Confiança nas Transações Eletrónicas, o Regime Jurídico de Pagamento em Moeda Eletrónica, e a normativa sobre os Crimes Informáticos. Ademais de considerar os acordos internacionais de integração relacionados com os elementos do estudo, e demais normas supranacionais, à vez de observar a legislação comparada.

Para isto, identificamos os elementos conceituais alusivos a dados pessoais, fazendo ênfase de aqueles que diz respeito às atividades de pagamentos à distância. Em seguida, justificamos a importância da privacidade desde sua origem nacional e internacional, e os riscos que estão expostos os dados pessoais ao estar numa rede informática. Depois, evidenciamos a proteção de dados pessoais no âmbito legal, ou seja, a tutela jurídica, e continuamos a identificar os direitos que tem o titular dos dados, estabelecendo o quadro jurídico integral, que levo à identificação de conceitos e mecanismos técnicos relacionados com a ciência da informática e as ações que no âmbito tecnológico seriam possíveis fomentar para uma proteção preventiva.

Assim foi possível estabelecer as relações dos dados pessoais de pagamento com as operações de comércio eletrónico e a sua relevância patrimonial, que é o principal interesse dos criminosos, para o qual foi necessário identificar as características, as causas, as consequências e a classificação dos crimes informáticos, assim como os atos típicos e penalidades, reconhecendo os tipos penais onde os dados pessoais de pagamento, são o fim ou o meio do ato criminoso, ou os elementos ou objetos que causam danos patrimoniais.

Isso nos levou a tomar em conta as desvantagens contempladas pela regulamentação, concluindo com a importância das provas digitais na investigação criminal, a eficácia probatória delas e a sua apresentação nos processos judiciais.

Desta forma, foi possível demostrar o tratamento legal que têm os dados pessoais de pagamento em Portugal, permitindo fazer uma reflexão para a análise da proteção destes dados, diferenciando os comportamento criminosos que causam graves danos materiais através do seu uso ilegal, e a partir disto, ponderar as ações técnicas que possam impedir tal conduta, à vez de demonstrar os diferentes direitos que possam ser exercidos pelo titular dos dados, para a segurança, e o fortalecimento da confiança dos usuários nas operações de comércio eletrónico.

ABSTRACT

The thesis entitled *THE PROTECTION OF DATA PERSONAL OF PAYMENT IN THE E-COMMERCE, IN PORTUGAL*, seeks to elucidate key aspects to be considered to protect the personal data of payment to the distance (B2C) e-commerce operations, with the to avoid un authorized use, as well ascomputer crimes related to them, noting precisely the technical and legal aspects contributing to the privacy and the legal validity of commercial transactions by electronic means.

Thus, this research aims to find on the one hand, the current technological tools that allow to provide security in the use of computer systems for e-commerce operations as well asto study, appreciate and provide the legal environment, whereas the legal system of electronic communications, personal data protection, electronic signatures, electronic commerce, electronic identification and trust services in transactions Electronic, the legal regime of electronic currency payments, and the rules on the computer crimes. In addition to considering integration international agreements related to the elements of study and other supranational rules, at the same time observe comparative legislation.

For this, we identified the conceptual elements alluding topersonal data, emphasizing those who say about distance payment activities. Then, we justify privacy and intimacy from its national and international origin, and risks that exposed the personal data to be in a computer network. Then we showed the data protection in the legal sphere, i.e., legal guardian ship, and continue to identify concepts and technical mechanisms related to the science of Informatic sand the actions that would be possible to promote in field of technology for a preventive protection.

Thus it was possible to establish the relations of personal payment data with e-commerce operations and its patrimonial relevance, which is the main interest of the criminals, which was necessary to identify the characteristics, causes, the consequences and the classification of computercrimes, as well as its typical acts and sanctions, recognizing the criminal types where the personal data of payment are the end or the Middle Act criminal, or elements or objects that cause economic damage.

That led us to take into account the disadvantages referred to by the regulation, concluding with the importance of digital evidence in criminal investigation and preliminary efficacy and presentation in judicial processes.

In this way, it was possible to demonstrate the legal treatment that has the personal data of payment in Portugal, allowing to make a reflection for the analysis of the protection of these data, differentiating criminal behaviour, causing serious material damage through its illegal use, and from this, ponder the technical actions that can prevent such conduct, at the same time demonstrate the different rights that can be exercised by the owner of the data, for security and the fortifications of the confidence of the user IOS in thee-commerce operations.

CONTEÚDO

ABREVIATURAS

As listas de abreviaturas, de siglas, ou de símbolos:

Ac.	Acordo
ANACOM	Autoridade Nacional de Comunicações
art.º	artigo
arts.º	artigos
ASAE	Autoridade de Segurança Alimentar e Económica
B2C	*Business to Consumer* (Comerciante para o Consumidor)
CC	Código Civil
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CEDH	Convenção Europeia dos Direitos do Homem
Cit.	Citada
COTS	(*Commercial Off The Shelf*) (comerciais de prateleira)
CP	Código Penal Português
CPP	Código de Processo Penal de Portugal
CRP	CONSTITUICÃO DA REPUBLICA PORTUGUESA
DL	Decreto-Lei
DSPII	Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015**,** relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE, e regula o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, bem como o acesso à atividade das instituições de moeda eletrónica e a prestação de serviços de emissão de moeda eletrónica.
EU	União Europeia
EUA	Estados Unidos da América
LCElec	Lei de Comércio Eletrónico, Assinaturas Eletrónicas e Mensagens de Dados do Equador.
LCI	Lei da Criminalidade Informática - Lei N.º 109/91 De 17 De Agosto
LPDP	Lei n.º 67/98 de Proteção Dados Pessoais
N.º, n.º, núm.	Número
OCDE	Organização para Cooperação e Desenvolvimento Económico
ONU	Organização das Nações Unidas
P., p.	Página
RGPD	REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)
SANS	*SysAdmin Audit, Networking and Security* Institute
TEDH	Tribunal Europeu dos Direitos do Homem
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC´s	Tenologias das informações e as comunicações
TJUE	Tribunal de Justiça da União Europeia.
TRP	Tribunal da Relação do Porto
TUE	Tratado da União Europeia

Modo de citar e outras convenções

No âmbito da normalização de referências bibliográficas o presente trabalho considera as referências bibliográficas de acordo com a norma portuguesa NP 405.

Citação em nota de rodapé ou de fim: a primeira citação de cada obra ou artigo é feita pelo(s) nome(s) do(s) autor(es) e o título completo (sem complemento do título), tais como são dados na referência bibliográfica, seguidos, caso seja necessário, das páginas citadas. As citações seguintes são feitas com referência ao nome do autor, **op. cit.,** e página citada. Se forem citadas duas obras redigidas pelo mesmo autor a segunda citação e seguintes serão feitas com referência ao nome do mesmo, parte do título da obra ou artigo, cit. e página citada.

A bibliografia está ordenada por ordem alfabética do último apelido de cada um dos autores. Se o autor for espanhol, referem-se os dois últimos apelidos.

Quando a autoria for da responsabilidade de até três autores, todos serão referenciados no cabeçalho da referência.

Quando a autoria for da responsabilidade de quatro ou mais autores, indica-se apenas o nome do primeiro, seguido da abreviatura **et al.**

No caso de obras colectivas com indicação do nome do editor literário, compilador, organizador ou director, deve indicar-se o nome do editor ou compilador, seguido da expressão adequada:
ed. ou **eds, org.**, ou **dir.**, conforme o caso.

INTRODUÇÃO

Graças à tecnologia das redes informáticas como a Internet[1], a qual teve a sua origem nos anos de 1960[2] com ARPANET, hoje vivemos na era digital, onde grande parte da humanidade está ligada a ela, demandando constantemente os seus serviços, pela ajuda na simplificação das atividades que o homem realiza, ao tempo que as faz mais dinâmicas, promovendo o desenvolvimento tecnológico, novos mercados, mais postos de trabalho, custos de transação reduzidos e grandes benefícios gerais para os indivíduos, as empresas, as indústrias, os Estados e a sociedade em geral.

Inicialmente, as aplicações através da Internet limitavam-se às pesquisas, preenchimento de formulários e envio de correios eletrónicos, entre outros, mas gradualmente surgiram novas ferramentas que permitiram uma maior interação com os sistemas existentes, tais como bancos de dados e sistemas de cobro por cartão bancário. Neste contexto, a Internet tornou-se um serviço global, principalmente a partir dos anos noventa, quando o Departamento de Defesa dos Estados Unidos da América do Norte (NSFNET) consentiu o uso da Internet para fins comerciais.

Isto somado ao surgimento da *World Wide Web* (WWW[3]) ou simplesmente *Web*, que pode entender-se como uma tecnologia informática com base num conjunto de protocolos que possibilitam a ativação e disponibilização de aplicações na Internet, permitiram atingir milhões de pessoas em todo o mundo[4], contribuindo entre outras atividades, a promoção do comércio eletrónico.

Fundado em isso, denotou-se nas áreas de *resorts*, companhias aéreas e instituições financeiras pelos benefícios na redução de intermediação em cada operação, bem como um menor tempo e custo de processamento, apontando-se como uma opção de eficiência no mercado, onde as empresas mais ousadas tardaram pouco em aproveitá-la para oferecer os seus produtos; Depois surgiram os "*shoppings virtuais"*, onde um fornecedor colocava toda a infraestrutura tecnológica para criar uma loja virtual e

---

[1] O termo deriva da expressão "*Interconection betwens computer network*" interação entre computadores. (BARBIERI, Diovanna – A PROTEÇÃO DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO)

[2] KUROSE, James e ROSS Keith; REDES DE COMPUTADORES E A INTERNET: p.45

[3] WWW por Tim Berners-Lee

[4] KUROSE, James e ROSS Keith - op. cit., p.48

alugar *espaços* virtuais para vários concorrentes interessados em vender produtos *on-line,* de modo que muitas empresas começaram a implantar sistemas operacionais baseados em formatos eletrónicos, mas sem um suporte tecnológico e jurídico eficaz que lhes permitisse lidar com sucesso os problemas relacionados com o roubo de dados, enquanto é feita transferências de dados sensíveis através da Internet.

A partir de uma abordagem empresarial, vemos que a Internet tem agilizado a velocidade de operação no mundo dos negócios, para a compra de bens ou serviços através dela, no entanto, tem mostrado grandes riscos sobre o uso ilegítimo da informação que em ela é processado, pela interceção e/ou subtração indevida de dados pessoais, tais como os relacionados com os sistemas e processos de pagamentos por meio de cartões de crédito, códigos de acesso aos serviços de banca eletrónica, chave dos cartões, PIN, etc., com a intenção de afetar o património do seu titular, sendo feito por uma pessoa não autorizada que usa as debilidades do sistema virtual ou aproveita a ignorância dos usuários na gestão de sistemas de informação, para cometer novos atos criminosos que deram origem ao cibercrime.

É assim como se observa, que as reclamações nos órgãos de justiça de Portugal, os crimes contra o património mais comuns levados a cabo através da rede de Internet, estão principalmente relacionados com a extração de informações pessoais de dados de Pagamento, onde as práticas individuais ou combinada de técnicas tais como *fhishing, vishing, pharming, spoofing, spyware, Sniffers* verme *e-mails* maliciosos que ao ser lidos ou abertos num dispositivo computacional, descarregam vírus informáticos que são instalados automaticamente nos dispositivos das vítimas, com a intenção de gravar e enviar todos os movimentos que o usuário faz através da Internet, incluindo os seus dados pessoais.

O principal dano é de natureza patrimonial feito mediante o engano da vítima para obter como foi mencionado, os seus dados pessoais de pagamento produzindo grandes perdas económicas; Além disso, tem o roubo de identidade para criar contas falsas e o roubo de dados confidenciais das vítimas; também os atacantes podem impedir o acesso[5] da vítima a sua conta bancária, correio eletrónico ou serviços eletrónicos associados aos dados que a vítima forneceu.

[5]Ato que esta relacionado com o delito de Sabotagem informática, previsto no art.º 5 da Lei de Cibercrime. 109/2009

Num contexto global, entre os anos 2005 ao 2010, 10 milhões de pessoas foram vítimas de criminosos que abriram contas de cartão de crédito ou com empresas de serviço público, ou que tenham solicitado pedidos de hipotecas com o nome das vítimas, todo o qual tem ocasionado uma rede fraudulenta que vai levar anos para desenrascar.[6]

O Ministério Público de Portugal anunciou em dezembro de 2016, "ter acusado 24 arguidos envolvidos numa rede internacional de burlas informáticas, que opera a partir do Brasil, e terá desviado um total de 266 mil euros de dezenas de contas de clientes de bancos portugueses (...) Este tipo de burla – conhecida como *phishing* – é cada vez mais frequente, raro é as autoridades conseguirem chegar tão longe na estrutura da organização criminosa."[7]

As páginas webs que oferecem plataformas informáticas para praticar o *Phishing* aumentaram um 25% durante 2016. Os usuários de mensagens eletrónicos abrem um 30% das mensagens que buscam capturar a informação pessoal e 12% clique no URL, sem prestar atenção ao que estão a fazer.[8]

Os Criminosos da rede concentram os seus esforços em alvos regionais, computadores e aplicativos da Web que lhes permitem roubar informações pessoais, empresariais, financeiras ou confidenciais. Por isso, surgiu nos últimos anos valorações políticas e jurídicas dos problemas resultantes do uso indevido dos computadores, o que, em alguns casos resultaram em alterações nas leis penais nacionais e internacionais.

É por esta razão que, conscientes da importância por um lado, do prejuízo financeiro que pode causar os cibercrimes relacionados com o uso indevido de dados pessoais de pagamento, e, por outro, o impacto negativo que tais atos geram nas operações do comércio eletrónico[9]; a maioria dos países têm estado focados em fazer esforços para regular e proteger os dados pessoais e as operações de comércio eletrónico, em alguns casos criando organismos de controlo, em outros, tipificando atos criminosos que se enquadram numa penalidade, com a intenção de fornecer as medidas necessárias para promover a

[6] DEL PINO, Santiago - Delitos Informáticos: Generalidades.

[7] OLIVEIRA, Mariana - Dezenas de clientes de bancos portugueses burlados por rede brasileira. [Em linha].

[8] MEDINA, Manel; MOLIST, Mercè - INFORME VIU: Ciberseguridad: Tendencias 2017.p.2

[9] Atividade que gera grandes benefícios para a economia do país ao ponto de ser visto como um componente importante da atividade motora de uma nação ao impulsionar o seu crescimento económico.

segurança e a proteção nas pessoas para contribuir ao crescimento das operações de *e-commerce*, especialmente na sua relação "B2C"[10], de uma forma transparente e fiável para os utilizadores, salvaguardando assim os interesses da parte mais frágil, neste caso conhecido como: consumidor, comprador ou cliente.

Tal é assim, que nossa época é caracterizada pelo aumento do acesso à tecnologia e globalização social da informação e da economia. O desenvolvimento tecnológico e o maior uso de redes abertas como a Internet têm proporcionado novas oportunidades e novos desafios relacionados com a infraestrutura da informação, onde esta tornou-se uma parte vital do eixo das nossas economias, assim, os usuários deveriam poder contar com a disponibilidade de serviços de informação e ter a certeza de que as suas comunicações e dados estão protegidos contra o acesso ou interceções não autorizadas. O desenvolvimento do comércio eletrónico e a plena realização da sociedade da informação pode depender disto.

Desde o *boom* da Internet, que na sua abordagem comercial, tem mostrado além de benefícios econômicos para a sociedade, também pontos fracos cujas consequências têm um impacto significativo sobre o património das pessoas, surgindo a necessidade de estudar a seguinte problemática com a intenção de proteger os dados pessoais de pagamento utilizados no comércio eletrónico, enfrentando assim os novos desafios colocados pelos avanços na tecnologia, incluindo a tecnologia da informação, permitindo não só regular transações eletrónicas e punir os infratores, senão também, revisar os diferentes mecanismo de proteção, em especial leis, políticas e práticas que intervêm no comércio eletrónico, e que ajudem a pôr limites nas condutas comerciais fraudulentas, enganosas e abusivas, mas acima de tudo, permitindo construir a confiança do consumidor e estabelecer uma relação mais equilibrada nas transações comerciais entre fornecedores e consumidores, para promover um crescimento das atividades de comércio eletrónico, e consequentemente, na criação de riquezas, geração de importantes quantidades de postos de trabalho, o aumento da concorrência e redução de custos, em beneficio da sociedade e do país.

[10] Business to Consumer B2C: Forma de comércio eletrónico onde as transações comerciais são entre uma empresa e um usuário final

CAPITULO I

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

1.1 OS DADOS PESSOAIS E A SUA PRIVACIDADE.

A era digital nasceu com a Internet, a rede informática global, descentralizada, formada pela conexão direta entre sistemas computacionais, através dum protocolo especial de comunicação[11], tornando-se numa gigantesca base de dados onde é possível encontrar informação e serviços de todos os tipos, através de vários dispositivos tecnológicos, como os computadores, telefones inteligentes ou televisores digitais, os quais, permitem interagir com o ser humano usando as conexões das redes eletrónicas de informação.

Esta interação está presente em muitas das atividades que o homem faz, como: produção, cultura, relações sociais, comércio, entretenimento, educação, política, economia, medicina, lar e até a lei, gerando muitos benefícios, oportunidades e comodidades para o ser humano.

No entanto, os benefícios oferecidos no ambiente criado pela Internet para nossas vidas, também trazem riscos significativos, incluindo a possibilidade de nossas comunicações eletrónicas serem intercetadas por pessoas indesejadas, que poderiam elaborar perfis de nós, e que ao associá-los a determinados dados permitir-lhes-ia conhecer nossa identidade, afetando assim nossa privacidade.

Ao respeito, Marco António Zanelatto[12] salienta que:

> "...Em nenhum lugar do mundo é tão difícil ter vida privada quando na internet. A cada clique do *mouse*, as pessoas são marcadas, seguidas, encaixadas em estatísticas anônimas – ou nem tanto – graças a tecnologias cada vez mais perversas e onipresentes. Estaríamos, assim, sob o domínio do mal na World Wide Web?..."

[11] Diccionario de la Real Academia Española, 22ª Edición, 2001

[12] Cit. por MACEIRA, Irma – A PROTEÇÃO DO DIREITO À PRIVACIDADE FAMILIAR NA INTERNET.p.154

A privacidade é algo que existe, relacionado direta ou indiretamente, na vida dos seres humanos, ao manterem um espaço pessoal, sem interferências de outras pessoas ou organizações. Trata-se de um direito humano, como igualdade, justiça ou liberdade perante à lei.[13]

Para Bernadette Lóscio, aquando a privacidade trata da região próxima dum individuo, fala-se de privacidade territorial. Aquando, trata de danos morais e interferências indesejadas, trata-se de privacidade do Indivíduo e aquando se trata de dados pessoais coletados tais como nome, número do cartão de crédito, número da identidade, número de segurança social, etc., armazenados, processados e propagados para terceiros, fala-se de privacidade da informação.[14]

Assim, os dados pessoais corresponderia, no direito da União Europeia, a qualquer "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"[15]

Ou seja, partindo da perspetiva de ALESSANDRA SILVEIRA, são dados que "possibilitam a identificação de uma pessoa, e também aqueles dados que permitam chegar a essa identificação por associação de conceitos e conteúdos, mesmo que não se faça uma referência direta como o IP (*Internet Protocol*) ou da matrícula de um veículo".[16] Nestes termos, os dados pessoais, fazem referência a qualquer detalhe, circunstância ou informação numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, suscetível de coleta, registro, tratamento ou transmissão, que permita estar associada a uma pessoa física determinada.[17]

---

[13] LÓSCIO, Bernadette. HARA, Carmem. Martins Vidal. Orgs. - Tópicos em Gerenciamento de Dados e Informações 2014. p. 47

[14] LÓSCIO, Bernadette. HARA, Carmem. Martins Vidal. Orgs. - Ibidem

[15] PARLAMENTO EUROPEU E DO CONSELHO – Regulamento (UE) 2016/679 - Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, art.° 4 n.°1

[16] SILVEIRA, Alessandra; MARQUES, João. DO DIREITO A ESTAR SÓ AO DIREITO AO ESQUECIMENTO. CONSIDERAÇÕES SOBRE A PROTEÇÃO DE DADOS PESSOAIS INFORMATIZADOS NO DIREITO DA UNIÃO EUROPEIA: SENTIDO, EVOLUÇÃO E REFORMA LEGISLATIVA, p. 96

[17] PLAZA PENADÉS, Javier (Dir.) [et al.] – DERECHO Y NUEVAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. p. 1139

Conforme Irma Maceira, a personalidade é o gênero da qual a privacidade é a espécie, portanto, remonta aos princípios da criação da humanidade.[18] A frase direito à intimidade costumava ser empregada como sinônimo da expressão direito à privacidade. A intimidade do indivíduo está na esfera do secreto, ou seja: a reserva, o sigilo, as informações da pessoa que não devem chegar ao conhecimento alheio;[19] Desta forma, é tudo quanto diga respeito única e exclusivamente à pessoa em si mesma, a sua modo de agir e de ser.[20]

No entanto, Maria Helena Diniz,[21] afirma que a privacidade e intimidade não se confundem, mas por integrar-se ambas o direito à vida privada, pode incluir-se naquela, e salienta que a privacidade trata de assuntos externos da pessoa, e a intimidade de assuntos internos. Nesse sentido, Tércio Sampaio Ferraz Jr.[22] entende que a privacidade volta-se a aspetos da exclusividade da pessoa aquando este se dirige a um grupo específico e limitado de pessoas, enquanto a intimidade volta-se a aspetos da pessoa consigo mesma, os seus devaneios e pensamentos.

André Ramos Tavares[23], sobre isso, sustenta que o direito à privacidade engloba o direito à intimidade, à vida privada, à honra e à imagem das pessoas. Na mesmas linha de entendimento segue Alexandre de Moraes[24] ao afirmar que: "...os direitos à intimidade e a própria imagem forma a proteção constitucional salvaguardando a vida privada um espaço íntimo intransponível por intromissões ilícitas externas"

No sentido etimológico, a palavra Privacidade, se originou no Latim "*privatus*, pertencente a si mesmo, colocado à parte, fora do coletivo ou do grupo; particípio passado de *privare*, retirar de, separar; de *privus*, próprio, de si mesmo, individual; que por sua vez vem de pri-, *antes, à frente de*."[25] Daí deriva-se que o Direito à privacidade faz referência a uma privacidade individual, ao fazer referência a cada pessoa em concreto, singularmente entendido.[26]

---

[18] MACEIRA, Irma – A PROTEÇÃO DO DIREITO À PRIVACIDADE FAMILIAR NA INTERNET. p.60
[19] MACEIRA, Irma, op. cit., p.63
[20] MACEIRA, Irma, op. cit., p.64
[21] Cit. por MACEIRA, Irma – op. cit..p.65
[22] Cit. por MACEIRA, Irma – ibidem.
[23] Cit. por MACEIRA, Irma – ibidem
[24] Cit. por MACEIRA, Irma, ibidem.
[25] ORIGEM DA PALAVRA - Consultas e artigos com a palavra "privacidade" http://origemdapalavra.com.br/site/?s=privacidade
[26] CORREIA, Victor – SOBRE A PRIVACIDADE. p.7

Desde a antiguidade clássica o conceito de privacidade surge com Aristóteles[27], quem distinguia a esfera privada ("*oikos*") da esfera pública ("*polis*"). A esfera privada dizia respeito à família, às questões biológicas e económicas, enquanto a esfera pública dizia respeito à liberdade política dos cidadãos. Com a passagem do tempo, o conceito de privacidade, passou a referir-se a tudo o que é pessoal, tanto á família, como outros círculos mais próximos dos relacionamentos individuais. Chegando ao indivíduo singularmente entendido.[28]

Nesse contexto, Miguel Davara Rodriguez[29] identifica que os dados pessoais podem ser públicos ou privados. Os privados, podem ser íntimos e segredos, e estos últimos podem ser profundos e reservados. Distingue, que os dados pessoais são públicos, quando, de acordo com o valor atribuído pela consciência social, são conhecidos por qualquer pessoa, como nome, apelido, idade, profissão, os quais uma vez conhecidos, não pode impedir que sejam divulgados.[30] São dados pessoais privados, os que de acordo com esse valor social, busca-se impedir a sua difusão, e só serão conhecidos ou por vontade do titular ou em circunstâncias especiais avaliadas pelas leis.

Esse autor também explica, que nem todos os dados pessoais privados podem ser tratados como íntimos, no mesmo grau e com a mesma proteção, ou com a mesma capacidade de decisão do seu dono, e complementa que, os dados pessoais privados - íntimos, são os que o titular deve fornecer regularmente em conformidade com as suas obrigações cívicas, e são dados pessoais privados - segredos, aqueles que, sem obrigação, apenas os fornecem sob sua vontade ou, em casos excecionais, muito específicos e regulados. Alguns doutrinários chamam esses "dados pessoais privados secretos" como dados "confidenciais" ou "sensíveis", e aqueles que foram chamados pelo autor como "dados privados secretos – reservados", são na teoria chamados dados "sensíveis" ou duma "sensibilidade especial," eles lidam com aqueles que, em nenhum caso, o titular será obrigado a entregá-los, e não

[27] Aristóteles (em grego clássico: Ἀριστοτέλης; transl.: Aristotélēs; Estagira, 384 a.C. — Atenas, 322 a.C.) foi um filósofo grego, aluno de Platão e professor de Alexandre, o Grande. Seus escritos abrangem diversos assuntos, como a física, a metafísica, as leis da poesia e do drama, a música, a lógica, a retórica, o governo. (fonte: https://pt.wikipedia.org/wiki/Arist%C3%B3teles)

[28] CORREIA, Victor – SOBRE A PRIVACIDADE**.** p.63

[29] DAVARA RODRÍGUEZ., Miguel Á. – Manual de Derecho informático.P. 59

[30] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 60

admitem exceções, a diferença dos "dados privados secretos – profundo" que apesar de não estar obrigados a entrega-los, sim admitem exceções[31].

Victor Correia entende, que foi no Iluminismo que a defesa da esfera privada adquiriu os contornos atuais. Um dos seus principais defensores, John Locke, sobre isso afirmou que o poder originava-se nos indivíduos, os quais tinham o direito de ser protegidos contra as intromissões do poder público.[32]

Podemos indicar que do ponto de vista jurídico, uma das primeiras teorias que tratarem da privacidade e intimidade da informação pessoal, foi com a publicação da obra Grundzüge des Naturrechts oder der Rechtsphilosophie, da autoria de Karl David August Roder, na Alemanha, em 1846, onde começa a manifestar-se uns dos quadros da doutrina relativa ao direito à privacidade e à vida privada, ao considerar que incomodar alguém com perguntas impertinentes ou entrar em um aposento sem se fazer anunciar são atos de violação ao direito natural à vida privada.

Não obstante, a maioria dos doutrinários, considera que o ponto de partida da formulação do direito à intimidade e à vida privada nasce com a publicação do artigo intitulado *The Right to Privacity*[33] na *Harvard Law Review* vol. IV, n.º 5, em 1890, dos autores Samuel Dennis Warren e Lois Dembitz Brandeis, advogados norte-americanos, os quais preocupados pelas constantes invasões da vida pessoal e familiar, traçaram os contornos de um direito à privacidade também denominado *Right to be let alone,*[34] fundamentado em bases morais, e na inviolabilidade da personalidade, para proteger as emoções, pensamentos e sentimentos íntimos do individuo, seja qual fora sua forma de expressão,[35] o que originou o surgimento da primeira formulação do direito à privacidade como algo que carecia de proteção legal e com o alvo de defender o direito de ser deixado só.[36]

Embora possam existir algumas abordagens anteriores, nenhuma teve o impacto deste. Os autores invocam no artigo, que a lei deve proteger a privacidade, a intimidade e, a vida privada,

---

[31] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 61

[32] CORREIA, Victor, op. cit., p.64

[33] Direito à Privacidade (tradução minha)

[34] Direito a estar só (tradução minha)

[35] MACEIRA, Irma – op. cit..p.31

[36] CORREIA, Victor, op. cit., ibidem

assegurando a cada indivíduo o direito de determinar a extensão até onde cada um quer ver conhecida e divulgada a sua vida privada, os seus sentimentos, os seus pensamentos, ou os seus gostos. "O direito à privacidade, assumindo um caráter evolutivo, vai aumentando a sua importância nos finais do século XIX e no século XX, devido ao desenvolvimento de novas tecnologias. Já Warren e Brandeis tinham advertido que as invenções e os avanços da técnica poderiam trazer sérios riscos para as liberdades dos indivíduos e, concretamente, para o seu âmbito mais privado, defendendo que as fotografias instantâneas e os jornais periódicos invadiram os sagrados recintos da vida privada (...); e numerosos engenhos mecânicos ameaçam tornar realidade a profecia de que: 'o que se murmura dentro de casa será proclamado aos quatro ventos."[37] Hoje, após um século, a profecia foi cumprida, já que o direito à privacidade encontra-se ameaçado como consequência dos desenvolvimentos tecnológicos.

O direito à privacidade e intimidade, surge como "o direito que cada pessoa tem para poder decidir por si só o quê (e quando) deve ser partilhado com terceiras pessoas, permitindo ao individuo o controle da sua vida propiá e as experiências, nas esferas em que não é permitida uma intromissão, nem por parte do Estado nem por parte de terceiras pessoas. Este é um direito intimamente ligado à liberdade pessoal, à construção da identidade, ao controle que cada um deve ter sobre os aspectos da identidade que deseja projetar para o mundo."[38]

De acordo com Sérgio Cavalieri Filho[39], a privacidade é o direito de estar só, de ser deixado em paz para tomar decisões no domínio da intimidade, para que determinados aspetos da vida privada não cheguem ao conhecimento de terceiros. Doutrinariamente, Celso Lafer[40], tornou o conceito do "direito do indivíduo de estar só" como a "possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só refere, e que diz respeito ao seu modo de ser no âmbito da vida privada"

---

[37] Cit. por ESTRADA, Manuel. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. p. 36,37

[38] Cit. por MONTE, Mario; BRANDÃO, Paulo; Coord.(s).- DIREITOS HUMANOS E SUA EFETIVAÇÃO NA ERA DA TRANSNACIONALIDADE. Com ANDRADE, Francisco Colab.– COMUNICAÇÕES ELETRONICAS E DIREITOS HUMANOS: O PERIGO DE "HOMO CONECTUS". P.215
O PERIGO DE "HOMO CONECTUS": Investigação que parte do risco de privacidade, ao que se sujeita o homem ao estar conectado nas redes telemáticas, onde os seus dados pessoais são constantemente monitoradas pelos serviços informáticos, tais como redes sociais, computação distribuída, geolocalização e ambientes inteligentes, invadindo assim a sua privacidade em qualquer momento e lugar que este, e criando uma vigilância completa e indetetável, tornando-se quase impossível o exercício do direito de apagamento e esquecimento.

[39] Cit. por MACEIRA, Irma –. op. cit., p.45

[40] Cit. por MACEIRA, Irma - Ibidem.

Assente em isso, a privacidade e a intimidade ganham novos contornos, devendo ser observadas pelos juristas como sustenta Têmis Limberger[41], em importante estudo sobre o Direito à intimidade e proteção de dados pessoais, ao dizer que "...a necessidade de proteção jurídica do cidadão se origina do facto de que os dados possuem um conteúdo económico". Para Limberger, as novas tecnologias, voltaram a informação numa riqueza essencial da sociedade,[42] por esse motivo, nasce para este autor, a necessidade de uma proteção jurídica das pessoas no concernente ao tratamento dos seus dados pessoais, com o objeto de evitar o uso não autorizado dos mesmos.

Leonardo Bessa[43], nesse sentido, explica como "a preocupação com a privacidade (...) no que se refere à proteção de dados pessoais, aumenta na mesma proporção da evolução tecnológica na área informática." Adiante desse ameaçador e complexo cenário, a inquietação de Têmis Limberger é conhecer "como proteger os dados informatizados frente a uma sociedade e um mercado cada vez mais livres de fronteiras,"[44] onde, a globalização da informação tem uma propagação incontrolável que vulnera a intimidade das pessoas.

Partindo dessa perspetiva, mesmo, que a recolha e o processamento de dados pessoais tenha sido realizado cumprindo as formalidades exigidas pela lei, pode acontecer que esses dados sejam transferidos para um terceiro sem autorização do seu dono, situação que representa sérios perigos para a proteção do direito à privacidade da pessoa, uma vez que essa transferência facilita o cruzamento de dados, permitindo o processamento informático e facilitando a utilização desses dados [45].

Tal é o caso do emprego de "sensores capazes de monitorar aspetos como a pressão arterial, a temperatura do corpo, os batimentos cardíacos, as expressões faciais, incluindo até a possibilidade de uma constante observação de escolhas, comportamentos, [e] emoções, tornando as pessoas cada vez menos capazes de viver de acordo com as suas escolhas e comportamentos totalmente libres e autónomos."[46]

---

[41] Cit. Por BARRETO, Ricardo – DIREITO & REDES SOCIAIS NA INTERNET. p.162

[42] BARRETO, Ricardo – DIREITO & REDES SOCIAIS NA INTERNET. p.162

[43] Cit. por BARRETO, Ricardo – op. cit., p.172

[44] BARRETO, Ricardo – op. cit., p.172

[45] DEL PESO NAVARRO, Emilio.- SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN (comércio electrónico y protección de datos). p.298

[46] Cit. por MONTE, Mario; BRANDÃO, Paulo; Coord.(s); ANDRADE, Francisco; Colab - op. cit. p.216

Pelo qual, existe uma enorme necessidade de proteção da intimidade e da vida privada, assim como de demarcar limites, e ser conscientes das práticas de publicação dos dados pessoais, procurando assegurar as garantias de confidencialidade dos dados pessoais, isto é, da "pessoa singular, identificada ou identificável, considerada titular dos dados,"[47] no especial, aqueles dados considerados sensíveis ou secretos, os quais precisam de uma proteção adicional em relação à privacidade, tais como, as informações pessoais sobre saúde (registros médicos), biometria de um indivíduo, ou os resultados de uma avaliação de desempenho realizada com os funcionários de uma determinada empresa. [48]

É por isso que, como resultado do desenvolvimento tecnológico atual, surge a dúvida se podemos controlar a transmissão de dados pessoais, quais parâmetros podemos estabelecer e como implementá-los, como sublinhava Howard W. Johnson, desde a década de 1970 "A questão não é saber se incorporaremos o computador ao solucionamento dos problemas da comunicação, do conhecimento e do poder. A questão é saber se estaremos à testa de seu desenvolvimento e se controlaremos o seu uso à luz das necessidades e aspirações humanas" [49].

Portanto, é necessário, não apenas entender aquilo que cada um de nós gostaria de ver protegido pelo direito da privacidade[50], senão também compreender que não todas as informações que elaboramos ou enviamos por meios eletrónicos podem ser de conhecimento público, por quanto, a rede é estruturada de forma que possibilita o maior fluxo de informações incluindo nossos dados pessoais, o que torna difícil ou quase impossível um controle sobre os mesmos, dificultando assim a tutela deles, e provoca a invasão da esfera intima, muitas vezes sem conhecimento da vítima, não só, por não saber discernir exatamente quando um *site* possui sistema de segurança integrado, senão pelo desconhecimento e da insuficiência de dispositivos de segurança que ele pode utilizar.[51]

Fundamentado em isso, a nossa informação privada está em jogo e as consequências são muito graves, pois podem ser usadas em detrimento de nossos direitos pessoais e garantias individuais, ferindo direitos legais protegidos como patrimônio e a honra dos proprietários, também pode ser usada com fins

---

[47] Cit. por MONTE, Mario; BRANDÃO, Paulo; ibidem.

[48] LÓSCIO, Bernadette. HARA, Carmem. Martins Vidal. Orgs. - Tópicos em Gerenciamento de Dados e Informações 2014. p. 48

[49] Cit. por MACEIRA, Irma – A PROTEÇÃO DO DIREITO À PRIVACIDADE FAMILIAR NA INTERNET.p.2

[50] BERNABÉ, Franco – LIBERDADE VIGIADA. p.56

[51] MACEIRA, Irma – A PROTEÇÃO DO DIREITO À PRIVACIDADE FAMILIAR NA INTERNET. p.70, 158.

discriminatórios, ou para estabelecer um perfil comportamental, por isso, que a proteção dos dados pessoais nasce como um direito à privacidade e intimidade o qual deve ser cuidadosamente resguardado, a fim de evitar o mau uso dos mesmos.

Como bem salienta Irma Maceira[52] ao dizer que a privacidade merece um tratamento especial "por ser algo que deve ser preservado como um dos mais importantes direitos conquistados pelo homem, no plano dos direitos da personalidade, como sinônimo de autonomia, integridade e liberdade, sempre no sentido de melhor preservar os valores pessoais, éticos e morais de todo e qualquer indivíduo"

Ultimamente, têm surgido novos conceitos jurídicos como à *autodeterminação informativa*, que reconhece a capacidade da pessoa de decidir quando e como ela está disposta a permitir que as suas informações pessoais sejam disseminadas, ou seja, o poder de controlar e conhecer os dados que sobre ela encontram-se em suportes informáticos ou são suscetíveis de um tratamento posterior.[53] No entanto consideramos que o conceito de "autodeterminação informativa" e assim como o conceito de "proteção de dados," não são mais do que uma nova aplicação jurídica do direito a privacidade, já que eles defendem implicitamente algo que, no fundo, está incluído no direito à privacidade[54].

Com base no que foi levantado, surge a questão de como proteger nossos dados no ciberespaço, como proteger a nossa privacidade, a confidencialidade, a integridade e a disponibilidade de dados, assim como o patrimônio, a dignidade humana e a segurança das redes que são os bens a tutelar ou salvaguardar, considerando que os riscos mais importantes derivados de uma troca de informações através de redes abertas são: Que o autor e a fonte da mensagem sejam suplantados; Que a mensagem seja alterado acidentalmente ou maliciosamente durante a transmissão; Que o remetente da mensagem nega ter transmitido ou o destinatário ter recebido; e que o conteúdo da mensagem seja lido por uma pessoa não autorizada[55]. Tudo isso, considerando que essa proteção tem sido associada a limitações e mecanismos de natureza territorial e com diferentes padrões culturais, sociais e políticos.

---

[52] MACEIRA, Irma – A PROTEÇÃO DO DIREITO À PRIVACIDADE FAMILIAR NA INTERNET. p.23

[53] DAVARA RODRÍGUEZ., Miguel Á. - op. cit., p. 79

[54] CORREIA, Victor - op. cit., p.72

[55] PAEZ, Juan y ACURIO Santiago, DERECHO Y NUEVAS TECNOLOGÍAS. p. 81.

Spiekermann e Cranor em 2009[56] sobre isso relacionou 3 áreas de atividades técnicas, que causam grande preocupação e portanto ameaçam à privacidade dos dados pessoais, e que as chamou "esferas da privacidade", conforme o seguinte:

I. Esfera do usuário:
   A. Acesso não autorizado a dados pessoais
   B. Coleção e armazenamento de dados não autorizados.
   C. Exposição de dados.
   D. Entrada indesejada de dados.

II. Esfera da organização:

   Ademais de "I.A";

   A. Uso não autorizado de dados por terceiros envolvidos na coleta dos dados ou por outras organizações com as quais os dados foram compartilhados.
   B. Mau julgamento a partir de dados parciais ou incorretos.
   C. Exposição de dados.

III. Esfera dos provedores de serviços:

   Ademais de "II.A" e "II.B";

   A. Erros acidentais ou deliberados em dados pessoais.
   B. Combinação de dados pessoais, a partir de diferentes bancos de dados para recriar o perfil dum sujeito.

Com efeito, a resposta poderia ser orientada para a integração de todos os sistemas dentro da diversidade dos mesmos, a integração desse pluralismo existente, que permite "garantir: Que a mensagem vem da pessoa que diz que o envia; Que a mensagem não foi alterado no caminho; Que o emissor não pode negar o seu envio nem o recetor a sua receção; e, quando seja apropriado, garantir a confidencialidade[57]. Essas necessidades serão atendidas por padrões que se referem a conceitos amplos e valores acordados, onde o direito à privacidade e a proteção de dados pessoais provavelmente são os mais invocados como princípios normativos clássicos da lei, cuja violação deve ser sancionada juridicamente, incluindo monetariamente, obrigando ao pagamento duma indemnização ao afetado,

[56] Cit. por LÓSCIO, Bernadette. HARA, Carmem. Martins Vidal. Orgs. - Tópicos em Gerenciamento de Dados e Informações 2014. p. 50

[57] PAEZ, Juan y ACURIO Santiago, ibidem.

permitindo assim, ter o poder de exigir que a sua privacidade não seja invadida, e reivindica-la no caso de ser necessário.

Não é demais destacar que, um quadro de proteção de dados sólido e coerente, apoiado por uma aplicação rigorosa das regras, onde as pessoas singulares titular dos dados que dizem respeito, sejam alertadas para os riscos, regras, garantias e direitos associados ao tratamento especifico, explicito, pertinente, adequado e legitimo dos seus dados pessoais e dos meios de que dispõem para exercer os seus direitos, assegurando que o prazo de conservação dos dados seja limitado ao mínimo, permitiria conduzir à confiança necessária ao desenvolvimento do comércio eletrónico[58].

Não há que esquecer que o mundo da informática e a sua relação com o comércio movem-se diversos e importantes interesses que o Direito esta obrigado a regular. Nesse sentido, a informática não é alheia ao Direito, portanto é lógico pensar, que o Direito proporcione à Informática uma regulação jurídica com pressupostos éticos baseados nos princípios de pertinência, veracidade, atualização, e consentimento, necessária para o seu desenvolvimento.[59]

Vale destacar, que um dos aspetos básicos para a justa coexistência social do homem, é a proteção legal da sua privacidade diante a potencial agressividade da informática. Por causa disso, os governos desenvolveram as chamadas leis de proteção de dados nas legislações mais modernas nas quais reconhecem Direitos de aceso à informação, diretos à autodeterminação informativa, direitos de retificação e cancelação; Bem como regulamentos sobre a transferência eletrónica de fundos ou dados a nível nacional e internacional; Regras legais sobre documentos eletrónicos e assinaturas eletrónicas; Leis sobre cibercrimes e, Direitos de compradores e usuários em geral, ante a posição dominante de algumas multinacionais de tecnologia da informação e a comunicação[60].

Estamos diante de um imenso desafio, onde o homem só acompanhará com segurança o movimento do mundo no ambiente virtual, traçando os limites entre o que é aceitável e o que é abuso à privacidade se houver um ajustamento à complexidade imposta pelos avanços tecnológicos,[61] desse

[58] TEIXEIRA, Angelina – A Chave para a Regulamentação da Protecção de Dados. p. 26
[59] DAVARA RODRÍGUEZ., Miguel Á. op. cit., P. 32
[60] DAVARA RODRÍGUEZ., Miguel Á. op. cit., P. 34,35
[61] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 151

ponto, uma nova postura ética e social deve ser discutida. Decerto, a proteção das informações da vida pessoal e a globalização da informação, as telecomunicações e o comércio, constituem uma realidade atual, cuja tutela dos direitos da pessoa no que respeita aos dados pessoais, merece uma profunda reflexão e relevância no mundo jurídico[62].

1.2.OS TRATADOS E AS CONVENÇÕES INTERNACIONAIS.

O direito a privacidade, intimidade e identidade, avançou após dos trabalhos doutrinários e jurisprudenciais, ganhando reconhecimento nos organismos internacionais de cooperação, devido à gravidade de tal transgressão e às consequências que derivam delas.

Desse modo, os países expressaram a sua opinião com a assinatura de declarações, acordos, pactos, tratados, convénios ou convenções internacionais:

- Em 1948, a Declaração Universal Dos Direitos Humanos;
- Em 1950, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais;
- Em 1968, a Resolução 68/509/CE, sobre os Direitos Humanos e os Novos Logros Científicos e Técnicos;
- Em 1969, a Convenção Americana sobre Direitos Humanos Americanos;
- Em 1976, o Pacto Internacional sobre os Direitos Civis e Políticos (ONU);
- Em 1981, a Convenção n.º 108, para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter pessoal, do Conselho de Europa;
- Em 1987, a Recomendação n.º R (87) 15 do Conselho da Europa;
- Em 1989, a Declaração dos Direitos e Liberdades Fundamentais. Parlamento Europeu;
- Em 1990, a Resolução 45/95, relativa às Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal;
- Em 1992, o Tratado Da União Europeia, em Maastricht;

[62] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 152

- Em 1995, a Diretiva 95/46/CE, relativa à Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Em 2000, a Diretiva 2000/31/CE relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre comércio eletrónico).
- Em 2000, a Carta dos Direitos Fundamentais da União Europeia.
- Em 2000, o Regulamento (CE) n.º 45/2001, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.
- Em 2002, a Diretiva 2002/22/CE, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas.
- Em 2002, a Diretiva 2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.
- Em 2009, o Tratado sobre o Funcionamento da União Europeia.
- Em 2014, o Regulamento (UE) 910/2014 de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, do Parlamento Europeu e do Conselho.
- Em 2016, a Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.
- Em 2016**,** o Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Em 2016, a Decisão de Execução (UE) 2016/1250 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

Instrumentos jurídicos concebidos não só para prevenir e processar o cibercrime, mas também para descrever o comportamento criminoso, a fim de unificar as tipificações de cada país, contribuindo à cooperação e divulgação de técnicas para proteger a privacidade dos dados pessoais.

Mencionamos alguns aspectos relevantes deles:

1.2.1. Declaração Universal Dos Direitos Humanos adotada pela Assembleia Geral das Nações Unidas em 1948.

A Declaração Universal Dos Direitos Humanos adotada pela Assembleia Geral das Nações Unidas na sua Resolução 217 A (III), de 10 de dezembro de 1948 em Paris, no seu artigo 12.º afirma que: Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques,[63] e no entanto, a sociedade da informação comporta riscos evidentes para estes direitos.

1.2.2. Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (Conselho da Europa) em 1950.

Por sua vez, a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais adotada pelo Conselho da Europa em 1950, entrou em vigor em 1953 e previne no seu artigo 5º no.º 1 que: "Toda a pessoa tem direito à liberdade e segurança" [64], e em consonância a isso, o artigo 8º expressa que:

> "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem – estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros." [65]

Além disso, a convenção reconhece como um direito, a proibição de discriminação no seu artigo 14.º: "O gozo dos direitos e liberdades reconhecidos na presente Convenção deve ser assegurado sem quaisquer distinções, tais como as fundadas no sexo, raça, cor, língua, religião, opiniões políticas ou

[63] ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS (ONU) - Declaração Universal dos Direitos Humanos. Art.º 12

[64] CONSELHO DA EUROPA - Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais. Art.º5.- Direito à liberdade e à segurança

[65] Ibidem. Art.º 8.- Direito ao respeito pela vida privada e familiar.

outras, a origem nacional ou social, a pertença a uma minoria nacional, a riqueza, o nascimento ou qualquer outra situação."[66]

Bem assim, o seu art.º 33 estipula, que na Tramitação de uma petição dirigida ao Tribunal Dos Direitos do Homem (TEDH) "Qualquer Alta Parte Contratante pode submeter ao Tribunal qualquer violação das disposições da Convenção e dos seus protocolos que creia poder ser imputada a outra Alta Parte Contratante"[67].

Também, o Tribunal "pode receber petições de qualquer pessoa singular, organização não-governamental ou grupo de particulares que se considere vítima de violação por qualquer Alta Parte Contratante dos direitos reconhecidos na Convenção ou nos seus protocolos. As Altas Partes Contratantes comprometem-se a não criar qualquer entrave ao exercício efectivo desse direito."[68] Disposições que serviram de base para o desenvolvimento posterior da proteção de dados pessoais.

1.2.3. Resolução 68/509/CE da Assembleia do Conselho da Europa sobre os Direitos Humanos e os Novos Logros Científicos e Técnicos, em 1968.[69]

No contexto europeu, o início e os primeiros germes institucionais sobre a preocupação com a potencial agressividade das tecnologias da informação com os direitos fundamentais das pessoas foram evidenciados no ano de 1968, através da Resolução No.º 68/509/CE da Assembleia do Conselho da Europa, que destacou a salvaguarda do cidadão, especialmente a sua esfera interna, cara à potencial agressividade da tecnologia, dando várias recomendações e resoluções sobre o assunto, que mais tarde seriam chamados de proteção de dados pessoais.[70]

---

[66] Ibidem. Art.º 14.- Proibição de discriminação.

[67] Ibidem. Art.º 33.- Assuntos interestaduais

[68] Ibidem. Art.º 34.- Petições individuais.

[69] A Resolução n.º 2450 (XXIII) da Assembleia Geral da ONU, tomada em sua 23ª seção ordinária, em 19 de dezembro de 1968, sobre Direitos Humanos e Progresso Científico e Tecnológico, solicitou ao Secretário-Geral, com a ajuda do Comitê Consultivo de Aplicação de Ciência e Tecnologia para o Desenvolvimento, apresentará um estudo sobre os problemas que, em relação aos direitos humanos, apresentam o progresso da ciência e da tecnologia, especialmente: O respeito pela privacidade dos indivíduos e a integridade das nações antes do progresso das técnicas de registros e de outra natureza; Às aplicações da eletrónica que podem afetar os direitos da pessoa e os limites que devem ser fixados para essas aplicações em uma sociedade democrática, e mm termos mais gerais, o equilíbrio que deve ser estabelecido entre o progresso científico e técnico e a elevação intelectual, espiritual, cultural e moral da humanidade.

[70] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 64

1.2.4. Convenção Americana sobre Direitos Humanos da Organização dos Estados Americanos (Pacto de San José) de 1969.

Por seu lado, a Convenção Americana sobre Direitos Humanos, assinada na Conferência Especializada Interamericana de Direitos Humanos em San José, Costa Rica, de 7 a 22 de novembro de 1969, publicada no Diário Oficial n.º 9460, de 11 de fevereiro de 1978, e também conhecida como o Pacto de San José de Costa Rica destaca no seu artigo 11.º que: **1.** Toda pessoa têm o direito de respeitar a sua honra e o reconhecimento da sua dignidade. **2.** Ninguém pode ser objeto de ingerência arbitrária ou abusiva na sua vida privada, na de sua família, na sua casa ou sua correspondência, ou de ataques ilegais a sua honra ou reputação. **3.** Toda pessoa tem direito à proteção da lei contra tais ingerências ou esses ataques. O número 2 do artigo 12.º, por sua vez, afirma que ninguém pode ser objeto de medidas restritivas que possam menoscabar a liberdade de preservar sua religião ou suas crenças.[71]

1.2.5. Pacto Internacional sobre os Direitos Civis e Políticos (ONU) de 1976

O Pacto Internacional sobre os Direitos Civis e Políticos, aprovado e aberto à assinatura, ratificação e adesão pela Assembleia Geral da ONU na sua resolução 2200 A (XXI), de 16 de dezembro de 1966, que entrou em vigor em 23 de março de 1976, de acordo com o seu "Artigo 17.º: Ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação. Toda a pessoa tem direito a protecção da lei contra essas ingerências ou esses ataques"[72].

1.2.6. Convenção N.º 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, do Conselho de Europa, em 1981.

A Convenção n.º 108 do Conselho da Europa, de 28 de janeiro de 1981[73], referente à Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, entrou em vigor

---

[71] ORGANIZACION DE LOS ESTADOS AMERICANOS - CONVENCION AMERICANA SOBRE DERECHOS HUMANOS. art.º 11, art.º 12

[72] ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS - Pacto Internacional dos Direitos Civis e Políticos. Art.º 17

[73] O dia 29 de Julho de 1981, a Comissão das Comunidades Económicas Europeias promulgo a Recomendação No. 81/679/CEE, relativa a uma convenção do Conselho da Europa para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, especificando no seu preambulo N.ë I.2 que: "...A protecção dos dados é uma componente necessária da protecção do individuo. Tem a natureza de um direito fundamental. É

em 1 de outubro de 1985 e tem como objeto conforme ao art.º1 *"...,*garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)"[74]

Com tal característica, esta convenção, aplica-se de forma geral aos ficheiros, e a todos os tratamentos de dados pessoais realizados tanto pelo sector privado como pelo sector público, incluindo os tratamentos efetuados pelas autoridades policiais e judiciárias, buscando proteger às pessoas contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais. Além do mais, procura simultaneamente regular por meio de disposições o fluxo transfronteiriço desses dados para Estados não signatários, também chamados países terceiros. [75]

No seu art.º 4.1 convida os Estados signatários a desenvolver leis e a adotar medidas para que os princípios estabelecidos no seu texto possam ser cumpridos, motivando assim, a criação de autoridades nacionais de controlo de proteção de dados

No referente à coleta de dados e o seu propósito, o art.º 5 manifesta: "Os dados de carácter pessoal que sejam objecto de um tratamento automatizado devem ser: a) Obtidos e tratados de forma leal e lícita; b) Registados para finalidades determinadas e legítimas, não podendo ser utilizados de modo incompatível com essas finalidades; c) Adequados, pertinentes e não excessivos em relação às finalidades para as quais foram registados: d) Exactos e, se necessário, actualizados; e) Conservados de forma que permitam a identificação das pessoas a que respeitam por um período que não exceda o tempo necessário às finalidades determinantes do seu registo."[76]

1.2.7. Recomendação n.º R (87) 15 do Conselho da Europa, em 1987

desejável que seja efectuada em todos os Estados-membros uma aproximação em matéria de protecção dos dados. Será assim dada uma contribuição importante para a realização dos direitos do cidadão a nível europeu" COMISSÃO DAS COMUNIDADES ECONÓMICAS EUROPEIAS - Recomendação Nº. 81/679/CEE, relativa a uma convenção do Conselho da Europa para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal.

[74] CONSELHO DA EUROPA - Convenção 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Art.º 1.

[75] TEIXEIRA, Angelina – A Chave para a Regulamentação da Protecção de Dados. p. 11

[76] CONSELHO DA EUROPA - Convenção 108, op. cit., art.º 5

O Conselho da Europa emitiu a Recomendação n.º R (87) 15 do Comité de Ministros, de 17 de Setembro de 1987, que regula a utilização de dados pessoais no sector da polícia. No seu art.º 2 exprime:

> "Princípio 2º - Coleta de dados
> 2.1. A recolha de dados pessoais para fins policiais deve ser limitada às necessárias para a prevenção de um perigo real ou a supressão de uma infracção penal específica. Qualquer exceção a esta disposição deve ser objeto de legislação nacional específica.
> 2.2. Quando os dados relativos a um indivíduo foram coletados e armazenados sem o seu conhecimento, e a menos que os dados sejam excluídos, devem ser informados, sempre que possível, (...)
> 2.3. A recolha de dados por vigilância técnica ou outros meios automatizados deve ser prevista em disposições específicas.
> 2.4. É proibida a recolha de dados sobre os indivíduos apenas com base em ter uma origem racial específica, convicções religiosas particulares, comportamento sexual ou opiniões políticas ou pertences a movimentos ou organizações particulares que não sejam proibidos por lei. A coleta de dados sobre esses fatores só pode ser realizada se for absolutamente necessário para os propósitos de um inquérito específico."[77]

1.2.8. Declaração dos Direitos e Liberdades Fundamentais de 12 de abril de 1989. Parlamento Europeu.

A Declaração dos Direitos e Liberdades Fundamentais, de 12 de Abril de 1989, do Parlamento Europeu, publicada mediante resolução em D.O.C.E. C 120/51, de 16 de maio de 1989, contém um repertório de direitos civis, políticos, econômicos, sociais e culturais, ratificando que a dignidade humana e os direitos fundamentais são o eixo jurídico em que a Europa deve-se desenvolver. Note-se, que em termos de privacidade e proteção de dados pessoais, o artigo 6º recolhe "o direito à privacidade individual, e o artigo 18º confere aos particulares o direito de acesso e retificação no que diz respeito aos documentos e dados administrativos que afetá-los "[78]

O artigo 8.º, número 1, que trata dos dados sensíveis, proíbe o processamento de dados que revelem origem racial e étnica, opinião política, convicções religiosas ou morais, afiliação sindical, bem como informações relacionadas à saúde, e a vida sexual. No entanto, os Estados-Membros podem adotar regulamentos legais que autorizem o processamento de dados sensíveis nos seguintes três casos: a)

---

[77] CONSELHO DA EUROPA. Recomendação n.º R (87) 15 do Comité de Ministros - A UTILIZAÇÃO DE DADOS DE CARÁCTER PESSOAL NO SECTOR DA POLÍCIA.- S.l.: Conselho da Europa, 1987.

[78] EKMERKDJIAN, Miguel Ángel y PIZZOLO Calogero. "*Hábeas Data. El derecho a la intimidad frente a la revolución informática.*" Argentina. 1998, pag. 55

Quando o interessado concordou por escrito com esse tratamento; b) Quando o processamento automatizado é realizado por uma associação ou fundação sem fins lucrativos, de natureza política, religiosa ou sindical, para fins legítimos, desde que se refira exclusivamente aos membros da fundação ou à associação e pessoas relacionadas, e desde que os dados não sejam comunicados a terceiros sem o consentimento do interessado; c) Quando o tratamento foi realizado em circunstâncias tais que é claro que não viola a privacidade ou as liberdades individuais.[79]

O artigo 17.º numero 1, trata dos diferentes tipos de medidas de segurança, afirmando que o proprietário do arquivo deve tomar as medidas técnicas e organizacionais adequadas para proteger os dados pessoais registrados, contra destruição acidental ou não autorizada, por perda acidental, alteração, comunicação e qualquer outro tratamento de dados pessoais não autorizado.[80]

1.2.9. Resolução 45/95 da Assembleia Geral das Nações Unidas, de 1990, relativa às Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Carácter Pessoal

A Resolução nº 95 da Assembleia Geral da ONU, tomada na 45ª seção ordinária, em 14 de dezembro de 1990, adotada como Declaração, um relatório sobre a regulamentação de dados pessoais automatizados, elaborado pelo Relator Especial da Subcomissão para Prevenção de Discriminação e Proteção de Minorias, Sr. Louis Joinet sob o nome de *Diretrizes para a regulamentação dos ficheiros informatizados de dados pessoais*. Com esta Declaração, os governos são convidados a estabelecer os princípios que defendem a proteção de dados pessoais, que, por sua natureza flexível e geral, facilitam a sua incorporação no regulamento interno de cada país, a fim de proteger os arquivos automáticos, tanto do setor público quanto do privado.

A ONU sustém que a informação sobre pessoas não deve ser coletada ou processada de forma injusta ou ilegal ou ser usada para fins contrários aos propósitos e princípios da Carta das Nações Unidas. Em relação aos dados sensíveis, as diretrizes indicam que existe um certo tipo de dados pessoais cujo uso pode levar a "discriminações ilegais ou arbitrárias", e portanto, não devem ser coletados. Entre eles menciona explicitamente aqueles que se referem a raça, étnica, cor, vida sexual, opinião política, religião,

[79] PARLAMENTO EUROPEO - Declaración de derechos y libertades fundamentales. Art.° 8

[80] PARLAMENTO EUROPEO - Declaración de derechos y libertades fundamentales. Art.° 17

filosofia e outras crenças, além de ser membro de sindicatos ou associações. Todos os dados pessoais coletados e processados devem ser relevantes limitados e adequados para fins específicos, tanto na coleta como no processamento.[81]

A finalidade do ficheiro e seu uso devem ser especificados para garantir que todos os dados pessoais coletados e armazenados sejam relevantes para os propósitos específicos e que nenhum dos dados pessoais possam ser usados ou divulgados para fins incompatíveis com aqueles, exceto com o consentimento do afetado. Este requisito enfatiza que a especificação para os fins mencionados, deve ser cumprida no momento inicial da criação do arquivo, bem como em qualquer atividade posterior.

Além disso, as diretrizes das Nações Unidas estabelecem que devem ser tomadas medidas de segurança adequadas para proteger os arquivos contra riscos naturais, como perda ou destruição acidental, além dos riscos humanos, como acesso não autorizado, uso fraudulento de dados ou contaminação por vírus informáticos.[82]

1.2.10. Tratado Da União Europeia, em Maastricht, 1992

O Tratado Constitutivo da União Europeia, assinado em Maastricht em 7 de fevereiro de 1992, declara no seu artigo 6.º número 1 que: *"1.-* A União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, de 7 de dezembro de 2000, com as adaptações que lhe foram introduzidas em 12 de dezembro de 2007, em Estrasburgo, e que tem o mesmo valor jurídico que os Tratados...."[83]

Alem do mais, o número 3 do artigo citado diz que: "...Do direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados Membros..."[84].

---

[81] EKMERKDJIAN, Miguel Ángel y PIZZOLO Calogero. Ob. cit., p. 44

[82] EKMERKDJIAN, Miguel Ángel y PIZZOLO Calogero. Ibídem. p. 46

[83] TRATADO DA UNIÃO EUROPEIA (TUE), art.º 6 núm. 1

[84] Ibidem, art.º 6 num. 3

Em consonância com o dito, o art.º 39 precisa que: "...Em conformidade com o artigo 16.º do Tratado sobre o Funcionamento da União Europeia e em derrogação do nº. 2 do mesmo artigo, o Conselho adota uma decisão que estabeleça as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação do presente capítulo, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes"[85].

1.2.11. Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, em 1995.

Em 1995, o Parlamento Europeu e o Conselho da União Europeia aprovaram a Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, aplicável no âmbito do mercado interno da União Europeia, a qual teve grande incidência no conhecimento e interpretação da normativa sobre proteção de dados, ao harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados.[86]

A alínea a) do art.º 2 estabelecia o conceito de dado pessoal ao exprimir: "a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social."[87] Onde, os dados pessoais foram definidos sobre a qualificação dos titulares, e informação associada a elementos específicos da personalidade do titular embora, eles não revestam um carater de imediata identificação.

Referimo-nos a esta Diretiva, devido à importância que teve no início da proteção dos dados pessoais para o direito da Comunidade Europeia, no entanto, esta Diretiva foi revogada pelo REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016

[85] TRATADO DA UNIÃO EUROPEIA (TUE), art.º 39

[86] TEIXEIRA, Angelina – A Chave para a Regulamentação da Proteção de Dados. p. 17

[87] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 95/46/CE Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Art.º 2

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, o qual abordaremos mais adiante neste capítulo.

1.2.12. Diretiva 2000/31/CE do Parlamento Europeu e do Conselho relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre comércio eletrónico»), no ano 2000.

A Diretiva 2000/31/CE de 8 de Junho de 2000 relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico no mercado interno («Diretiva sobre comércio eletrónico»), estabelece o quadro do mercado interno na EU para o comércio eletrónico, com padrões harmonizados em questões como requisitos de transparência e informação para provedores de serviços *on-line*, comunicações comerciais, contratos eletrónicos e limitações à responsabilidade dos fornecedores de serviços intermediários.

As empresas que enviam mensagens de *spam*[88] devem consultar regularmente e respeitar os registos de opção negativa («*opt-out*») onde se podem inscrever as pessoas que não desejem receber esse tipo de mensagens. O correio eletrónico não solicitado («*spam*») também deve ser claramente identificável.[89]

Assim o dispõe o art.º 7 relativo à Comunicação comercial não solicitada (...) "2. Sem prejuízo da Diretiva 97/7/CE e da Diretiva 97/66/CE, os Estados-Membros deverão tomar medidas que garantam que os prestadores de serviços que enviem comunicações comerciais não solicitadas por correio eletrónico consultem regularmente e respeitem os registos de opção negativa («*opt-out*») onde se podem inscrever as pessoas singulares que não desejem receber esse tipo de comunicações."[90]

1.2.13. Carta dos Direitos Fundamentais da União Europeia, no ano 2000.

[88] "SPAM (Sending and Posting Advertisement in Mass) são mensagens eletrónicas não solicitadas enviadas para uma grande quantidade de pessoas. Ou seja, é o ato de enviar e postar publicidade em massa. Geralmente, a propaganda é o tipo de SPAM mais conhecido e o e-mail é a maneira mais usual de enviá-las". SANTOS, Barbara - SPAM: o que é e como evitar essa prática.

[89] EUR-LEX - Comércio eletrónico — Normas comuns da EU.

[90] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2000/31/CE relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre comércio eletrónico»). art.º 7

O Parlamento Europeu, o Conselho e a Comissão proclamaram solenemente a Carta dos Direitos Fundamentais da União Europeia em Nice, no ano 2000, que faz parte do direito primário da União, uma vez que tem efeito direto após a aprovação do Tratado de Lisboa (TUE) em 1º de dezembro de 2009, conforme o expressado no número 1 do Artigo 6.º: « A União reconhece os direitos, as liberdades e os princípios enunciados na Carta dos Direitos Fundamentais da União Europeia, (...), e que tem o mesmo valor jurídico que os Tratados....»[91].

A Carta lista os direitos básicos que a União tem de respeitar, criando dessa forma, segurança jurídica dentro da EU pois, oferece um conjunto de direitos políticos, pessoais, cívicos, sociais e económicos dos cidadãos e residentes na EU, e reafirma o respeito pelas atribuições e competências da EU, além da observância do princípio da subsidiariedade, e dos direitos que decorrem, nomeadamente, das tradições constitucionais e das obrigações internacionais comuns aos países da EU.

Ademais, é um instrumento juridicamente vinculante, concebido para reconhecer formalmente e dar visibilidade ao papel desempenhado pelos direitos fundamentais na ordem jurídica da União, ao respeitar a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, as Cartas Sociais aprovadas pela UE e pelo Conselho da Europa, bem como a jurisprudência do Tribunal Europeu dos Direitos do Homem e do Tribunal de Justiça da União Europeia.

No seu artigo 7º consagra o direito ao respeito pela vida privada e familiar, ao fixar que: "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações" [92].

Assim também foi consagrado no seu art.º 8 que a proteção de dados pessoais é um direito fundamental ao estabelecer que:

> "1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por

[91] TRATADO DA UNIÃO EUROPEIA (TUE), art.º 6 num. 1

[92] UNION EUROPEIA (2000/C 364/01) CARTA DOS DIREITOS FUNDAMENTAIS. Art. 7

lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."[93]

Alessandra Silveira observa que "as disposições da CDFUE não alargam as competências da UE tal como definidas nos Tratados, mas as disposições da Carta obrigam às instituições europeias e os Estados-Membros a respeitar e promover a aplicação dos direitos fundamentais nela previstos (artigo 51.º, n.º 1[94], da CDFUE) (...) Para o direito da União, nem todos os dados pessoais são susceptíveis, pela sua natureza, de causar prejuízo à vida privada da pessoa em causa – mas devem ser igualmente protegidos."[95] Dai que a CDFUE "dá um passo adiante em relação a várias Constituições dos Estados-Membros da UE e em relação à Convenção Europeia dos Direitos do Homem (...) no domínio da proteção de dados, na medida em que consagra um direito fundamental que protege dados que não têm de ser privados e muito menos íntimos – basta que sejam pessoais."[96]

1.2.14. Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, em 2000.

O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho de 18 de Dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, é aplicável ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União, tendo sido criada inclusivamente uma Autoridade Europeia para Proteção de Dados.

Exprime no seu art.º 1 o seu objeto:

---

[93] UNION EUROPEIA (2000/C 364/01) CARTA DOS DIREITOS FUNDAMENTAIS. Art.º 8.

[94] As disposições da presente Carta têm por destinatários as instituições e órgãos da União, na observância do princípio da subsidiariedade, bem como os Estados-Membros, apenas quando apliquem o direito da União. Assim sendo, devem respeitar os direitos, observar os princípios e promover a sua aplicação, de acordo com as respectivas competências. (artigo 51.º, n.º 1[95], da CDFUE)

[95] SILVEIRA, Alessandra; MARQUES, João. op. cit. p.4

[96] SILVEIRA, Alessandra; MARQUES, João. op. cit. p. 94,95.

"1. As instituições e os órgãos criados pelos Tratados que instituem as Comunidades Europeias, ou com base nesses Tratados, adiante designados «instituições e órgãos comunitários», asseguram, nos termos do presente regulamento, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais, e não limitam nem proíbem a livre circulação de dados pessoais entre eles ou entre eles e destinatários abrangidos pela legislação nacional dos Estados-Membros que transponha a Directiva 95/46/CE.
2. A autoridade independente de controlo criada no presente regulamento, adiante designada Autoridade Europeia para a protecção de dados, controla a aplicação das disposições do presente regulamento a todas as operações de tratamento efectuadas pelas instituições e órgãos comunitários."[97]

No quanto a seu âmbito de aplicação o art.º 3 assinala:

"1. O presente regulamento é aplicável ao tratamento de dados pessoais por todas as instituições e órgãos comunitários, na medida em que esse tratamento seja executado no exercício de actividades que dependam total ou parcialmente do âmbito de aplicação do direito comunitário.
2. O presente regulamento é aplicável ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados."[98]

1.2.15. Diretiva 2002/22/CE, do Parlamento Europeu e do Conselho relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, de 2002.[99]

A Diretiva 2002/22/CE[100] do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, alterada pela Diretiva 2009/136, determina no seu Art.º 1, o seu âmbito e objetivos:

"**Artigo 1.º** Âmbito e objetivos:

[97] PARLAMENTO EUROPEU E DO CONSELHO - Regulamento (CE) n.º 45/2001 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Art. 1

[98] PARLAMENTO EUROPEU E DO CONSELHO - Regulamento (CE) n.º 45/2001, op. cit. Art. 3

[99] Alterada pela DIRECTIVA 2009/136/CE de 25 de Novembro de 2009.

[100] A Diretiva 2002/22/CE foi alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho.

1. O objectivo é garantir a disponibilidade em toda a Comunidade de serviços de boa qualidade acessíveis ao público, através de uma concorrência e de uma possibilidade de escolha efectivas, e atender às situações em que as necessidades dos utilizadores finais não sejam convenientemente satisfeitas pelo mercado (...)
2. A presente directiva estabelece os direitos dos utilizadores finais e as correspondentes obrigações das empresas que oferecem redes e serviços de comunicações electrónicas acessíveis ao público. (...)
3. (...) As medidas nacionais relativas ao acesso ou à utilização de serviços e aplicações através de redes de comunicações electrónicas pelos utilizadores finais devem respeitar os direitos fundamentais dos cidadãos, nomeadamente em relação à privacidade e ao direito a um processo equitativo previsto no artigo 6.º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais..."[101]

"Artigo 25.º Serviços de informações de listas telefónicas:
1. Os Estados Membros garantem que todos os assinantes dos serviços telefónicos acessíveis ao público tenham uma entrada nas listas acessíveis ao público referido na alínea a) do n.º 1 do artigo 5.º (...)
5. O disposto nos n.os 1 a 4 é aplicável sob reserva do disposto na legislação comunitária sobre a protecção dos dados pessoais e da privacidade e, em especial, no artigo 12.º da Directiva 2002/58/CE (Directiva 'Privacidade e Comunicações Electrónicas')"[102]

1.2.16. Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), de 2002

Em 31 de julho de 2002, foi publicada no Jornal Oficial das Comunidades Europeias, a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, também conhecida como a Diretiva relativa à privacidade e às comunicações eletrónicas, foi uma norma que se adapto ao desenvolvimento dos mercados e das tecnologias dos serviços de comunicações eletrónicas, de modo a proporcionar um nível idêntico de proteção dos dados pessoais e da privacidade aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas.[103]

[101] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/22/CE Relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas. Art.º 1 (conforme alteração feita pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho.)

[102] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/22/CE Relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas., Art.º 25 (conforme alteração feita pela **Diretiva 2009/136/CE** do Parlamento Europeu e do Conselho)

[103] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/58/CE Relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, Considerando Nº. 4.

Em quanto a seu âmbito e objeto, o art.º 1 determina:

> "**1.** A presente directiva prevê a harmonização das disposições dos Estados Membros necessárias para garantir um nível equivalente de protecção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no sector das comunicações electrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações electrónicas na Comunidade..."[104]

Sobre a proteção de dados, o art.º 15 trata da Aplicação de determinadas disposições da Diretiva 95/46/CE, ao precisar que:

> "...**1-B**. Os prestadores estabelecem procedimentos internos para responder aos pedidos de acesso aos dados pessoais dos utilizadores com base nas disposições nacionais aprovadas nos termos do n.º 1. Aqueles prestam às autoridades nacionais competentes, a pedido destas, informação sobre esses procedimentos, o número de pedidos recebidos, a justificação jurídica invocada e a resposta dada (...)
> **3**. O Grupo de Protecção das Pessoas no que respeita ao Tratamento de Dados Pessoais, instituído nos termos do artigo 29 da Directiva 95/46/CE, realizará também as tarefas previstas no artigo 30 da mesma directiva no que respeita às matérias abrangidas pela presente directiva, nomeadamente a protecção dos direitos e liberdades fundamentais e dos interesses legítimos no sector das comunicações electrónicas."[105]

A Diretiva 2002/58/CE foi alterada pela Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho. Não obstante, a Diretiva 2006/24/CE foi declarada nula na sentencia C-293/12 do TJUE datada de 8 de abril de 2014, nos processos apensos C-293/12 e C-594/12, porque não oferecia as seguranças suficientes para a conservação dos dados.

1.2.17. Tratado sobre o Funcionamento da União Europeia - TFUE, de 2009.

---

[104] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/58/CE Relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, art.º 1 (conforme alteração feita pela **Diretiva 2009/136/CE do** Parlamento Europeu e do Conselho)

[105] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/58/CE Relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, art.º 15 (conforme alteração feita pela **Diretiva 2009/136/CE** do Parlamento Europeu e do Conselho).

O Tratado sobre o Funcionamento da União Europeia foi assinado em Roma, o 25 de março de 1957, como Tratado Constitutivo da Comunidade Económica Europeia e, desde então, sobreviveu com várias reformas e diferentes denominações, até 1992 aquando é chamado Tratado CEE e de 1992 a 2009 foi identificado como "Tratado que institui a Comunidade Europeia"; finalmente, em dezembro de 2009, momento que entra em vigor o Tratado de Lisboa[106], é chamado Tratado sobre o Funcionamento da União Europeia.

Este tratado, é a base jurídica da EU, e portanto a sua carta constitucional, que consagra a ordem jurídica fundamental do poder público europeu, determinando as categorias e os domínios de competência da União, descreve as políticas e as ações internas da União, e integra as disposições institucionais, financeiras e relativas à cooperação reforçada da União, e no que respeita aos dados pessoais introduze, como entende Angelina Teixeira, uma (única) base jurídica para a proteção de dados pessoais na União Europeia, ao igual que a competência, nomeadamente o artigo 16.º do TFUE[107]:

> *TFUE Artigo 16.º* (ex-artigo 286.º TCE)
> "1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de actividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes."[108]

1.2.18. Regulamento (UE) 910/2014 de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, do Parlamento Europeu e do Conselho:

Em 1 de julho de 2016, entrou em vigor o Regulamento (UE) n.º 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno,

[106] O Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de Dezembro de 2007, vem publicado no Jornal Oficial da União Europeia, C, n.º 306, de 17.12.2007

[107] TEIXEIRA, Angelina – A Chave para a Regulamentação da Protecção de Dados. P. 8-9

[108] TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA. Art.º 16

do Parlamento Europeu e do Conselho, que estabelece um quadro jurídico comum para as assinaturas eletrónicas na União Europeia.

O Regulamento visa regular a identificação eletrónica e marca diretrizes para os serviços de confiança relacionados com transações eletrónicas que são comuns a todos os países da UE, tais como: estabelecimento dos selos eletrónicos, os selos temporais, os documentos eletrónicos, os serviços de envio registado eletrónico e os serviços de certificados para autenticação de sítios web. Além disso, regula o estabelecimento duma base comum para a interação eletrónica segura entre cidadãos, empresas e autoridades públicas europeias, com a intenção de aumentar a eficácia dos serviços *on-line* públicos e privados, promovendo o comércio eletrónico no território europeu e fazendo com que os indivíduos confiem mais em transações eletrónicas.

O Regulamento busca eliminar a barreira entre os países membros, ao dispor de sistemas de identificação de cidadãos e validez da suas assinaturas eletrónicas de modo que permitam operar com maior agilidade, menor custo e ser mais eficiente a nível europeu.

1.2.19. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

Em 4 de maio de 2016, foi publicada no Jornal Oficial da União Europeia, a Diretiva (EU) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga com efeitos a partir de 6 de maio de 2018 a Decisão-Quadro 2008/977/JAI do Conselho.

A Diretiva (EU) 2016/680 visa estabelecer uma troca eficiente de informações entre as autoridades policiais nacionais e assegurar que os dados das vítimas, testemunhas e suspeitos de crimes sejam devidamente protegidos no contexto de uma investigação criminal ou de uma ação policial. Todas

as ações judiciais na UE devem cumprir os princípios de necessidade, proporcionalidade e legalidade e oferecer garantias adequadas para as pessoas.

No seu Art.º 1 a Decisão designa o Objetivo ao manifestar:

> **"1.** A presente diretiva estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.
> **2.** Nos termos da presente diretiva, os Estados-Membros asseguram:
> a) A proteção dos direitos e das liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais; e
> b) Que o intercâmbio de dados pessoais entre autoridades competentes na União, caso seja previsto pelo direito da União ou do Estado-Membro, não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais."[109]

Em quanto a seu âmbito de aplicação, o Art.º2 núm. 2 precisa:

> "...**2.** A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados...."[110]

Nos termos da citada Diretiva, entende-se por dados pessoais, as "informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»), considerando-se identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular."[111]

Nos termos do artigo 14.º da Diretiva, instaura-se o Direito de acesso do titular aos seus dados pessoais, e "...sem prejuízo do artigo 15.º[112], os Estados-Membros preveem que o titular dos dados

---

[109] PARLAMENTO EUROPEU E DO CONSELHO – Diretiva (EU) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Art.º 1

[110] Ibidem, art.º2

[111] Ibidem, art.º2

[112] "**Artigo 15**. Limitações do direito de acesso 1. Os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática,

tenha o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe dizem respeito estão ou não a ser objeto de tratamento..."[113]

1.2.20. Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, em 2016.

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) visa considerar os novos desenvolvimentos tecnológicos nas TIC´s e reforçar as medidas para o tratamento e a utilização correta de dados pessoais armazenados.

A proteção conferida nesta regulamentação aplica-se ao tratamento por meios automatizados de dados pessoais das pessoas singulares, independentemente da sua nacionalidade ou local de residência e não aos dados pessoais das pessoas coletivas. O âmbito de aplicação inclui ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros, excluindo os ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos.[114]

Como salientam Ana Simões e Mariana Ferreira, os principais câmbios na proteção e a privacidade de dados pessoais, são:

a) "O alargamento do âmbito de aplicação às entidades responsáveis (ou subcontratantes) pelo tratamento de dados pessoais no território da União Europeia, independentemente do local onde se encontram sediadas;

---

tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de: a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais; c) Proteger a segurança pública; d) Proteger a segurança nacional; e) Proteger os direitos e as liberdades de terceiros.
2. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, por uma das categorias previstas no n.º 1.
3. Nos casos a que se referem os n.os 1 e 2, os Estados-Membros preveem que o responsável pelo tratamento informe por escrito o titular dos dados, sem demora injustificada, de todos os casos de recusa ou limitação de acesso, e dos motivos da recusa ou da limitação. Essa informação pode ser omitida caso a sua prestação possa prejudicar uma das finalidades enunciadas no n.º 1. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados do direito que lhe assiste de apresentar reclamação à autoridade de controlo ou de intentar uma ação judicial.
4. Os Estados-Membros preveem que o responsável pelo tratamento detalhe os motivos de facto ou de direito em que a sua decisão se baseou. Essa informação deve ser facultada às autoridades de controlo." (PARLAMENTO EUROPEU E DO CONSELHO – Diretiva (EU) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados)

[113] PARLAMENTO EUROPEU E DO CONSELHO – Diretiva (EU) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Art.º 14.

[114] TEIXEIRA, Angelina – op. cit. p. 19

b) A previsão de regras de especial tutela quanto a menores – estando em causa uma oferta directa de serviços a menores, o tratamento dos respectivos dados pessoais só será lícito se estes tiverem pelo menos 16 anos. No caso de o menor ter menos de 16 anos, o tratamento só será lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das respectivas responsabilidades parentais;

c) O reforço e maior concretização dos direitos do titular dos dados – designadamente (i) o aprofundamento do direito à transparência e do direito de informação e acesso aos dados pessoais, pela exigência de maior rigor no tipo de informações a prestar ao titular dos dados e pelo incremento dos requisitos do consentimento; e (ii) a introdução do direito de rectificação, do direito ao apagamento dos dados pessoais (o "direito a ser esquecido")[115] e do direito de portabilidade dos dados, sendo que neste último caso, e assim o requeira o titular dos dados, as empresas serão obrigadas a enviar os dados pessoais que àquele digam respeito e que ele tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, bem como não se poderão opor à transmissão desses dados a outro responsável pelo tratamento;

d) A imposição de diversas obrigações aos responsáveis pelo tratamento dos dados – tais como: (i) a adopção de políticas específicas de protecção de dados (como a pseudonimização, a cifragem de dados, entre outras); (ii) a cooperação com a autoridade de controlo; (iii) a notificação de uma violação de dados pessoais à autoridade de controlo, no prazo máximo de 72 horas; (iv) a avaliação do impacto das operações de tratamento de dados, antes de iniciá-lo; (v) a consulta prévia à autoridade de controlo, no caso de a avaliação referida revelar um risco elevado para a protecção dos dados pessoais; e (vi) a designação de um especialista 'Encarregado para a Protecção de Dados'[116] sempre que, em geral:

   1. O tratamento seja efectuado por uma autoridade ou um organismo público; ou

---

[115] O direito ao esquecimento, pode-se definir como o direito do titular de um dado de que seja apagado ou bloqueado, quando ocorrem certas circunstâncias e, em particular, que não poda ser acessível através da rede de internet. (DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 127). No concernente, Alessandra Silveira e João Marques, destacam que: "o afetado reclama proteção contra a difusão de dados pessoais que são processados/propagados e se tornam acessíveis por intermédio de motores de busca – ou seja, um direito originariamente concebido para ser exercido *online*. Nessa medida, assentam os autores, que o direito ao esquecimento se distingue do direito ao apagamento originariamente previsto na Diretiva 95/46 para ser exercido *offline*, pois o último implica que os dados pessoais sejam conservados apenas por um certo período de tempo, exigindo-se o seu apagamento a partir de um prazo adequado às finalidades do tratamento."(op. cit. P.102). No entanto, este direito possui características que dificultam o controle: como a impossibilidade de apagar todos os traços e, em particular, que os dados não sejam acessíveis indiretamente pelos motores de busca *online* que se afastam do controle do titular dos dados e responsáveis pelo ficheiro. Por outro lado, também pode colidir com liberdade de expressão ou informação (DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 128)

[116] O Delegado de Proteção de Dados desempenhará funções de informar, assessorar e supervisionar o cumprimento do Regulamento, dando a devida atenção aos riscos associados às operações de tratamento, levando em consideração a natureza, o alcance, o contexto e os objetivos do tratamento, cooperando sempre com a autoridade de controlo, atuando como interlocutor para questões relacionadas ao tratamento.

2. As actividades principais do responsável pelo tratamento ou do subcontratante consistam:

   i. Em operações de tratamento que, pela sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

   ii. Em operações de tratamento em grande escala de categorias especiais de dados e de dados pessoais relacionados com condenações penais e infracções

e) A densificação do 'Princípio geral das transferências' – em matéria de transferências de dados pessoais para países terceiros ou organizações internacionais, o Regulamento 2016/679 estabelece que qualquer transferência de dados pessoais, que sejam ou venham a ser objecto de tratamento após transferência para um país terceiro ou uma organização internacional, só será realizada se as condições nelas estabelecidas forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional; e

f) A estatuição de coimas com montantes especialmente elevados – prevê-se a possibilidade de as coimas chegarem até 20.000.000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial."[117]

Com tais características o regulamento, aponta à uniformização do direito aplicável no domínio europeu, sem necessidade de intermediação legislativa das autoridades nacionais, e pretende eliminar eventuais contradições na aplicação do direito entre os vários Estados-Membros, aplicando-se ainda no caso de empresas localizadas fora da UE que direcionem as suas atividades para pessoas da UE e realizem um processamento de dados pessoais, reforçando a confiança e a segurança jurídica, promovendo também a concorrência leal.

1.2.21. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.[118]

[117] SIMÕES, Ana; FERREIRA, Mariana - PROTECÇÃO DE DADOS PESSOAIS. REGULAMENTO (UE) 2016/679.

[118] Esta decisão substitui à Decisão 520/2000/CE, por quanto, em 6 de outubro de 2015, o TJUE, no âmbito do processo Schrems, invalidou a Decisão 520/2000/CE que declara o nível adequado de proteção do regime de porto seguro entre a UE e os EUA, em conformidade com à Diretiva 95/46/CE. Na decisão do tribunal, afirmou-se que o regime de porto seguro US permite interferência por parte das autoridades públicas desse país sobre os direitos fundamentais dos indivíduos, porque a lei dos EUA permite deixar de aplicar as regras de protecção previsto pelo regime, e acrescenta que a Comissão não mostra que os Estados Unidos têm regras para limitar estes possíveis interferências ou que não há efetiva proteção legal contra elas. Na Decisão 520/2000/CE, por ser um sistema voluntário entre a UE e os EUA, para controlar o tratamento dos dados transmitidos aos EUA, qualquer empresa ou entidade americana que afirme respeitar os princípios do porto seguro teria direito a receber dados da UE, razão pela qual não oferecia garantias suficientes

A Comissão Europeia aprovou a Decisão de Execução (UE) 2016/1250, de 12 de Julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE, pelo qual, os dados pessoais podem ser transferidos livremente para organizações nos Estados Unidos incluídos na "Lista de Proteção da Privacidade", que é preparada e publicada pelo Departamento de Comércio dos Estados Unidos.[119]

O escudo de privacidade UE-EUA baseia-se num sistema de autocertificação pelo qual as entidades americanas se comprometem a cumprir uma série de princípios de proteção da privacidade nomeadamente, os princípios de enquadramento do Escudo de Privacidade UE-EUA, incluindo princípios complementares, estabelecidos pelo Departamento de Comércio dos Estados Unidos e o listado do anexo II da decisão.

Para estar na lista, as empresas dos EUA devem se comprometer a respeitar um forte conjunto de regras e garantias em relação à proteção de dados. Por exemplo, eles devem: exibir a sua política de privacidade no seu *site* de acordo com os princípios do *Privacy Shield*; Assegurar o cumprimento, no que diz respeito às transferências de dados para países terceiros, e responder rapidamente a qualquer reclamação e submeter-se à supervisão de um órgão independente de resolução de disputas, que pode ser uma autoridade de proteção de dados da EU[120].

1.3.LEGISLAÇÃO COMPARADA.

Com a publicação da obra *Grundzüge des Naturrechts oder der Rechtsphilosophie*,[121] da autoria de Karl David August Roder, na Alemanha, em 1846, começa a manifestar-se uns dos quadros da doutrina relativa ao direito à privacidade e à vida privada, ao considerar que incomodar alguém com

[119] 28. COMISSÃO EUROPEIA - Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Art.º 1

[120] EUR-LEX - Proteger la privacidad de los ciudadanos de la UE en las transferencias de datos a los Estados Unidos. [Em linha].

[121] Fundamentos da Lei Natural ou da Filosofia do Direito (tradução minha)

perguntas impertinentes ou entrar em um aposento sem se fazer anunciar são atos de violação ao direito natural à vida privada.[122]

Não obstante, a maioria dos doutrinários, considera que o ponto de partida da formulação do direito à intimidade e à vida privada nasce com a publicação do artigo intitulado *Right to Privacity*[123] na *Harvard Law Reviem*, em 1890, dos autores Samuel Dennis Warren e Lois Dembitz Brandeis, advogados norte-americanos, os quais preocupados pelas constantes invasões da vida pessoal e familiar, traçaram os contornos de um direito à privacidade também denominado *Right to be let alone,*[124] fundamentado em bases morais, e na inviolabilidade da personalidade, para proteger as emoções, pensamentos e sentimentos íntimos do individuo, seja qual fora sua forma de expressão.[125]

No decorrer dos anos, o Código Civil **Italiano** de 1942, reconheceu o direito à proteção do nome e da imagem nos seus artigos 7.º e 10º respetivamente, possibilitando a inibição do uso ilegítimo deles;

> *"Art. 7 Tutela del diritto al nome*
> *La persona, alla quale si contesti il diritto all'uso del proprio nome o che possa risentire pregiudizio dall'uso che altri indebitamente ne faccia, può chiedere giudizialmente la cessazione del fatto lesivo, salvo il risarcimento dei danni.*
> *L'autorità giudiziaria può ordinare che la sentenza sia pubblicata in uno o più giornali.*
>
> *Art. 10 Abuso dell'immagine altrui*
> *Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione e dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni."*[126]

Nesse enquadramento, observa-se na Constituição italiana de 1947, o art.º 15 que, não pode haver uma liberdade de comunicação efetiva se o segredo não for garantido, e o último parágrafo introduz uma reserva absoluta da lei e uma reserva de jurisdição:

---

[122] MACEIRA, Irma – op. cit..p.30

[123] Direito à Privacidade (tradução minha)

[124] Direito a estar só (tradução minha)

[125] MACEIRA, Irma – op. cit..p.31

[126] Regio Decreto 16 marzo 1942, n. 262 - **Codice civile.** Art.º 7 Proteção do direito ao nome. A pessoa, que é desafiada pelo direito de usar seu nome ou que pode ser prejudicada pelo uso que outras pessoas fazem incorretamente, pode solicitar judicialmente a rescisão do evento prejudicial, com exceção da indenização por danos. A autoridade judicial pode ordenar que a sentença seja publicada em um ou mais jornais. (tradução minha)
Art.º 10 Abuso da imagem dos outros. Se a imagem de uma pessoa ou de seus pais, cônjuge ou filhos tiver sido exposta ou publicada fora dos casos em que a exposição ou publicação é permitida por lei, ou com prejuízo para o decoro ou reputação da pessoa ou disse, a autoridade judicial, a pedido do interessado, pode ordenar a suspensão do abuso, com exceção da indenização por danos. (tradução minha)

> *"ART. 15. La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge."*[127]

No **Equador**, a proteção de dados pessoais tem a sua gênese com a Constituição de 1967, que mencionou no seu capítulo II, sobre os Direitos da Pessoa, em particular, o artigo 28º que:

> ***"Artículo 28.-*** *Sin perjuicio de otros derechos que se deriven de la naturaleza de la persona, el Estado le garantiza: (...) 4. El derecho a la honra y a la intimidad personal y familiar;"*[128]

Mais tarde, este direito é reforçado com o direito de "*Habeas Data*"[129], garantia constitucional denominada metade em latim "*Habeas*" retirada do antigo instituto de "*Habeas Corpus*" e metade em inglês *"Data"* que significa informação ou dados e que em síntese, uma tradução literal da frase seria: "*que você tenha os dados*", "*que os dados venham*" ou "*mantenha os seus dados*"; procura proteger a integridade moral das pessoas, garantindo a sua informação privada, e foi consagrada no artigo 94º da CONSTITUIÇÃO POLÍTICA DA REPÚBLICA DO EQUADOR em 1998, afirmando que:

> *"Art. 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.*
> *Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional."*[130]

---

[127] ASSEMBLEA COSTITUENTE – COSTITUZIONE DELLA REPUBBLICA ITALIANA. Art.º 15 A liberdade e o sigilo da correspondência e de todas as outras formas de comunicação são invioláveis. A sua limitação só pode ocorrer por ato fundamentado da autoridade judicial com as garantias estabelecidas por lei. (Tradução minha)

[128] ASAMBLEA NACIONAL CONSTITUYENTE CONSTITUCIÓN DE 1967. ECUADOR. Art.º 28 Sem prejuízo de outros direitos decorrentes da natureza da pessoa, o Estado garante: (...) 4. O direito à honra e a privacidade pessoal e familiar. (tradução minha)

[129] Como sustenta Franco Bernabé, Em América Latina, o direito de poder acessar e modificar os próprios dados pessoais, é comumente chamado "habeas data", expressão com a qual se faz referencia ao direito de controle ao autodeterminação sobre as informações que lhe dizem respeito. (Liberdade vigiada p. 213).

[130] ASAMBLEA NACIONAL CONSTITUYENTE - CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DEL ECUADOR. Art.º 94 Toda pessoa terá o direito de acessar aos documentos, bancos de dados e relatórios que sobre si próprios ou seus bens, constem em entidades públicas ou privadas, bem como conhecer o uso feito e a finalidade deles. Poderá solicitar ao respetivo funcionário, a atualização dos dados ou a sua retificação, eliminação ou cancelamento, se eles forem errôneos ou prejudicam seus direitos de forma ilegítima. Se a falta de atenção causará danos, a parte afetada pode exigir indemnização. A lei estabelecerá um procedimento especial para acessar os dados pessoais contidos nos arquivos relacionados à defesa nacional. (tradução minha)

Este direito permite que uma pessoa aceda às informações sobre ela ou seus ativos num registro, relatório ou banco de dados. Saber desde quando os dados são armazenados pelo possuidor e quais são as seguridades para prevenir a divulgação não autorizada. Além disto, permite conhecer, o que uso estão recebendo os dados, e solicitar que seus dados sejam atualizados, corrigidos, anulados ou eliminados; Também pressupõe o objetivo de garantir a confidencialidade de certas informações legalmente obtidas para impedirm o seu conhecimento por parte de terceiros, conferindo ao proprietário o poder de disposição e controle dos seus dados pessoais, representando desta forma uma garantia que se tornou muito importante com o desenvolvimento da tecnologia atual, pois é um direito fundamental à proteção de informações privadas.

O que precede é consistente com o disposto no parágrafo 2 do Artigo 18° da Constituição da República do Equador publicado no Registo Oficial n° 449,o dia 20 de outubro de 2008, indicando que:

> *"Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho: (...) 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información*"[131]

Isto, em concordância com o art.° 92 ibidem, o qual indica que a pessoa afetada poderá demandar pelos danos relacionados aos seus dados pessoais, conhecer o uso feito deles, a sua finalidade, o origem e o destino:

> ***"****Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico.*
> *Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.*

[131] ASAMBLEA NACIONAL CONSTITUYENTE - CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR 2008. Art.° 18.- Todas as pessoas, individual ou coletivamente, têm o direito: (...) 2. Acessar livremente informações geradas em entidades públicas ou em entidades privadas que gerenciam fundos estaduais ou desempenham funções públicas. Não haverá reserva de informações, exceto nos casos expressamente estabelecidos na lei. Em caso de violação de direitos humanos, nenhuma entidade pública negará a informação. (tradução minha)

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación.
En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias.
Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez.
La persona afectada podrá demandar por los perjuicios ocasionados."[132]

Portanto, o Habeas Data fornece a cada pessoa um meio ou uma ação para impedir que terceiras pessoas não autorizadas utilizem indevidamente as informações pessoais sem autorização do titular, protegendo o seu direito à dignidade, do qual derivam seus direitos de privacidade e privacidade.

Por outro lado, a proteção da intimidade em Internet no Equador, baseia-se no núm. 19 e 21 do Artigo 66° da sua Constituição, afirmando que reconhece e garante às pessoas:

"*19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"*[133] ,

"21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación."[134]

A primeira Lei de Proteção de Dados tivesse sido aprovada pela **Alemanha**, em 1970. Depois de três anos, em 1973, a **Suécia** emite sua lei nesta matéria e, nesse mesmo ano, nos **Estados Unidos**

---

[132] ASAMBLEA NACIONAL CONSTITUYENTE - CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR 2008. Art.° 18.- Todas as pessoas, individual ou coletivamente, têm o direito: (...) 2. Acessar livremente informações geradas em entidades públicas ou em entidades privadas que gerenciam fundos estaduais ou desempenham funções públicas. Não haverá reserva de informações, exceto nos casos expressamente estabelecidos na lei. Em caso de violação de direitos humanos, nenhuma entidade pública negará a informação. (tradução minha)

[133] ASAMBLEA NACIONAL CONSTITUYENTE - CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR 2008. Art.° 66 n.° 19.- O direito à proteção de dados pessoais, que inclui o acesso e a decisão sobre informações e dados dessa natureza, bem como sua correspondente proteção. A coleta, arquivamento, processamento, distribuição ou disseminação desses dados ou informações exigirá a autorização do titular ou o mandato da lei. (tradução minha)

[134] ASAMBLEA NACIONAL CONSTITUYENTE - CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR 2008. Art.° 92.- Toda pessoa, por seus próprios direitos ou como representante legítimo para esse fim, terá o direito de saber da existência e de aceder aos documentos, dados genéticos, bancos ou arquivos de dados pessoais e relatórios que sobre si mesmo, ou sobre seus ativos, constem em entidades públicas ou privadas, em suporte material ou eletrónico.
Da mesma forma, o titular terá o direito de saber o uso que é feito deles, seu propósito, a origem e o destino das informações pessoais e o tempo de validade do arquivo ou banco de dados. As pessoas responsáveis pelos bancos ou arquivos de dados pessoais podem divulgar as informações armazenadas com a autorização do titular ou da lei. A pessoa titular dos dados pode solicitar à pessoa responsável o acesso livre ao arquivo, bem como atualizar os dados, retificando, eliminando ou cancelando. No caso de dados sensíveis, cujo arquivo deve ser autorizado por lei ou pelo titular, será necessária a adoção das medidas de segurança necessárias. Se o seu pedido não for atendido, ele poderá acudir ao juiz. A pessoa afetada poderá demandar pelos danos causados. (tradução minha)

de América foram publicados os *Fair Information Practice Principles*[135], desenvolvidos pelo *Department of Health, Education and Welfare*,[136] que, junto com o intensivo uso de computadores e de uma tecnologia complexa de informação que capta, conserva, usa e difunde informação pessoal em detrimento da privacidade individual, motivou a promulgação da chamada Lei de Privacidade nesse país no ano de 1974. Lei que foi modificada várias vezes devido à dinâmica e flexibilidade que as novas tecnologias da informação impõem à sociedade [137]

Nos Estados Unidos de Norteamérica, segundo Franco Bernabé, a privacidade é considerada um direito do consumidor e não um direito fundamental do cidadão como acontece na Europa. Essa autoria desvela que, para os americanos a proteção da privacidade é um interesse individual que deve ser entendido junto aos interesses dos negócios, por isso, as violações à privacidade são competência da *Federal Trade Commission* (Comissão Federal de Comércio).[138]

Além disso, as leis estadunidenses permitem aos operadores da Tecnologia da Informação e Comunicação, orientar os seus sistemas visando a exploração e o uso extensivo dos dados pessoais, gerenciando a coleta de dados para o seu benefício, em desvantagem dos interesses do consumidor.[139]

Na **Argentina**, o seu Código Civil do ano de 1975, prescreve no *art.º1071 bis* sobre a proteção da privacidade que:

> *"Art. 1.071 bis.. El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; ..."*[140]

---

[135] Princípios práticos de Justos de Informação (tradução minha)

[136] TEIXEIRA, Angelina – A Chave para a Regulamentação da Protecção de Dados. p. 7

[137] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 65

[138] BERNABÉ, Franco. – LIBERDADE VIGIADA. p.84

[139] BERNABÉ, Franco. – op. cit., p. 87

[140] Cit. por MACEIRA, Irma – op. cit..p.84

Na Constituição **Espanhola** de 1978, instaura um limite no que se refere ao exercício de direitos reconhecidos, incluindo o direito à intimidade e o segredo das comunicações, visando a manutenção da soberania individual, e o uso de tecnologia da informação, pelo que estabeleceu no artigo 18, que:

> *Art.°18.1 (...) "Se garantiza el derecho al honor, a la intimidad personal y familiar y própria (Sic.) imagen,...4 La ley limitara el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*[141]

Entretanto, o Real Decreto-lei 14/99 espanhol, este estabeleceu que as certificadoras não podem armazenar e nem copiar os dados da chave privada do subscritor do documento,[142] e em quanto à proteção civil, esta é fundamentada no direito à indemnização por danos de natureza moral derivados de interferência ilegítima nos direitos da proteção de dados pessoais.

Do ponto de vista da proteção criminal, o Código Penal espanhol de 1995 prevê o art.° 197.1, o tipo básico do crime de descoberta e divulgação de segredos, que protege o direito fundamental à intimidade pessoal garantido pela Constituição da Espanha, e que decreta:

> *Art.° 197.1 El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*[143]

O art.° 197.1 mencionado, contém uma tipologia em que existem dois tipos básicos definidos por diferentes modalidades de comissários, como a apreensão de papéis, cartas, *e-mails* ou outros documentos ou efeitos pessoais, ou a interceção de telecomunicações ou o uso de dispositivos técnicos para ouvir, transmitir, gravar ou reproduzir som ou imagem, ou qualquer outro sinal de comunicação. O

---

[141] Cit. por MACEIRA, Irma, op. cit., p.38 Art.° 18.1 (...) É garantido o direito de honra, à privacidade pessoal e familiar e a própria imagem... 4 A lei limitará o uso da informática para garantir a honra e intimidade pessoal e familiar dos cidadãos e o pleno exercício de seus direitos. (Tradução minha)

[142] Cit. por MACEIRA, Irma – op. cit..p.91

[143] Cit. por PLAZA PENADÉS, Javier (Dir.) [et al.] – DERECHO Y NUEVAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. p.1144. Art.° 197.1 Aquele que, para descobrir os segredos ou violar a intimidades de outro, sem seu consentimento, apreende seus papéis, cartas, e-mails ou quaisquer outros documentos ou efeitos pessoais ou intercepta suas telecomunicações ou usa dispositivos técnicos de Ouvir, transmitir, gravar ou reproduzir som ou imagem, ou qualquer outro sinal de comunicação, será punido com prisão de um a quatro anos e multa de doze a vinte e quatro meses. (Tradução minha)

que é relevante é que é um crime em qualquer uma das suas versões que não exige para sua consumação a descoberta efetiva do segredo ou da privacidade do sujeito passivo, uma vez que o uso do sistema de gravação ou reprodução de som ou imagem é suficiente (elemento objetivo) juntamente com o propósito indicado no preceito de descobrir segredos ou violar a privacidade (elemento subjetivo), ou seja, o tipo básico é consumido pelo mero facto de capturar imagens com o objetivo de violar a privacidade.

Em 1981, **França** publica a Lei de Imprensa, introduzindo limitações no que toca à vida privada.[144] O Código Civil francês, por sua vez, afirma, o direito de cada um ao respeito da sua vida privada, no artigo 9º:

> ***"Article 9*** *Chacun a droit au respect de sa vie privée.*
> *Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé."*[145]

No **Brasil**, a dignidade da pessoa humana e os direitos da personalidade, estão previstos na Contituição Federal de 1988 como um direito fundamental, decorrendo amplamente o direito à vida privada, à honra, à intimidade, à aimagem entre outros, como vemos no Art.º 5 no inciso X da constituição; Além do mais, o inciso XII, garante a inviolabilidade do sigilo de correspondência e das comunicações telegráficas e telefónicas , e a alínea LXXII do mesmo artigo, garante aos cidadãos o direito de acessar e modificar as informações que o governo tem sobre eles.[146]

> "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

---

[144] MACEIRA, Irma, op. cit., p.32. Art. 1.071 bis. Qualquer pessoa que interfira arbitrariamente na vida de outros, publicando retratos, espalhando correspondência, mortificando aos outros em seus costumes ou sentimentos, ou perturbando de qualquer forma sua privacidade, e o facto não for uma ofensa criminal, estará obligado cessar em tais atividades, se antes de não terem cessado e pagar uma compensação que o juiz estabelecerá de forma equitativa, de acordo com as circunstâncias (Tradução minha)

[145] CODE CIVIL DES FRANÇAIS Art.º 9 Todos têm o direito ao respeito pela vida privada. Os juízes podem, sem prejuízo da compensação por danos sofridos, prescrever quaisquer medidas, como sequestro, apreensão e outros, para prevenir ou pôr fim a uma invasão de privacidade: essas medidas podem, se houver urgentemente, para ser ordenado em processos urgentes ". (Tradução mina)

[146] Cit. por BERNABÉ, Franco. – op. cit., p. 213

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> LXXII - conceder-se-á *habeas data:*
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"[147]

Nesse cenário, O Código Civil brasileiro de 2002, permitem ao prejudicado a prerrogativa de pleitear que cesse o ato abusivo ou ilegal, ou ainda assegurando o direito à indenização.

> Código Civil de 2002:
>
> "Art.º 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
> Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
>
> Art.º 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".[148]

Por outro lado, a Lei 12.965/14 do Brasil, que trata do Marco Civil da Internet do ano 2014, combina princípios, garantias, direitos e deveres para o uso da Internet nesse país. O texto do projeto trata de questões como a neutralidade da rede, a privacidade, a retenção de dados, a função social que a rede precisará cumprir especialmente garantindo a liberdade de expressão e a transmissão do conhecimento, além de impor obrigações de responsabilidade para os cidadãos, usuários e fornecedores. Uns dos princípios basilares desse diploma é a proteção da privacidade dos usuários da internet assinalado no art.º 3:

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

[147] SENADO FEDERAL - CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL. Art.º 5

[148] CONGRESSO NACIONAL - CÓDIGO CIVIL. Art.º 20, Art.º21

II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;"[149]

Além disto, o Marco Civil da Internet institui no art.º 7 que:

"Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;..."[150]

A **Colômbia**, em 1999 impõe a proteção à confidencialidade das informações do subscritor do documento eletrónico com a Lei 527/99 no seu art.º 32, e com o Decreto 1747/200 impede que as certificadoras obtenham os dados da chave privada do subscritor do documento eletrónico, conforme art.º 13 num. 7:[151]

"*ARTICULO 13. DEBERES. Además de lo previsto en el artículo 32 de la Ley 527 de 1999, las entidades de certificacacion deberán: [...] 7. Abstenerse de acceder o almacenar la clave privada del suscriptor. [...]*"[152]

No **Peru**, o Congresso da República promulgou no ano 2000, a *LEI DE ASSINATURAS E CERTIFICADOS DIGITAIS* (Lei 27.269), que visa assegurar a confidencialidade no seu art.º 8 ao dispor que a autoridade certificadora deve armazenar e resguardar os dados do solicitante da certificação e do documento eletrónico e revelá-lo somente por meio de ordem judicial ou do subscritor.[153]

Do mencionado, observa-se várias leis dos Estados soberanos que acolhem o direito à proteção de dados pessoais de forma expressa e autônoma (Itália, Suécia, Brasil), ou como derivação do direito à intimidade ou vida privada já estabelecida (Estados Unidos, Argentina, França, Equador).

---

[149] CONGRESSO NACIONAL - MARCO CIVIL DA INTERNET. Art.º 3
[150] CONGRESSO NACIONAL - MARCO CIVIL DA INTERNET. Art.º 7
[151] MACEIRA, Irma – op. cit..p.92
[152] Cit. por MACEIRA, Irma – op. cit..p.92
[153] MACEIRA, Irma – op. cit..p.91

1.4. A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS EM PORTUGAL.

Em 1976, a proteção dos dados pessoais foi consagrado como um direito fundamental[154] no texto constitucional da República Portuguesa *Parte I (Direitos e Deveres Fundamentais),* dentro do *Titulo II* que tratava dos *Direitos, Liberdades e Garantias*[155], no seu art.º 35 sob a epígrafe "*Utilização da informática*".

Embora de uma forma indireta, foi a primeira Constituição do mundo em proteger expressamente os dados pessoais dos cidadãos, da potencial agressividade e riscos da informática,[156] garantindo que todo cidadão gozava de acesso à informação sobre a sua pessoa, de quaisquer registros, em bancos de dados informatizados e do fim a que se destinavam, assegurando também o traçamento dessas informações a terceiras pessoas:

> *ARTIGO 35.º (Utilização da informática) (1976)*
> "1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
> 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
> 3. É proibida a atribuição de um número nacional único aos cidadãos."[157]

Na sétima revisão constitucional do dia 12 de agosto de 2005, é modificado o art.º 35 da Constituição, ao acrescentar a proteção sobre os dados relativos às convicções filosóficas ou politicas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, ficando no seguinte sentido:

> *CRP Artigo 35.º (Utilização da informática) (2005)*

---

[154] O artigo 16.º da CRP que trata sobre o Âmbito e sentido dos direitos fundamentais, estabelece uma cláusula aberta, de não tipicidade ao indicar: "1. Os Direitos fundamentais consagrados na CRP não excluem quaisquer outros constantes das leis e das regras aplicáveis de Direito internacional. 2. Os preceitos constitucionais e legais relativos aos direitos fundamentais devem ser interpretados e integrados de harmonia com a Declaração Universal dos Direitos do Homem."

[155] Os direitos, liberdades e garantias constitucionais, têm uma aplicabilidade imediata, sem necessidade de mediatização legislativa e obrigam tanto às entidades públicas como as privadas de acordo com o múm.1 do art.º 18 da CRP (2005): 1. *Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são diretamente aplicáveis e vinculam as entidades públicas e privadas.*

[156] TEIXEIRA, Angelina – op. cit. p. 7

[157] ASSEMBLEIA CONSTITUINTE - CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. Texto originário da Constituição, aprovada em 2 de Abril de 1976. Art.º 35

> "1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
> 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
> 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
> 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
> 5. É proibida a atribuição de um número nacional único aos cidadãos.
> 6. A todos é garantido livre acesso às redes informáticas[158] de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
> 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."[159]

Estes direitos, que regulam juridicamente problemas levantados pelo uso do computador e das novas tecnologias, constituindo uma primeira expressão do Direito da Informática ou Direito da Eletrónica, compõem o direito fundamental do individuo à *autonomia informacional*, também conhecido como o Direito à *Autodeterminação Informativa,* derivado do direito à privacidade, focado no direito da pessoa de exercer o controle sobre as informações pessoais contidas em registros públicos ou privados e decidir quando e como ela está disposta a permitir que suas informações pessoais sejam divulgadas ou difundidas por ela mesma ou por terceiras pessoas.

Mas este Direito à *Autodeterminação Informativa* não é, somente, um direito de caráter defensivo em face da realização de tratamentos de dados pessoais, como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a difusão ou qualquer outra forma de disponibilização, a comparação ou a

[158] O numero 6 estabelece um direito de acesso à redes informáticas, o que pode ser considerado como um direito fundamental instrumental, potenciador e amplificador de outros direitos e liberdades. Nestes direitos fundamentais pode incluir-se a liberdade de expressão e de comunicação, de informar, de se informar e de ser informado, o direito de associação, reunião e manifestação, o direito de acesso ao conhecimento, à educação e à cultura, bem como o direito de participação democrática, sendo o direito à Internet, igualmente, indispensável à concretização da democracia eletrónica, ou para o acesso à informação administrativa, ou a serviços administrativos eletrónicos, funcionando, neste caso, como pressuposto necessário ao exercício de um *eDireito* ao relacionamento do cidadão com a Administração Pública. Em suma, o direito à Internet, que o n.º 6 do artigo 35.º consagra, é, nesta perspetiva, um direito funcionalizado à garantia de outros direitos, ou ao pleno gozo destes

[159] ASSEMBLEIA CONSTITUINTE - CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. VII Revisão Constitucional [2005]. Art.º 35

interconexão, a limitação, o apagamento ou a destruição dos dados pessoais, além de tudo, dota ao titular dos dados de instrumentos que lhe permitem dispor e controlar os dados pessoais objeto de tratamento que lhe respeitem, seja ele realizado pelo sector público ou pelo sector privado.[160]

Nas palavras de Catarina Sarmento e Castro, "este direito à *Autodeterminação Informativa* é um verdadeiro direito fundamental, com conteúdo próprio (com o seu especial "*Schutzbereich*[161]"), e não apenas uma garantia do direito à reserva da intimidade da vida privada. Embora possa proteger informação íntima, e se assuma, instrumentalmente, como direito-garantia daquela (reserva da intimidade da vida privada seria, então, o direito-*direito*, na noção de VIEIRA de ANDRADE), é também um direito dirigido à defesa de novas facetas da personalidade – é um direito de personalidade[162] – traduzido na liberdade de controlar a utilização das informações que lhe respeitem (desde que sejam pessoais), e na protecção perante agressões derivadas do uso dessas informações"[163]

Dessarte, o poder fascinante, mas ameaçador, das novas tecnologias levara a que muitas ordens jurídicas autonomizassem um direito à *autodeterminação informativa* traduzido num feixe de direitos através dos quais se pretende impedir que o homem se transforme em "simples objeto de informações[164]

O art.º 35 da CRP não é a única referência à proteção de dados e ao uso da tecnologia da informação que a constituição faz, porque, embora não direta e expressamente, sim encontrarmos uma referência indireta ao indicar no seu artigo 26 sobre a reserva da intimidade da vida privada e proteção contra qualquer discriminação ao indicar:

"*Artigo 26.º (Outros direitos pessoais)*

---

[160] Veja-se que o núm. 1 do art.º18 da CRP sobre Força Jurídica estabelece que: "Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas."

[161] Zona protegida. Área pessoal protegida por direitos fundamentais. (Consultado em: https://www.duden.de/suchen/dudenonline/Schutzbereich)

[162] O tribunal Constitucional, no Ac. N.º 6/84, de 18 de Janeiro, interpretou o art.º 1.º da Constituição como fonte do direito geral da personalidade ao indicar: "Tudo parece levar à conclusão de que a nossa Constituição admite e consagra um direito geral de personalidade. O mais poderoso argumento pode equacionar-se assim: a nossa Constituição logo no seu artigo 1.º declara que Portugal è uma República soberana baseada na dignidade da pessoa humana, logo acolhe o princípio de que a todo e qualquer direito de personalidade, isto é, a todo e qualquer aspecto em que necessariamente se desdobra um direito geral de personalidade, deve caber o maior grau de protecção do ordenamento jurídico, ou seja o que assiste aos direitos fundamentais, pois os direitos da personalidade são inerentes à propiá pessoa, não podendo, por isso, ser postergados por qualquer modo, sob pena de se negar o papel de pessoa como figura central da sociedade". Cit. Por Alexandre PINHEIRO, Op. cit. P.763

[163] CASTRO, Catarina Sarmento - O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro. p.11

[164] Cit. por CASTRO, Catarina Sarmento, op cit. p.1

1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação[165].
2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.
3. A lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica[166].
4. A privação da cidadania e as restrições à capacidade civil só podem efectuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos."[167]

Nesse universo de proteção constitucional também encontramos ao art.º 32 núm. 8 relativo às Garantias do processo criminal ao considerar nulas as provas obtidas com a abusiva intromissão na vida privada nas telecomunicações:

"CRP Artigo 32.º (Garantias de processo criminal) (....)
8. São nulas todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações. (...)"[168]

Analogamente, o art.º 34 da constituição protege o sigilo da correspondência e dos outros meios de comunicação:

"*CRP Artigo 34.º (Inviolabilidade do domicílio e da correspondência)*
1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis. (...)
4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal."[169]

Esta proteção também esta no art.º 65 sobre a preservação da intimidade pessoal, número 1:

"*CRP ARTIGO 65.º (Habitação e urbanismo*)

---

[165] O direito à reserva enquanto direito à informação sobre a vida privada é sobre a proteção da informação da vida pessoal, e da identidade da pessoa.

[166] Inclui dados relativos à Identidade, marcas ou sinais de identidade, filiação, residência, numero de telefone, estado de saúde, vida conjugal, afetiva do individuo, vida de lar, património e situação financeira (Acórdão 355/97). Mesmo que a obtenção de informação não tenha sido ilícita, a revelação a terceiros da informação pode ser ilícita.

[167] ASSEMBLEIA CONSTITUINTE - CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. VII Revisão Constitucional [2005]. Art.º 26

[168] ASSEMBLEIA CONSTITUINTE - CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. VII Revisão Constitucional [2005]. Art.º 32

[169] ASSEMBLEIA CONSTITUINTE - CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. VII Revisão Constitucional [2005]. Art.º 34

1. Todos têm direito, para si e para a sua família, a uma habitação de dimensão adequada, em condições de higiene e conforto e que preserve a intimidade pessoal e a privacidade familiar."[170]

Com a Lei n.º 67/98, de 26 de Outubro de 1998, de Proteção Dados Pessoais, foi transposta para a ordem jurídica portuguesa[171] a Diretiva n.º 95/46/CE[172], do PE e do Conselho, 24/10/95, relativa à proteção das pessoas singulares[173] no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

No art.º7.º desta Lei, se consideram que os dados relativos a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, são dados sensíveis, e adita os dados referentes a origem racial, saúde, vida sexual e dados genéticos. No que respeita aos dados de saúde, a jurisprudência constitucional – Ac. n.º 355/97, trata-os como dados sensíveis, apesar da ausência do art.º 35.º da CRP, procedendo à sua integração nos dados originários da esfera mais privada da vida íntima da pessoa, [174] por isso, tais dados, também fazem parte do estrito dever de sigilo profissional.

Assim mesmo, como em qualquer tratamento de dados pessoais, esta lei contempla princípios relacionados à proteção de dados, transunto do artigo da Diretiva, que faz eco ao artigo 5.º da Convenção n.º 108 do Conselho da Europa, e que tratam da legitimidade, a proporcionalidade, a transparência, e dos dados adequados.

---

[170] ASSEMBLEIA CONSTITUINTE - CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA. VII Revisão Constitucional [2005]. Art.º 65

[171] Note-se que: "...2. As normas constantes de convenções internacionais regularmente ratificadas ou aprovadas vigoram na ordem interna após a sua publicação oficial e enquanto vincularem internacionalmente o Estado Português. 3. As normas emanadas dos órgãos competentes das organizações internacionais de que Portugal seja parte vigoram directamente na ordem interna, desde que tal se encontre estabelecido nos respectivos tratados constitutivos. 4. As disposições dos tratados que regem a União Europeia e as normas emanadas das suas instituições, no exercício das respectivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União, com respeito pelos princípios fundamentais do Estado de direito democrático (CRP Artigo 8.º sobre o Direito internacional).

[172] Atualmente esta Diretiva foi revogada pelo REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. No entanto, e de conformidade com o comunicado da CNPD de 28 de maio de 2018: "Enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98, de 26 de outubro, esta lei manter-se-á em vigor em tudo o que não contrarie aquele diploma europeu. No que diz respeito aos tratamentos de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º 67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680." (COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – Comunicado da CNPD Aplicação do novo quadro legal de proteção de dados. [Em linha]: Lisboa, 25 de maio de 2018, [Consult. 18 agosto 2018]. Disponível na internet https://dre.pt/documents/10184/826042/Comunicacao+CNPD_25_5_2018.pdf/87e28703-4e8c-4439-9ba9-f0f7b75ceab1)

[173] Da mesma forma, o atual REGULAMENTO (UE) 2016/679 estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conforme o menciona o seu art.º 1 núm.1. Unicamente se excluem de forma expressa: "...ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública." (Art.º 2 núm. 2, ibidem)

[174] PINHEIRO, Alexandre – Privacy e Protecção de dados pessoais; a construção dogmática do direito à identidade informacional. p.723

O princípio de Legitimidade significa que os dados sejam recolhidos para o fim lícito estabelecido na norma, e só devem ser conservados para a época e as necessidades do objetivo inicial. Quer dizer, que eles devem sempre ser justificados com a natureza da atividade ao objetivo inicial, sendo proibido coletar dados por meios fraudulentos, desleais ou ilegais, e sem prejuízo das responsabilidades criminais que isso possa implicar, também é proibido processar os dados assim obtidos.

O artigo 5º da Lei n.º 67/98 concede este princípio da legitimidade[175] do processamento de dados, os quais, uma vez determinados os objetivos que perseguem, os dados obtidos e processados devem ser utilizados de acordo com a finalidade que foi invocada no momento da recolha, de um modo seguro e confidencial, isto é, que a natureza dos dados deve corresponder ao objetivo prosseguido. E sempre que a finalidade que preside à utilização seja alterada, necessário se tornará um novo consentimento do titular.[176] "Os dados devem ser conservados apenas durante o período necessário de acordo com as finalidades da recolha e do tratamento (...) há que estabelecer um prazo adequado para a conservação dos dados, de modo a evitar uma apropriação perpétua de aspetos muito vastos da vida pessoal do titular dos dados."[177]

> *"Artigo 5.º Qualidade dos dados*
> 1. Os dados pessoais devem ser:
> *a*) Tratados de forma lícita e com respeito pelo princípio da boa fé;
> *b*) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;
> *c*) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;

[175] No atual Regulamento (UE) 2016/679 - Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, este princípio encontra-se no art.º 5 ao indicar: Princípios relativos ao tratamento de dados pessoais 1. Os dados pessoais são: a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»); b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º n.º 1 («limitação das finalidades»); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»); d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»); e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»); f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»); 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»).

[176] Cit. por MONTE, Mario; BRANDÃO, Paulo; **Coord.(s)** - op. cit. P.217

[177] Cit. por MONTE, Mario; BRANDÃO, Paulo; **Coord.(s)** - op. cit. P.218

d) Exactos e, se necessário, actualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou rectificados os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;
e) Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.
2. Mediante requerimento do responsável pelo tratamento, e caso haja interesse legítimo, a CNPD pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao referido na alínea *e*) do número anterior.
3. Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores."[178]

O princípio de proporcionalidade[179], que também se aprecia no art.º 5 núm. 1, letra "c" ibidem, trata que os dados recolhidos têm que ser apenas os necessários e não excessivos, atendendo á referida finalidade, quer dizer, que os dados devem ser proporcionais aos objetivos e ao tratamento e processamento, pelo que os dados, não podem exceder aquilo que é realmente necessário para a prossecução das referidas finalidades.[180]

O princípio de transparência[181] faz referência que os dados pessoais devem processar-se de forma transparente e, o titular dos dados deve contar com a informação nos termos do artigo 2ºe 10º, da Lei n.º 67/98, isto é, que o titular tem de ser explicitamente informado sobre os objetivos da recolha dos dados, o propósito e outras informações necessárias para garantir o tratamento justo em relação à pessoa em causa, para que possa estar ciente das consequências de dar o seu consentimento[182]:

"Artigo 2.ºPrincípio geral
O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais."[183]

"Artigo 10.º Direito de informação

[178] Lei n.º 67/98 Lei de Protecção de Dados Pessoais. Art.º 5

[179] No atual Regulamento (UE) 2016/679 - Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, este princípio encontra-se no art.º 5 já citado.

[180] Cit. por MONTE, Mario; BRANDÃO, Paulo; Coord.(s) - op. cit. P.218

[181] No atual Regulamento (UE) 2016/679 - Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, este princípio encontra-se nos artigos: 12º, 13º, 14º

[182] A necessidade de consentimento é derivada da capacidade de cada pessoa de decidir quais dados e em quais circunstâncias pode estar sujeita o tratamento e cessão de dados, e quem tem permisso para realizar tais atos.

[183] Lei n.º 67/98 Lei de Proteção de Dados Pessoais. Art.º 2

1. Quando recolher dados pessoais directamente do seu titular, o responsável pelo tratamento ou o seu representante deve prestar-lhe, salvo se já dele forem conhecidas, as seguintes informações:
a) Identidade do responsável pelo tratamento e, se for caso disso, do seu representante;
b) Finalidades do tratamento;
c) Outras informações, tais como:
Os destinatários ou categorias de destinatários dos dados;
O carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder;
A existência e as condições do direito de acesso e de rectificação, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir ao seu titular um tratamento leal dos mesmos.
2. Os documentos que sirvam de base à recolha de dados pessoais devem conter as informações constantes do número anterior.
3. Se os dados não forem recolhidos junto do seu titular, e salvo se dele já forem conhecidas, o responsável pelo tratamento, ou o seu representante, deve prestar-lhe as informações previstas no n.º 1 no momento do registo dos dados ou, se estiver prevista a comunicação a terceiros, o mais tardar aquando da primeira comunicação desses dados.
4. No caso de recolha de dados em redes abertas, o titular dos dados deve ser informado, salvo se disso já tiver conhecimento, de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.
5. A obrigação de informação pode ser dispensada, mediante disposição legal ou deliberação da CNPD, por motivos de segurança do Estado e prevenção ou investigação criminal, e, bem assim, quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação do titular dos dados se revelar impossível ou implicar esforços desproporcionados ou ainda quando a lei determinar expressamente o registo dos dados ou a sua divulgação.
6. A obrigação de informação, nos termos previstos no presente artigo, não se aplica ao tratamento de dados efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária."[184]

Outro princípio é que os dados deve ser adequados[185] aos fins conforme o previsto no artigo 5º, núm. 1, letra "c" e "d", da Lei n.º 67/98, desta maneira, os dados devem ser pertinentes, apropriados, mantidos corretos o que implica uma avaliação cuidadosa da recolha para o processamento de dados, a qual deve tentar ser feita com a maior precisão possível, sendo que qualquer modificação adicional de tal propósito só será legítima se for compatível com o objetivo inicial. Se os dados incorretos ou

[184] Lei n.º 67/98 Lei de Protecção de Dados Pessoais. Art.º 10

[185] No atual Regulamento (UE) 2016/679 - Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, este princípio encontra-se no art.º 5 dantes citado.

incompletos devem ser corrigidos ou retificados, ou apagados de ofício, para isso a pessoa responsável pelo tratamento deve ser diligente.

Com o DECRETO-LEI Nº 47/344, de 25 de Novembro de 1966 expediu-se o CÓDIGO CIVIL PORTUGUÊS, e com a sua atualização no ano de 1999 mediante a Lei 59/99, encontramos normas orientadas à proteção de dados pessoais ao tratar da tutela geral da personalidade, o direito ao nome, e à reserva da intimidade, como a limitação aos direitos da personalidade:

> "*CC ARTIGO 70º (Tutela geral da personalidade*)
> 1. A lei protege os indíviduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.
> 2. Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida."[186]
>
> ***"****CC ARTIGO 72º (Direito ao nome*)
> 1. Toda a pessoa tem direito a usar o seu nome, completo ou abreviado, e a opor-se a que outrem o use ilicitamente para sua identificação ou outros fins...."[187]
>
> "*CC ARTIGO 80º (Direito à reserva sobre a intimidade da vida privada)*
> 1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem.
> 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas."[188]
>
> "*CC ARTIGO 81º (Limitação Voluntária dos Direitos de Personalidade)*
> 1. Toda a limitação voluntária ao exercício dos direitos de personalidade é nula[189], se for contrária aos princípios da ordem pública.
> 2. A limitação voluntária, quando legal, é sempre revogável, ainda que com obrigação de indemnizar os prejuízos causados às legítimas expectativas da outra parte."[190]

[186] DECRETO-LEI nº 47/344, Código Civil Português. Art.º 70

[187] DECRETO-LEI nº 47/344, Código Civil Português. Art.º 72

[188] DECRETO-LEI nº 47/344, Código Civil Português. Art.º 80

[189] A limitação voluntária é nula, quando o consentimento não é libre, sendo este condicionado a algum benefício. Em princípio, os dados pessoais devem ser coletados para um propósito legítimo e proporcional à legitimidade pretendida.

[190] DECRETO-LEI nº 47/344, Código Civil Português. Art.º 81

Levando em conta que um dos princípios básicos da legislação de proteção de dados pessoais é a segurança da informação incluído tudo o ficheiro[191] seja este automatizado ou não[192], é proibido o registro de dados pessoais em ficheiros que não atendam às condições de integridade e segurança determinadas nos regulamentos. Se for o caso, a pessoa responsável, ou o encarregado pelo tratamento, deve adotar as medidas técnicas e organizacionais necessárias para garantir a segurança dos dados pessoais e evitar a sua alteração, perda, tratamento ou acesso não autorizado.[193]

Esta proteção integra diferentes posições jurídicas como a disposição legal que autoriza o tratamento de dados; o consentimento do titular; o direito de acesso à informação recolhida, bem como a proibir o aceso de terceiros à mesma; direito de retificação ou apagamento de dados; e garantia de intervenção da autoridade de controlo como a CNPD e de normalização como a ANACOM relativamente ao cumprimento das disposições constitucionais e legais aplicáveis.[194]

A Comissão Nacional de Proteção de Dados é uma entidade administrativa nacional de Controlo de Dados Pessoais, independente com poderes de autoridade, que funciona junto da Assembleia da República e que tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei, cooperando com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro, e que tem como atribuições[195]:

> Controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais; Emitir parecer prévio sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos comunitários ou

---

[191] «Ficheiro», qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico (Art.º 4 núm. 6 do REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016). Levando em conta que um dos princípios básicos da legislação é a segurança da informação, é proibido o registro de dados pessoais em ficheiros que não atendam às condições de integridade e segurança determinadas nos regulamentos. Se for o caso, a pessoa responsável, ou o encarregado pelo tratamento, deve adotar as medidas técnicas e organizacionais necessárias para garantir a segurança dos dados pessoais e evitar sua alteração, perda, tratamento ou acesso não autorizado (PLAZA PENADÉS, Javier (Dir.) [et al.] – DERECHO Y NUEVAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. P.1154)

[192] O Regulamento (UE) 2016/679 - Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, "aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados". (Art.º2 núm.1)

[193] PLAZA PENADÉS, Javier (Dir.) [et al.] – DERECHO Y NUEVAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN. P.1154

[194] PINHEIRO, Alexandre – op. cit. P. 772

[195] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - O que é a CNPD. [En linha]

> internacionais relativos ao tratamento de dados pessoais; Exercer poderes de investigação e inquérito, podendo para tal, aceder aos dados objeto de tratamento; Exercer poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, assim como o de proibir temporária ou definitivamente o tratamento de dados pessoais; Advertir ou censurar publicamente o responsável do tratamento dos dados, pelo não cumprimento das disposições legais nesta matéria; Intervir em processos judiciais no caso de violação da lei de proteção de dados; Denunciar ao Ministério Público as infrações penais nesta matéria, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de provas.[196]

A Autoridade Nacional de Comunicações é uma entidade administrativa nacional reguladora do sector das comunicações por meio de atividades de normalização que consideram normas europeias e internacionais, em especial as normas constantes da lista desenvolvida pela Comissão Europeia, no âmbito das comunicações eletrónicas, publicada no Jornal Oficial das Comunidades Europeias em 31.12.2001. No seus estatutos conferem independência como entidade orgânica, funcional e financeiramente separada do governo, dotada dos meios necessários ao desempenho de suas funções.

O Decreto-Lei n.º 309/2001 atribui à ANACOM a responsabilidade de assegurar que todos os cidadãos tenham acesso ao serviço universal das comunicações eletrónicas. Este serviço universal trata de um conjunto de serviços mínimos de qualidade especificada, disponíveis para todos os utilizadores, independentemente da sua localização geográfica, e em atenção às condições nacionais, e deve ser oferecido a preços depreciados, enquadrados na proteção dos direitos e interesses dos cidadãos. Por força do art.º 86. Núm. 3 da citada lei, cabe ao governo e ANACOM, adotar soluções mais eficientes e adequadas para assegurar o serviço universal, respeitando os princípios de transparência, objetividade, não discriminação e da proporcionalidade, para reduzir as distorções de mercado e salvaguardar o interesse público.

Embora esta Autoridade não tem poderes legislativos nem jurisdicionais, tem poderes administrativos que permitem regular o setor das telecomunicações, bem como supervisionar e fiscalizar aos atores deste mercado, pudendo até impor sanções administrativas, tais como coimas e suspensões.

---

[196] COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - O que é a CNPD. [En linha]

Além disso, pode resolver disputas entre empresas do setor das telecomunicações, sendo capaz de intervir por meio de licitação de uma das partes, e a sua decisão é vinculante.

Por conseguinte, vemos que a forma como o individuo se apresenta para a sociedade, e a sua dignidade, são elementos que a legislação portuguesa valoriza através de a promulgação da Lei n.º 67/98,[197] a criação e posta em funcionamento da CNPD, a publicação e entrada em vigor da Diretiva 95/46/CE e, o atual Regulamento (UE) n.º 2016/679 de Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, além do impulso que, em forma certeira ou não, tem dado nesta matéria os numerosos foros, seminários, palestras, cursos e outras manifestações, com caracter mais ou menos informativos, que se tem desenvolvido em várias instituições tanto públicas como privadas, promovendo assim os recursos necessários para que, num âmbito ainda reduzido mas significativo pela sua qualidade e incidência, tenha tomado forma e protagonismo a proteção de dados pessoais e a sua privacidade, no fim de preservar a integridade moral, a intimidade, a imagem e as informações pessoais, os quais com o avance da tecnologia, se tem visto mais ameaçados.

[197] Atualmente esta Diretiva foi revogada pelo REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. No entanto, e de conformidade com o comunicado da CNPD de 28 de maio de 2018: "Enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98, de 26 de outubro, esta lei manter-se-á em vigor em tudo o que não contrarie aquele diploma europeu. No que diz respeito aos tratamentos de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º 67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680." (COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – Comunicado da CNPD Aplicação do novo quadro legal de proteção de dados. [Em linha]: Lisboa, 25 de maio de 2018, [Consult. 18 agosto 2018]. Disponível na internet https://dre.pt/documents/10184/826042/Comunicacao+CNPD_25_5_2018.pdf/87e28703-4e8c-4439-9ba9-f0f7b75ceab1)

CAPITULO II

TÉCNICAS INFORMÁTICAS QUE VISAM PROTEGER OS DADOS PESSOAIS.

A segurança e a confiança representam elementos indispensáveis para o desenvolvimento do comércio eletrónico, fornecer serviços e fechar transações financeiras na internet, o qual está tornando-se cada vez mais num lugar privilegiado para a economia global. No entanto, este quadro vê-se afetado pelos contínuos ataques informáticos, que mostram a falta das medidas de segurança dos sistemas informáticos, e evidenciam o ambiente inseguro no que foi concebida a internet.

Com efeito, Franco Bernabé assinala que os riscos crescentes em matéria de segurança informática também são determinados pelo aumento e pela diversificação dos dispositivos através dos quais pode ser levado um ataque. Por exemplo, as janelas temporais existentes entre a entrada no mercado de novos dispositivos e novas tecnologias, assim como a liberação de novos *softwares* oferecem oportunidades ótimas para ataques informáticos, no especial, as primeiras versões dos produtos, sobre os quais revelam medidas de segurança pouco testadas e por conseguinte, são fracas.[198]

Segundo dados de fevereiro de 2012, ao menos 37% dos aplicativos disponíveis gratuitamente na Android Store apresentam grandes riscos à segurança, ao poder estar escondidos códigos capazes de provocar a perda ou a interceção de dados reservados; ou a interceção de números de cartão de crédito ou de senhas para aceder contas bancarias, ademais de outras informações íntimas, chegando a comprometer a privacidade do titular dos dados.[199]

No entanto, os sistemas computacionais não são apenas um problema social, mas também um problema técnico, porque a multiplicidade de sistemas operativos e suas versões, arquiteturas de *hardware*, aplicações, protocolos e requisitos fazem com a definição e implantação de políticas em sistemas distribuídos conectados à Internet seja uma tarefa difícil, quer de pôr em prática quer de

[198] BERNABÉ, Franco. – op. cit., p. 107

[199] BERNABÉ, Franco. – op. cit., p. 108

manter. De mais a mais, a maioria dos utentes usam sistemas operativos COTS,[200] que pelo geral favorecem a facilidade de uso, em detrimento da segurança dos sistemas computacionais.[201]

Segundo o SANS *Intitute*, o tempo médio de sobrevivência de um computador sem proteções espaciais ligado à Internet, normalmente é da ordem de apenas algumas dezenas de minutos.[202]

Ante esta realidade, no presente capítulo, tentaremos explicar de que forma os problemas de segurança dos dados pessoais de pagamento utilizados no comércio eletrónico podem ser identificados, minimizados ou evitados em internet, que é um meio inseguro por natureza.

Destarte, no âmbito da segurança nas atividades de comércio eletrónico é necessário adotar uma série de medidas específicas de proteção contra a fraude. O oferente, como responsável pelo serviço, deve implementar toda a segurança possíveis para a defesa dos sistemas computacionais contra atividades não autorizadas, detetar e prevenir fraudes e ações deliberadas que visam a corrupção ou subversão dos sistemas, e fornecer aos clientes ferramentas que mantenham a sua segurança.

Esta defesa consiste no conjunto de mecanismos e políticas desenhadas, implantadas e concretizadas para diminuir vulnerabilidades que torna um sistema computacional sensível a certos ataques, além de detetar ou anular ataques que são ações ilícitas, e por ultimo, minimizar os danos, riscos ou ameaças decorrentes de ataques bem-sucedidos com planos de contingências que deverão ter em consideração a recuperação do bens ou serviços.[203]

Como destaca André Zúquete[204], as atividades não autorizadas ou ilícitas relacionadas com os dados pessoais podem ser:

---

[200] Refere-se a um produto disponível comercialmente. Ou seja, aquele que é desenvolvido com requisitos genéricos, com uma tecnologia que, quando aplicada corretamente, ajuda a reduzir custos, tanto no desenvolvimento quanto na manutenção dos sistemas, com a intenção de serem vendidos de forma massiva.

[201] ZÚQUETE, André - Segurança em redes informáticas. p. 7

[202] Cit. por ZÚQUETE, André - Segurança em redes informáticas. p. 8

[203] ZÚQUETE, André - Segurança em redes informáticas. p. 6

[204] ZÚQUETE, André - Segurança em redes informáticas. p. 5

i. Acesso a informação: Trata dos acessos às informações confidenciais ou guardadas em sistemas computacionais ou que transitam em redes. Inclui-se as atividades de compilação dessas informações. Pela dificuldade de detetar este ilícito, deve ser previsto e contrariado de forma preventiva.
ii. Alteração de informação: Trata das atividades normalmente detetadas que eliminem ou alterem de forma explícita ou camuflada e sem autorização, informações confidenciais ou reservadas guardadas em sistemas computacionais ou que transitam em redes.

Ainda assim, deve prever-se que as políticas, mecanismos e equipamentos de segurança servem para limitar ou vigiar ações, aliás impor barreiras. Mas se a segurança for excessiva, pode criar fricções com a privacidade das pessoas ou com o funcionamento liberal no âmbito de redes informáticas ao interferir com a atividade das pessoas, pelo que estas últimas terão a tendência de omitir tais políticas e mecanismos de segurança.

As políticas de segurança, são um conjunto de padrões, diretrizes e regras estáveis ao longo do tempo de uma organização que limitam atividades e definem o foco e os requisitos de segurança que devem ser respeitados pelos colaboradores, clientes, parceiros e fornecedores para garantir um determinado resultado, aumentar a conscientização entre cada membro de uma organização sobre a importância e a sensibilidade das informações e os serviços críticos. Esta politica também define as sanções no caso de incumprimento.[205]

Exemplos das políticas de segurança são: O *Principio do Privilégio Mínimo ou Hardering*, no qual os sujeitos devem usufruir, apenas dos direitos suficientes e necessários para exercer as suas atividades, no fim de minimizar os estragos de aceso ou alteração de informação pessoal sim autorização, de forma intencional ou não;[206] Também temos o padrão ISO1779 que fornece um enquadramento de boas práticas para gerir o risco em sistemas informáticos e a segurança pela ocultação (*Security by obscurity*) a qual consiste em não divulgar os mecanismos de segurança publicamente, partindo dessa perspetiva o facto do protocolo ser reservado reforça a sua segurança.[207]

[205] ZÚQUETE, André - op. cit., p. 10
[206] ZÚQUETE, André - op. cit., p. 12
[207] ZÚQUETE, André - op. cit., p. 17

Os mecanismos de segurança são as inúmeras tecnologias em constante evolução que permitem pôr em prática as políticas de segurança. Ao entendimento de ANDRÉ ZÚQUETE[208], entre os mecanismos de segurança temos:

a) Mecanismos de Confinamento[209]: Estes criam barreiras à difusão de atividades, como por exemplo:

   - A zona desmilitarizadas para separação de redes, é uma rede isolada do resto da rede interna, onde apenas os servidores acessíveis pela Internet estão localizados. Dessa forma, se um desses servidores for atacado e comprometido, o restante da rede será protegido.

   - Os ambientes de execução controlada (*sandboxing*), de "caixa de areia" (sandbox), permite executar um programa num espaço fechado e limitado. Ou seja, por meio dessa técnica, os processos recebem um espaço virtual que pode ser controlado, monitorado e automatizado.

b) Mecanismos de Controlo de Acesso: Permite verificar se determinado dado pode ou não executar determinada ação sobre um objeto. Encontramos três tipos principais:

   - O Controle de Acesso Discricionário (DAC): É um método de restringir o acesso a objetos que é baseado na identidade dos sujeitos que pretendem operar ou acessá-los. O exemplo mais representativo é o mecanismo de permissão estabelecido pelo proprietário (usuário/grupo) do sujeito.

   - O Controle de Acesso Baseado em roles (RBAC) consiste na definição de perfis (roles) aos quais são atribuídas uma série de características que se aplicam às permissões e ações que podem ser realizadas, incluindo o controle sobre outros perfis.

   - O controle de Acesso Obrigatório (MAC). Este modelo é o sistema que protege os recursos, comparando rótulos de acesso dos sujeitos, ou seja, a autorização de um sujeito para acessar para um objeto depende dos níveis de segurança que eles têm, que permissão de segurança tem e o nível de sensibilidade.

[208] ZÚQUETE, André - Segurança em redes informáticas. p. 16,17

[209] As *firewalls* ainda que são mecanismos de filtragem, também podem ser usados como mecanismos de confinamento.

c) Mecanismos de Execução Privilegiada: Concedem privilégios acrescidos que sejam executas por utentes que normalmente não usufruem dos mesmos. Um exemplo são os mecanismos *setuid* ou *setgid* num sistema UNIX/Linux. Setuid (Set User ID) é um atributo de arquivo especial válido para o usuário que o sistema regula, para executar os programas selecionados com um determinado ID de usuário previamente indicado. O atributo Setgid possui as mesmas propriedades mas para o grupo. Quer dizer, que um programa será executado com a identificação do grupo que foi indicada, independentemente do usuário que o inicio.

d) Mecanismos de Filtragem: Permitem identificar actividades não necessárias ou autorizadas e evitar que as mesmas sejam ejecutadas. Por exemplo:
- As firewalls, é um único ou vários sistemas, que podem trabalham em conjunto com o antivírus, para controlar o tráfego de entrada e saída dos dados, de modo tal que permite ou bloqueia a passagem dos dados entre as redes, dessa forma evita que a rede protegida fique vulnerável e exposta a ataques.

e) Mecanismos de Registro: Produzem relatórios de atividades, o que permite analisar se o sistema esta a operar correctamente e de forma esperada, assim como detetar causas de erro e anomalias, ainda post mortem de sistemas atacados. Nesse caso, é possível saber a causa do problema ou modus operandi do atacante. Exemplo são: O Registro de eventos (*Event Register*) dos sitemas MS Windows ou Ficheiros de registro (log) usados nos sistemas UNIX/LINUX

f) Mecanismos de Inspecção: Observam o sistema para detetar uma atividade não esperada, legal ou ilícita, ainda pelos abusos efetuados por utentes priviligiados. Um exemplo são os sistemas de deteccão de intrusos - IDS (*Intrusion Detection System*), que é um composto de *hardware* e *software* que trabalham para monitorar e descrever os eventos imprevistos ou anormais do segmento de rede interna, quando ele ainda irá acontecer, está acontecendo no momento ou ainda que já aconteceu, varrendo todo tráfego que por ele passar.

g) Algoritmos Criptograficos e Afins: Na informatica, a criptografia e seus algoritmos permitem concretizar cifras complejas e sofisticas formadas por blocos de *bits*. O poder de cálculo dos computadores passo a tornar viáveis algoritmos de cifra complexos e dificeis de efetar mecanica ou manualmente. Nos contratos eletrónicos, é possível proteger as informações por meio de

criptografia ou cifrado de dados, garantindo a confidencialidade das transações, para que os dados contidos em tais transações sejam acessíveis e compreensível apenas pelas partes envolvidas, e não para terceiros, indivíduos, entidades ou processos não autorizados. A técnica de criptografia é transformar um texto compreensível em um texto criptografado ou ininteligível por meio de uma informação secreta ou chave de criptografia baseada em um método de cálculo ou fórmulas conhecidas como algoritmos.

A criptografia pode ser clasificada segundo o modo de operação em Cifras por Blocos[210] ou Cifras Contínuas[211]; E segundo o tipo de Chave em sistema Simétrico ou Assimetrico[212]. Segundo o tipo de chave, o sistema criptográfico será simétrico, quando usa a mesma chave para as operações de cifrado e decifrado, sendo este um dos sistemas mais rápidos, mas sua desvantagem é que o método ou meio de transporte para divulgar a chave para o destinatário pode ser vulnerado ou interceptado e descoberto a chave secreta com a qual a mensagem seria decifrada, portanto a proteção da chave é essencial. Quando um par de chaves é usado, sendo uma chave privada e a outra pública para separar os processos de cifrado e decifrado, o sistema criptográfico é chamado de chave pública ou assimétrica. Neste último sistema, ambas as chaves são geradas simultaneamente com o algoritmo matemático, embora diferentes umas das outras, são matematicamente relacionadas, porque algo que é cifrado com a chave privada só pode ser decifrado com a chave pública e vice-versa.

Um uso da Criptografia assimentrica, é a assinatura digital, tem um algoritmo para identificar individualmente o valor ou dados que existe em algum campo ou o apêndice original da mensagem eletrónica pertenecente à pessoa com quem se faz uma transação. O remitente do mensagem o cifra com a sua chave privada, e quem conhece a chave pública do remitente, pode decifrar a mensagem e verificar a identidade e autenticidade do remetente, quem é o único

---

[210] Os algoritmos de Cifra por Blocos a sua vez podem ser Simétrico ou Assimétricos. Quanto aos algoritmos de Cifra por Blocos Simétricos mais usados na prática ou em normas, são o DES *(Data encription standard)* que apareceu no ano de 1970 com uma chave pequena de 56-bit. Nos anos 90, surgiu o 3-DES, que se baseava em replicar a técnica DES três vezes; O IDEA *(International Data Encryption Standar*) foi desenhado em 1991 e utiliza uma chave de 128 bits, no entanto, o IDEA nunca foi padronizado; O AES (Advanced Encripted Standard) sugerida pela NIST em 1998 e usa chaves de 128 bits e de 256 bits, e é uma cifra por blocos adotada como padrão de criptografia pelo governo dos Estados Unidos. O AES está em vigor desde 2002 e estima-se que o seu tempo de vida seja de cerca de 30 anos. Quanto aos algoritmos de Cifra por Blocos Assimétricos mais usados na prática ou em normas, são as técnicas do RSA (Rivest, Shamir, Adleman) desenvolvida no ano 1977 e com as técnicas de Pohlig-Hellman e Merkle-Hellman desenvolvidas 1978.

[211] Os algoritmos de Cifra Contínua (simétrica) mais usados na prática ou em normas, são o A5 que usa uma chave de 64-bit; O RC4 (algoritmo não público) que usa uma chave de 40-2048 bit; O SEAL que usa uma chave de 160-bit; A Cifra por blocos em modo OFB ou CFB onde a chave depende da cifra por blocos.

[212] O primeiro algoritmo de Cifra por Chave Assimetrico, é a técnica de Diffie-Hellman publicado em 1976.

que conhece a sua chave privada com a qual tem criptografado a sua mensagem. Uma característica peculiar deste sistema de criptografia é que, cada assinatura digital feita pelo emissor em um documento será diferente, porque para a sua formação, ainda de intervir a chave privada, também envolveu o conteúdo do documento através do algoritmo usado.[213]

Um problema com a criptografia assimétrica, no entanto, é que é mais lenta do que a criptografia simétrica. Ela requer muito mais capacidade de processamento para cifrar e decifrar o conteúdo da mensagem.

Há ainda uma combinação dos dois criptositemas, conhecidos por cifra mista ou híbrida, onde utiliza-se o sistema assimétrico para mandar a informação para o outro sujeito com uma chave aleatória gerada que o sujeito recetor vai conseguir decifrar com a chave privada. E depois, a partir daí usa-se o sistema simétrico para o resto da comunicação.

h) Protocolos Criptograficos: Descrevem a maneira como um algoritmo deve ser usado para a troca ordenada de dados cifrados entre entidades. Pelo geral são usados para o transporte seguro de dados no nível do aplicativo. Exemplo são os mecanismos de segurança para Sistemas

[213] Nos processos de troca segura de mensagens de dados, a assinatura digital garante a validade das chaves públicas utilizadas, oferecendo serviços de autenticidade que protegem ao destinatário da mensagem, garantindo que a mensagem foi gerada pelo sujeito identificado no documento como emissor do mesmo; Eles também oferecem serviços de confidencialidade, ao permitir que quem conheça a chave pública do emissor decifre a mensagem; Oferece serviços de integridade porque a informação é protegida contra modificações de dados intencionais ou acidentais, isto é, se houve modificação de informação durante a transferência, o destinatário pode notar que o documento tenha sido alterado através valores de verificação ou referências de integridade e pode rejeitar o mesmo, por exemplo, para enviar uma mensagem assinada digitalmente, esta mensagem é resumido (ou hash em Inglês) com algoritmos de resumem ou autenticação, gerando um número ou código, de modo que é quase impossível que outro documento seja criado com o mesmo número. Esse número é cifrado ou criptografado usando a chave privada, sendo esta a assinatura digital enviada com a mensagem original. O destinatário recebe a mensagem, faz o seu próprio resumo para obter o número ou código e com a chave pública do remetente decifra a assinatura e compara as mensagens, se ambos são iguais significa que o remetente é válido e que a mensagem não foi alterada. Todo esse processo é invisível para o usuário, o sistema é responsável por realizar os algoritmos, sumários e verificações. Entre os algoritmos mais usados para autenticar um documento estão os conhecidos pelas siglas **MD-2, MD-4 y MD5** (de Messages Digest) y **SHA** (Standar Hash Algorithm); E, finalmente, oferece o serviço de não repúdio que também protege o recetor da negação do emissor de ter enviado o documento. Atualmente, existem vários métodos de autenticação, como a celebração de uma mensagem com um fac-símile eletrónico de sua assinatura como sinal distintivo pessoal para informá-los sobre a identidade do autor de um documento e expressar o seu acordo sobre o conteúdo do ato, gerado através de uma caneta eletrónica, ou assinar a mensagem com uma assinatura digital que obedeça a mesma intenção e expressão da vontade de uma assinatura manuscrita, como é um método de autenticação da pessoa e não-repúdio que dão origem a direitos e obrigações e valor probatório e confidencialidade das mensagens de dados. Também existem assinaturas biométricas baseados na tecnologia do scanner para medir e analisar as características físicas, tais como retinas, íris, padrões faciais, veias da mão, a geometria da palma da mão ou voz para fins de autenticação. Estes métodos estão evoluindo rapidamente, e permitem que as pessoas que fazem transações na rede podam identificar os seus homólogos com um identificador digital.

Distribuidos,[214] o *TransportLayer Security* (TLS)[215], o Rede Rrivada Virtual – (VPN *Virtual Private Network*)[216]

Ao mesmo tempo, os autocuidados que podem ter os usuários, sempre ajudaram a garantir a privacidade dos dados. Neste ponto "Edward Snowden (Ex analista de sistema do Sistema de Segurança Nacional dos Estados Unidos – NSA, que divulgou para o mundo como todos são monitorados virtualmente) fiz as seguintes recomendações para proteger a privacidade e a intimidade na internet:

a) Usar a rede Tor durante a navegação. (...)
b) Usar um *adblocker* (bloqueador de anúncios).
c) Usar um gerenciador de senhas.
d) Usar a autenticação de dois fatores. Muitos serviços, como o Gmail, Twit- ter, Dropbox, Hotmail e Facebook oferecem isso sem nenhum custo. Assim, mesmo que a senha seja exposta, ainda há uma cópia de segurança, como uma mensagem de texto para o celular para proteger as informações.
e) Usar o *plugin* HTTPS Everywhere, feito pela *Electronic Frontier Foun - dation* (EFF), ele tentará encriptar toda a comunicação do navegador com a internet.
f) Criptografar o disco duro.

---

[214] A segurança num sistema distribuído deve ser vista como algo abrangente de todos seus componentes, ou seja, deverão existir politicas e mecanismos globais como a defensa em perímetro, e ainda, políticas e mecanismos locais em cada computador, rede e equipamento de rede do sistema. ZÚQUETE, André - Segurança em redes informáticas. p. 17

[215] O Transport Layer Security (**TLS**) é um protocolo criptográfico usado em conexões seguras da Web (HTTP). Ele possui um mecanismo de autenticação de entidade baseado no sistema X.509, uma fase de configuração de chave, na qual uma chave de criptografia simétrica é decidida através do uso de criptografia de chave pública e uma função de transporte de dados de nível de aplicação.

[216] **VPN** é uma extensão segura de uma rede privada sobre uma rede insegura normalmente pública. Quando o nosso dispositivo ou computador se conecta à internet através da rede VPN, esta última funciona como um filtro para a Internet usando geralmente a criptografia para ocultar informação ao provedor da Internet, portanto, todo o tráfego que passa por essa rede é assegurado e protegido de olhos indesejados. As VPN conhecidas como "confiáveis" garantem que o encaminhamento dos dados numa rede pública passem por fornecedores de acesso e encaminhamento de confiança. No entanto, As VPN conhecidas como "seguras" tem evoluído em larga escala, pela flexibilidade, e garantem que a segurança dos dados entre o emissor e o recetor é independente da honestidade dos fornecedores de acesso e encaminhamento. Dentro destas soluções temos: **IPSec (**IP Segurity Protocol) para explorar associações seguras ao nível de IP nas comunicações na Internet, **SSL** (Secure Socket Layer) O padrão desenvolvido pela Netscape que usa tecnologia de criptografia para comunicações HTTP entre navegadores e servidores para proporciona segurança razoável al oferecer integridade e confidencialidade, mas não realiza nenhum processo de autenticação; **SSH** (Secure SHell) para permitir o estabelecimento de sessões seguras; O **SET** (Secure Electronic Transaction) é um protocolo desenvolvido por iniciativa da VISA e MasterCard em 1995, e baseia-se na utilização de uma assinatura eletrónica a nível do comprador e uma transação. Com efeito, o número do cartão de crédito é enviado diretamente ao banco do comerciante, o comerciante não fica com os dados do titular do cartão de pagamento porque a transferências de dados de pagamento é diretamente entro o comprador e o banco, oferecendo assim uma série de serviços que convertem transações comerciais através da Internet em um processo seguro e confiável para todas as partes envolvidas (comprador, comerciante e banco), esses serviços são: Autenticação, Confidencialidade, Integridade, Intimidade, Verificação imediata, e Não repúdio. E **PPTP** (Point-to-Point Tunneling) que permite troca segura de dados em uma rede de trabalho via TCP / IP.

g) Ser inteligente com as perguntas de segurança. Parar de usar o nome de solteira da mãe para tudo. Da mesma forma o nome da primeira escola. A chave é misturar as coisas, tanto quanto possível, de modo que se alguém entrar em uma das contas pessoais, eles não poderão usar as mesmas informações para entrar em qualquer outro lugar.[217]

Com as politicas e mecanismos de segurança nos sistemas de e-commerce busca-se cumprir com:

i. Aumentar a conscientização das pessoas. O envolvimento e participação de todos os funcionários, incluindo aqueles no mais alto nível na hierarquia da empresa, é essencial para garantir o gerenciamento adequado da segurança cibernética na empresa. Por essa razão, aumentar a conscientização e treinar os membros da organização torna-se uma peça-chave do quebra-cabeça da segurança cibernética na empresa.
ii. Evitar o fraude. Por exemplo, o sistema eletrónico de pagamento implementado na loja virtual deve ter um certificado SSL de validação estendida, dessa forma o cliente identificará o banco ao qual ele pertence inequivocamente e os dados do banco dele serão criptografados. O sistema eletrónico de pagamento escolhido deve ter medidas de segurança antifraude, desta forma, as possíveis perdas econômicas da loja virtual são reduzidas.
iii. Confidencialidade ou privacidade. Garantir que as informações transmitidas pela Internet sejam ilegíveis para pessoas e entidades não autorizadas, de tal forma, que nenhuma outra pessoa possa acessar às informações pessoais ou bancárias do usuário.
iv. Autenticação. Os sistemas de e-commerce devem ser capazes de identificar todos os participantes na troca, bem como seus elementos. Eles devem garantir que a identidade do estabelecimento ou do comércio virtual não possa ser suplantada, de modo que nenhuma outra pessoa, física ou jurídica, possa realizar ataques de *phishing*.
v. Integridade. Detectar alterações introduzidas no conteúdo original das mensagens e certificar de que as mensagens recebidas correspondam às enviadas. O sistema estará completo se garantir a detecção de qualquer alteração nas informações da troca comercial.
vi. Não repúdio. Os sistemas de segurança da Internet devem ter a capacidade de garantir que as informações enviadas sejam recebidas e lidas pelo destinatário, de modo que não possam

[217] Cit. Por ESTRADA, Manuel. O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade. P. 51,52.

recusar recebê-las; O serviço de não repúdio também protege ao destinatário da negação do remetente de ter enviado o documento. Assim, o não repúdio de uma informação ou pagamento eletrónico refere-se à impossibilidade do comprador negar ter adquirido certos compromissos quando, de fato, ele tivesse adquirido.

Dessa forma, as técnicas de segurança no comercio eletrónico devem ser cumpridas em todas as operações que envolvam uma troca comercial e, especialmente, na comunicação de dados pessoais, em pedidos de compras, na autorização de pagamentos e na efetiva realização dos mesmos.

Como pode ser visto, existem diferentes politicas e mecanismos de segurança que podem ser usados para criar ambientes seguros no comercio eletrónico. A implementação de um ou de outro depende das necessidades de segurança e do potencial risco segurável.

CAPITULO III

OS DADOS PESSOAIS DE PAGAMENTO UTILIZADOS NO COMÉRCIO ELETRÓNICO (B2C)

3.1. IMPORTÂNCIA DO COMÉRCIO ELETRÓNICO E OS MEOIS DE PAGAMENTO.

Os últimos anos do século XX, se tornaram os anos da bolha da internet com a difusão do serviço *on-line,* gerando perspetivas de crescimento da economia baseada na rede, e criando as condições para uma maior atenção por parte da comunidade financeira, a qual colocou muito capital à disposição de qualquer um que tivesse projetos para o desenvolvimento e para a utilização dessas novas tecnologias, dando origem, à chamada *new economy,* cujo nascimento provocou um aumento no mercado de Bolsas da NASDAQ de Nova Iorque e de empresas como Yahoo e Nestcape, que atingiram cotações muito elevadas nos primeiros dias de contrato.[218]

Um dos tempos mais eufóricos da história do comércio mundial foi, no período de 1995-2000, onde se formaram milhares de empresas *dot com*[219], apoiadas por mais de 125 biliões de USD em capital financeiro, sendo uma das maiores expansões de capital de risco na história mundial. Foi também um tempo em que conceitos fundamentais do comércio eletrónico foram desenvolvidos e explorados.[220]

De tal modo, que as iniciativas de comércio eletrónico por pessoas e organizações têm permitido transformar a condução dos negócios aos mas diversos níveis e abrangências em todo o mundo, desde as multinacionais até às microempresas, facilitando a entrada a novos mercados, clientes, fornecedores, alianças, parcerias, produtos e serviços, tudo isto sem os limites geográficos, materiais e temporais que a forma convencional de conduzir os negócios impõe.[221]

Incluso, as redes sociais, que num início se apresentavam como meios ou *sites* de relacionamento, se tornaram verdadeiros facilitadores das atividades comerciais, ou seja, dos *mercados virtuais* onde se

---

[218] BERNABÉ, Franco. – op. cit., p. 34

[219] Término inglés utilizado para descrever os sites da Internet de domínio ".com".

[220] GONÇALVES, Ramiro Manuel [et al.]. - Modelo das iniciativas de comércio electrónico em organizações portuguesas.

[221] GONÇALVES, Ramiro Manuel [et al.]. - op. cit.

transacionam bens e serviços. De facto, para as empresas, essas redes funcionam como agregadores de indivíduos e de interesses aos quais se torna fácil oferecer produtos e serviços conforme os seus hábitos e preferências de consumo.[222]

José Eduardo Faria[223], do mesmo modo, reconhece a importância das TIC's num cenário de globalização económica, quando produto dos avanços tecnológicos surgem modos inéditos de comunicações e de transmissões culturais instantâneas entre polos distantes, que ampliam as possibilidades de encontros sociais entre as pessoas. De esses encontros emergem importantes consequências, tais como a mundialização da económia, a desterritorialização e reorganização do espaço de produção.

Nessa situação, Pierre Lêvy[224] entende, que os processos de conceção, de comercialização e de produção serão condicionados pela sua imersão no espaço virtual, de tal modo que, no comércio eletrónico, a maior parte dos produtos será concebida e comprada pelos consumidores na rede antes de serem fabricados.

Ao respeito, Alian Rallet[225] considera que este comércio eletrónico é formado por quatro camadas. A primeira compreende as atividades relacionadas à infraestrutura da internet, contemplando os fornecedores de *backbone*[226], rede, *software* e *hardware*, servidores e soluções de segurança. A segunda contém as aplicações de internet que permitem o comércio *on-line,* tais como consultores, aplicações multimédia, motores de busca e bancos de dados. A terceira camada é dos intermediários, como: organizadores de mercado em plataformas de comércio eletrónico, agências de viagens *on-line*, portais, corretores *on-line*, agentes inteligentes[227] como os *bots shopping* para a comparação automática de

---

[222] BERNABÉ, Franco. – op. cit., p. 50

[223] Cit. por BARRETO, Ricardo – op. cit.,. p.80

[224] Cit. por BARRETO, Ricardo – op. cit.,. p.80

[225] Cit. por BARRETO, Ricardo – op. cit.,. p.87

[226] refere-se às principais sociedades troncais da Internet. É composto de um grande número de roteadores comerciais, administrativos, universitários e outros roteadores interconectados de alta capacidade que transmitem dados por países, continentes e oceanos do mundo usando cabos de fibra ótica. O termo backbone também se refere ao cabeamento de tronco do subsistema vertical em uma instalação de rede local que segue os regulamentos de cabeamento estruturado. (F. AUGUST - CABLEADO VETICAL O BACKBONE.)

[227] Refere-se a um programa que navega ao invés do usuário, incorporando tecnologias de sistemas especialistas e técnicas de Inteligência Artificial de aprendizado e planejamento. Da mesma forma, eles atuam como assistentes eletrónicos que executam tarefas que, de outra forma, seriam executadas manualmente. Os Agentes Inteligentes podem automatizar muitas tarefas rotineiras ou tarefas que não envolvem pesquisa, típicas de usuários da WWW, fornecendo também um método eficiente de busca, coleta e filtragem de informações em pesquisas entre redes. Entre as principais aplicações em uma empresa está seu uso para melhorar a produtividade dos usuários da rede, fluxo de trabalho e administração, no comércio eletrónico e em agendas compartilhadas. Eles têm a capacidade de perceber e observar, o que lhes permite aprender e tomar decisões mais precisas, gerando conhecimento, para deduzir e diagnosticar decisões, pensando como seres humanos.

preços, publicidade virtual, sites web, etc. A quarta camada, trata do comércio real, por exemplo: comerciantes, fabricantes de vendas *on-line*, companhias aéreas que vendem bilhetes *on-line*, serviços de entretenimento, etc.

Desta forma, vemos como a expansão do comércio eletrónico, apresenta-se com efeito, como um elemento decorrente do processo de globalização. Todavia, Denise Tellini[228] vai além, afirmando que o comércio eletrónico é "umas das causas (e das consequencias) do avanço do fenomeno da globalização, pela simplificação de barreiras como espaço e tempo entre as partes envolvidas," no entanto, para que o comércio eletrónico tenha um desenvolvimento sustentável, deve haver meios de pagamentos eletrónicos que permitam a transferência de recursos de forma segura, garantindo a autenticação, autorização, não repúdio, integridade das informações e confidencialidade dos mesmos.

A partir daí, os meios de pagamento gozam de uma relevância essencial no comércio eletrónico, em virtude que os problemas que surgiram nessa forma de comércio tem sido, encontrar um meio de pagamento útil e seguro para os estabelecimentos e os clientes (consumidores e não consumidores). Para tal fim, nós compartilhamos a sugestão de Gerna Garcia, quem para esses casos propõe, o uso de uma assinatura digital com criptografia assimétrica, ou seja, com uma senha dupla, uma privada e uma pública, como foi exposto no Capítulo II sobre *as TÉCNICAS INFORMÁTICAS QUE VISAM PROTEGER OS DADOS PESSOAIS* no presente trabalho, acompanhada dum certificado digital,[229] tentando para tal efeito adotar um critério de neutralidade tecnológica que não crie um obstáculo ao desenvolvimento do comércio eletrónico.

3.2 OS DADOS DE PAGAMENTO E A SUA RELAÇÃO COM O COMÉRCIO ELETRÓNICO (B2C).

Em sentido amplo, o comércio eletrónico se descreve como toda transação comercial feita em parte ou na sua totalidade, através de redes ou meios eletrónicos de informação em base a um contrato

---

Pelo modus operandi os agentis inteligentes se podem classificar em: Agentes inteligentes de busca, os quais visam a obtenção de determinado tipo de informação (o conhecido "Google", mas também agentes que operam a nível comercial na Web procurando informação comercial concreta, por exº quem vende o quê e a que preços) e os agentes inteligentes decisórios que são agentes interventivos que demonstram capacidade para aceitar ou cancelar uma encomenda, prestar "consentimento" ou aceitar uma proposta, acusar recepção (ANDRADE, Francisco António Carneiro Pacheco de – DA CONTRATAÇÃO ELECTRÓNICA – EM PARTICULAR DA CONTRATAÇÃO ELECTRÓNICA INTER-SISTÉMICA INTELIGENTE)

[228] Cit. por BARRETO, Ricardo – op. cit.,. p.89

[229] BOTANA GARCIA, Gerna Alejandra. Coord. – COMERCIO ELECTRONICO Y PROTECCION DE LOS CONSUMIDORES. p. 558

"Eletrónico", o qual surge do conceito tradicional de contrato, ou seja, como um ato em que duas ou mais pessoas expressam a sua vontade com a intenção de criar, transmitir, modificar ou extinguir obrigações, com a particularidade de que para a sua formação intervêm uma rede telemática[230] usada como meio de transmissão dos mensagens de dados eletrónicos à distância. Como identifica Cláudia Lima Marques, "O contrato é velho, o método da contratação é atual, e o meio da contratação é novo"[231]

Portanto, o comércio eletrónico nasce dum contrato *Eletrónico*, mesmo que resulta da utilização do instrumento ou meio eletrónico através do qual o contrato é celebrado. A declaração de vontade será através de um contrato escrito em suporte de papel ou eletrónico antes antes de usar o sistema eletrónico com o qual será feita a transmissão de dados informáticos.

Entre estes dados, estarão os dados de identificação pessoal, a informação sobre contas e o número da conta, as senhas ou *identificador único*[232], e os *Dados de Pagamento Sensíveis,* todos relativos à forma ou instrumentos de pagamento eletrónico[233], que pelo geral, poderão ser com um cartão de débito, cartão de crédito[234], cartão inteligentes, transferência eletrónica, cheque eletrónico[235], contas bancarias, moeda eletrónica (E-Money)[236], etc..., cujos dados fazem referencia aos dados pessoais de pagamento em que se baseia o presente trabalho.

---

[230] "Telemática" do inglês *telematic*, palavra formada por duas vozes, *tele* do grego que significa "à distância" " e *informatics* de informática, e é definida como o conjunto de serviços informáticos fornecidos através de uma rede de telecomunicação. Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, [consultado em 30-03-2018]. https://priberam.pt/dlpo/telematica

[231] Cit. por BARBIERI, Diovanna – A PROTEÇÃO DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO. p. 85

[232] Diretiva (UE) 2015/2366) relativa aos serviços de pagamento no mercado interno, Art.º 4. Definições: 33) «Identificador único», uma combinação de letras, números ou símbolos, especificada ao utilizador de serviços de pagamento pelo prestador de serviços de pagamento, fornecida pelo utilizador de serviços de pagamento para identificar inequivocamente outro utilizador de serviços de pagamento e/ou a respetiva conta de pagamento tendo em vista uma operação de pagamento;

[233] O pagamento eletrónico não deve confundir-se com a transferência eletrónica de fundo, pois, este último não sempre será uma operação de compra venta, pelo contrário, ser uma simples transação sim objeto de pago.

[234] Embora o cartão de crédito seja um dos meios de pagamento mais utilizados, quer pela rapidez quer pela facilidade para adquirir bens ou serviços no comércio eletrónico, este instrumento de pagamento não foi criado para ser utilizado remotamente, a partir daí, o uso que foi fornecido com pagamentos remotos, teve impacto na perda de confidencialidade dos dados pessoais nele contidos e das operações realizadas, e outros elementos associados a ele, como os dados pessoais do titular, incluindo o numero de cartão de credito, a data de expiração e o chamado número segredo que cada detentor pode ter, afetando assim a vida privada do titular do cartão e colocando até mesmo seus ativos em risco, quando estes dados são utilizados indevidamente por pessoas não autorizadas, embora, o direito do titular do cartão de crédito de pedir a anulação da cobrança feita persistirá quando nenhuma operação for autorizada por ele. Nas palavras de MARIA RAQUEL GUIMARÃES "Não se pode, porém, mitificar um risco que é afinal comum a toda a desmaterialização dos meios de pagamento" (RUIZ Miguel, C., [et al.];- op. cit., p.165). O cartão de crédito, se diferencia do cartão de débito, principalmente pela alínea de crédito concedido no contrato associado ao cartão de crédito, portanto, será um empréstimo numerário, com a particularidade de que o montante emprestado não é definido exatamente, mais o importante é que não exceda do limite máximo estabelecido no contrato. Para INFANTE PERZ, o cartão de crédito é um Documento privado de caráter mercantil, cujo conteúdo essencial são os dados identificadores do documento, da entidade emissora e de seu proprietário, distribuídos sobre um suporte rígido de material plástico, ao qual, em alguns casos, é incorporada uma fita magnética para leitura por meio de eletrónico, cujo objetivo é permitir ao seu proprietário realizar diversas transações comerciais, utilizando-o como meio ou ordem de pagamento. (DAVARA RODRÍGUEZ., Miguel Á. Op. Cit., p. 343)

[235] Usado principalmente na França e nos Estados Unidos da América.

[236] Para GERNA GARCIA, os cartões eletrónicos são cartões de crédito, débito e por moeda eletrónica, enquanto o dinheiro eletrónico e os títulos eletrónicos são formados por cheques eletrónicos, letras de câmbio eletrónicas e cartões de embarque eletrónicos. (BOTANA GARCIA, Gerna Alejandra. Coord. – COMERCIO ELECTRONICO Y PROTECCION DE LOS CONSUMIDORES.p542)

Voltando ao contrato eletrónico, de acordo com o modo de uso, este pode ser classificados como: *CONTRATAÇÃO ELETRONICA INTER-PESSOAL*, *CONTRATAÇÃO ELETRÓNICA INTER-ACTIVA (SEMI-AUTOMATIZADO)*[237], ou *CONTRATAÇÃO ELETRÓNICA INTER-SISTEMATICA*[238].

Para o presente capitulo, onde se deseja conhecer sobre *"OS DADOS PESSOAIS DE PAGAMENTO UTILIZADOS NO COMÉRCIO ELETRÓNICO (B2C)",* necessariamente intervém o consumidor como uma pessoa singular, portanto, o contrato eletrónico de acordo com o seu uso estaria baseado numa: Contratação Eletrónica Inter-pessoal ou uma Contratação Eletrónica Inter-ativa.

Na Contratação Eletrónica Inter-pessoal, o computador é utilizado como mero instrumento ou meio de comunicação entre as partes, limitando-se a transmitir / receber mensagens elaboradas pelas pessoas, portanto e um contrato celebrado através das redes telemáticas, que utiliza a tecnologia com a interação humana.[239]

Em relação à Contratação Eletrónica Inter-ativa, uma das partes é uma pessoa e a outra é um sistema computacional de processamento de dados, que interagem entre si por meio de uma rede de dados eletrónicas[240]. Parte de uma proposta de oferta de produto ou serviço ao público com cláusulas de

---

[237] DL 7/2004 Comércio Eletrónico. Artigo 29° Trata apenas da contratação interativa: "Ordem de encomenda e aviso de recepção:
1 — Logo que receba uma ordem de encomenda por via exclusivamente electrónica, o prestador de serviços deve acusar a recepção igualmente por meios electrónicos, salvo acordo em contrário com a parte que não seja consumidora.
2 — É dispensado o aviso de recepção da encomenda nos casos em que há a imediata prestação em linha do produto ou serviço. (se refiere al CE directo)
3 — O aviso de recepção deve conter a identificação fundamental do contrato a que se refere.
4 — O prestador satisfaz o dever de acusar a recepção se enviar a comunicação para o endereço electrónico que foi indicado ou utilizado pelo destinatário do serviço.
5 — A encomenda torna-se definitiva com a confirmação do destinatário, dada na sequência do aviso de recepção, reiterando a ordem emitida."

[238] CONTRATAÇÃO ELETRÓNICA INTER-SISTEMATICA: Os próprios sistemas informáticos "aplicações" das partes se encontram interligados e interagem entre si de modo automatizado sem a atuação humana, em cada negócio jurídico efetuado, existindo tal intervenção somente no momento da programação para a comunicação, e são derivados de contratos preexistentes, firmados entre os titulares dos referidos sistemas computacionais. No entanto, o computador, por si só, não é fonte de obrigações contratuais, não tem personalidade nem capacidade jurídicas, e portanto não pode vincular-se, por si sós, juridicamente. (ANDRADE, Francisco António Carneiro Pacheco de – DA CONTRATAÇÃO ELECTRÓNICA – EM PARTICULAR DA CONTRATAÇÃO ELECTRÓNICA INTER-SISTÉMICA INTELIGENTE). Ao respeito, o DL 7/2004 Comércio Eletrónico no Artigo 33. Considera: " o Contratação sem intervenção humana:
1 Ð À contratação celebrada exclusivamente por meio de computadores, sem intervenção humana, é aplicável o regime comum, salvo quando este pressupuser uma actuação.
2 Ð São aplicáveis as disposições sobre erro: a) Na formação da vontade, se houver erro de programação; b) Na declaração, se houver defeito de funcionamento da máquina; c) Na transmissão, se a mensagem chegar defor- mada ao seu destino.
3 Ð A outra parte não pode opor-se à impugnação por erro sempre que lhe fosse exigível que dele se apercebesse, nomeadamente pelo uso de dispositivos de detecção de erros de introdução."

[239] ANDRADE, Francisco António Carneiro Pacheco de – DA CONTRATAÇÃO ELECTRÓNICA – EM PARTICULAR DA CONTRATAÇÃO ELECTRÓNICA INTER-SISTÉMICA INTELIGENTE. P. 26

[240] Como sítios web na Internet, a "Amazon"

utilização estabelecidas unilateralmente pelo fornecedor do sítio web, e o utilizador deve aceitar ou rejeitar o serviço web. Nesta modalidade, há liberdade contratual porque o utilizador não está obrigado a comprar os bens ou serviços. No momento da aceitação, o utilizador deve fornecer dados pessoais pela contratação, tais como: identificação, endereço e os dados de pagamento.[241]

O Diploma DL 24/2014[242], relativa aos direitos dos consumidores e que Transpõe a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho de 25 de outubro de 2011, para além de ser uma diretiva de harmonização máxima, também junta vários matérias tales como, proteção do consumidor, contratação à distância, contratos a domicílios, aspetos relativos aos de bienes de consumos, e segundo o art.º 2 núm. 1, é aplicável aos contratos celebrados à distância e aos contratos celebrados fora do estabelecimento comercial, tendo em vista promover a transparência das práticas comerciais e salvaguardar os interesses legítimos dos consumidores.

A contratação à distância antes mencionada é entre ausentes como o assinala o art.º 3 letra f) do DL 24/2014[243], toda vez, que não há a presencia física do consumidor nem do fornecedor num contrato organizado para o comércio à distância mediante a utilização técnicas de comunicação à distância.

Deve-se notar que, o princípio de liberdade de celebração do contrato por via eletrónica ou informática é consagrado em Portugal com o Decreto-lei 7/2004[244] sobre o Comércio Eletrónico nos artículos 24º[245] e 25º[246], indicando que é livre, e a validez do contrato não pode ser afetada pelo medio

---

[241] ANDRADE, Francisco António Carneiro Pacheco de – DA CONTRATAÇÃO ELECTRÓNICA – EM PARTICULAR DA CONTRATAÇÃO ELECTRÓNICA INTER-SISTÉMICA INTELIGENTE. P. 29

[242] Alterado pela Lei n.º 47/2014, de 28 de julho (artigos 3.º, 4.º, 5.º, 15.º, 16.º e 17.º; aditamento da alínea n) ao n.º 2 do artigo 2.º e revogação do artigo 18.º).

[243] DECRETO-LEI nº 24/2014 Regime aplicável aos contratos celebrados à distância e aos contratos celebrados fora do estabelecimento comercial, bem como a outras modalidades contratuais de fornecimento de bens ou serviços, incorporando a Diretiva n.º 2011/83/UE, do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores, "Art. 3 letra f) «Contrato celebrado à distância», um contrato celebrado entre o consumidor e o fornecedor de bens ou o prestador de serviços sem presença física simultânea de ambos, e integrado num sistema de venda ou prestação de serviços organizado para o comércio à distância mediante a utilização exclusiva de uma ou mais técnicas de comunicação à distância até à celebração do contrato, incluindo a própria celebração."

[244] O DL 7/2004 transpõe para a ordem jurídica interna a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Directiva sobre Comércio Eletrónico) bem como o artigo 13.º da Diretiva o 2002/58/CE, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e a proteção da privacidade no sector das comunicações electrónicas (Diretiva relativa à Privacidade e às Comunicações Eletrónicas). Artigo 2.º

[245] DECRETO-LEI nº 7/2004 Comércio Eletrónico. "Art.º 24.- Âmbito. As disposições deste capítulo são aplicáveis a todo o tipo de contratos celebrados por via electrónica ou informática, sejam ou não qualificáveis como comerciais."

[246] DECRETO-LEI nº 7/2004 Comércio Eletrónico. Art.º 25.- "Liberdade de celebração:
1 — É livre a celebração de contratos por via electrónica, sem que a validade ou eficácia destes seja prejudicada pela utilização deste meio.
2 — São excluídos do princípio da admissibilidade os negócios jurídicos:
a) Familiares e sucessórios;
b) Que exijam a intervenção de tribunais, entes públicos ou outros entes que exerçam poderes públicos, nomeadamente quando aquela intervenção condicione a produção de efeitos em relação a terceiros e ainda os negócios legalmente sujeitos a reconhecimento ou autenticação notariais;

no qual se celebro o contrato. No entanto, são excluídos os negócios jurídicos familiares ou sucessórios; Os que exijam a intervenção de tribunais, entes públicos ou autenticação notariais; Os Reais imobiliário; e os de caução e de garantia.

O exposto vai em concordância com o art.º 219[247] (liberdade da forma) do Código Civil ao indicar que a declaração negocial depende de forma especial só quando a lei a exigir, e o art.º 405[248] (liberdade contratual) ao afirmar que as partes podem fixar livremente o conteúdo dos contratos dentro dos limites da lei.

A da **Diretiva (UE) 2015/2366[249] do Parlamento Europeu e do Conselho de 25 de novembro de 2015,** relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE, e regula "o acesso à atividade das instituições de pagamento e a prestação de serviços de pagamento, bem como o acesso à atividade das instituições de moeda eletrónica e a prestação de serviços de emissão de moeda eletrónica."[250] também conhecida como **DSPII**, regula o regímen jurídico de pagamentos da moeda eletrónica, para o desenvolvimento de uma maior integração do mercado interno de pagamentos eletrónicos, procurando promover o alcance do *eCommerce,* aumentar a concorrência e garantir a segurança dos pagamentos na Internet.

A norma considera na sua sistematização os diferentes tipos de *instrumentos de pagamento*[251] que tínhamos mencionados, incluindo os serviços de banca eletrónica, tanto nas operações presenciais, como à distância, efetuadas por utilizadores, consumidores ou utilizadores profissionais, pelo que visa

---

c) Reais imobiliários, com excepção do arrendamento;
d) De caução e de garantia, quando não se integrarem na actividade profissional de quem as presta.
3 — Só tem de aceitar a via electrónica para a celebração de um contrato quem se tiver vinculado a proceder dessa forma.
4 — São proibidas cláusulas contratuais gerais que imponham a celebração por via electrónica dos contratos com consumidores."

[247] DECRETO-LEI nº 47/344, Código Civil Português. Art.º 219 (Liberdade de forma) A validade da declaração negocial não depende da observância de forma especial, salvo quando a lei a exigir.

[248] DECRETO-LEI nº 47/344, Código Civil Português. Art.º 405 (Liberdade contratual):
1. Dentro dos limites da lei, as partes têm a faculdade de fixar livremente o conteúdo dos contratos, celebrar contratos diferentes dos previstos neste código ou incluir nestes as cláusulas que lhes aprouver.
2. As partes podem ainda reunir no mesmo contrato regras de dois ou mais negócios, total ou parcialmente regulados na lei

[249] A Lei 57/2018 Autoriza o Governo de Portugal a regular o acesso à atividade das instituições de pagamento e instituições de moeda eletrónica, bem como a prestação de serviços de pagamento e emissão de moeda eletrónica, no âmbito da transposição da Diretiva (UE) 2015/2366, do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE [DR I série N.º160/XIII/3 2018.08.21]

[250] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno (DSPII), art. 1.º

[251] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno (DSPII), art. 4.º núm. 14) «Instrumento de pagamento», um dispositivo personalizado e/ou um conjunto de procedimentos, acordados entre o utilizador do serviço de pagamento e o prestador do serviço de pagamento, utilizados para iniciar uma ordem de pagamento;

melhorar as regras da UE existentes no que diz respeito aos pagamentos eletrónicos, além, tem em consideração serviços de pagamentos emergentes e inovadores como os pagamentos através de dispositivos móveis[252] nas redes eletrónicas de transferências de dados, estabelecendo requisitos de segurança rigorosos aplicáveis aos pagamentos eletrónicos e à proteção dos dados financeiros dos consumidores, garantindo a autenticação segura e reduzindo o risco de fraude.[253]

Conforme á definição de Dados de Pagamento Sensíveis dada na Diretiva (UE) 2015/2366 (DSPII), estes incluem as *credenciais de segurança personalizadas,*[254] uma vez que eles podem ser usados para cometer fraudes, igualmente considera que a informação sobre contas, o nome do titular da conta e o número da conta não constituem dados de pagamento "sensíveis".

Esta diferenciação é importante, porque a Diretiva (UE) 2015/2366, estabelece obrigações específicas para o tratamento dos *Dados de Pagamento Sensíveis*, como por exemplo as instituições de pagamentos, devem ter um procedimento para classificar, verificar, rastrear e restringir o acesso a dados de pagamento sensíveis; mais a política de segurança dessas instituições deve incluir as avaliações dos riscos dos serviços de pagamento com as medidas de controlo da segurança e de redução desses riscos, incluindo a fraude e a utilização ilícita de dados pessoais e sensíveis. Bem assim, estabelece regras de acesso à conta de pagamento em caso de *serviços de iniciação do pagamento*[255], quando proíbe ao *prestador do serviço de iniciação do pagamento*[256] armazenar dados de pagamento sensíveis, ou quando proíbe ao *prestador de serviços de informação sobre contas*[257], exigir dados de pagamento sensíveis associados às contas de pagamento.

A referida Diretiva enfatiza que a operação de pagamento, por exemplo no comércio eletrónico, é autorizada desde que o pagador tenha dado o seu consentimento ao beneficiário do pagamento ou ao

---

[252] «Instrumento de pagamento baseado em cartões», um instrumento de pagamento, incluindo cartões, telemóveis, computadores ou outros dispositivos tecnológicos que contenham a aplicação de pagamento adequada, que permite ao ordenante iniciar uma operação de pagamento baseada num cartão. (Definições)

[253] EUR-LEX - Regras revistas relativas aos serviços de pagamento na União Europeia.

[254] Diretiva (UE) 2015/2366) relativa aos serviços de pagamento no mercado interno, Art.º 4. Definições: 31) «Credenciais de segurança personalizadas», elementos personalizados fornecidos pelo prestador de serviços de pagamento a um utilizador de serviços de pagamento para efeitos de autenticação;

[255] "Os serviços de iniciação de pagamentos permitem que o prestador do serviço de iniciação do pagamento assegure ao beneficiário que o pagamento foi iniciado, a fim de incentivar o beneficiário a disponibilizar o bem ou a prestar o serviço sem demora indevida. Esses serviços oferecem uma solução pouco onerosa tanto aos comerciantes como aos consumidores e dão aos consumidores uma possibilidade de efetuarem compras em linha, mesmo que não disponham de cartoões de pagamento" (DSPII considerando 29).

[256] São intermediários que garantem o pagamento do consumidor diretamente ao comerciante.

[257] São entidades que consolidam todas as informações das diferentes contas que um usuário abriu em diferentes entidades e as classifica por categorias

provedor de serviços de iniciação de pagamento para executar a operação de pagamento; O pagador pode dar este consentimento antes ou depois da operação se for acordado pelas partes, e sempre terá a possibilidade de retirar o consentimento dado, mas nunca depois do momento de irrevogabilidade[258].

3.3. A PROTEÇÃO JURÍDICA EM PAGAMENTOS À DISTANCIA COM MOEDA ELETRÓNICA.

O risco de utilização fraudulenta das informações contidas nos instrumentos de pagamento à distância, no especial, no cartão de crédito ou débito, é potenciado pela velocidade e facilidade com que os pagamentos são feitos sem a necessidade de exibir o cartão nas operações de comércio eletrónico através de Internet, e na maioria dos casos, sem deixar qualquer rastos e sem que o titular dos dados de pagamento tenha a possibilidade de detetar de imediato as operações não autorizadas.

Nessa conjuntura, a obtenção de informação suscetível de desencadear um pagamento fraudulento no comércio eletrónico pode ocorrer:

i. Pela perda, ou o roubo do um cartão de crédito ou de débito;
ii. Nas operações presenciais no momento da transação quando se duplica ou contrafaz o cartão (*clonagem*[259]) com ajuda do aparelho que efetua a leitura da fita magnética do cartão, quer por o beneficiário do pagamento quer pela instalação desse aparelho numa caixa automática;

---

[258] Directiva (UE) 2015/2366) relativa aos serviços de pagamento no mercado interno, Art. 80.º Caráter irrevogável de uma ordem de pagamento:
1. Os Estados-Membros asseguram que uma ordem de pagamento não possa ser revogada pelo utilizador de serviços de pagamento após a receção da mesma pelo prestador de serviços de pagamento do ordenante, salvo disposição em contrário do presente artigo.
2. Caso uma operação de pagamento seja iniciada por um prestador do serviço de iniciação do pagamento ou pelo beneficiário ou através deste, o ordenante não pode revogar a ordem de pagamento depois de ter dado consentimento ao prestador do serviço de iniciação do pagamento para iniciar a operação de pagamento, ou de ter dado consentimento ao beneficiário para executar a operação de pagamento.
3. Todavia, em caso de débito direto e sem prejuízo dos direitos de reembolso, o ordenante pode revogar a ordem de pagamento até ao final do dia útil anterior ao dia acordado para o débito dos fundos.
4. No caso referido no artigo 78.º, n.º 2, o utilizador de serviços de pagamento pode revogar uma ordem de pagamento até ao final do dia útil anterior à data acordada.
5. Decorridos os prazos fixados nos n.os 1 a 4, a ordem de pagamento só pode ser revogada se tal tiver sido acordado entre o utilizador e os prestadores de serviços de pagamento em causa. No caso referido nos n.os 2 e 3, é também necessário o acordo do beneficiário. Se tal tiver sido acordado no contrato-quadro, o prestador de serviços de pagamento em causa pode cobrar encargos pela revogação." («Contrato-quadro», um contrato de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento; (Diretiva (UE) 2015/2366))

[259] Também conhecido como a técnica de *skimming*. (GUIMARÃES, Maria – Separata Infrações Económicas e Financeiras. Estudos de Criminologia e Direito. p.587)

iii. Pela intercetação dum cartão de crédito ou débito quando este é enviado para o seu titular pela entidade emissora;

iv. O uso de correio eletrónico é um novo canal através do qual são obtidas informações dos dados pessoais de pagamento[260] através da conhecida engenheira social.[261]

Decerto, para proteger a vida privada e a intimidade dos dados de pagamento pessoais dos usuários no comércio eletrónico, é preciso observar atentamente os instrumentos e mecanismos de pagamento dispostos na Internet. Nesse sentido, Rodrigo do Canto destacou que "diante os complexos avanços tecnológicos, os pleitos sociais de proteção da privacidade e segurança no comércio eletrónico reclamam um movimento decisivo dos aparatos legiferantes estatais, de maneira a fortalecer o princípio de vulnerabilidades, boa-fé objetiva e confiança, bem como os seus deveres derivados."[262]

Para tal efeito, uma vez identificado a origem das operações fraudulentas, a questão é saber sobre quem recai os prejuízos decorrentes destas operações. Isto é, quem devera suportar as perdidas correspondentes: Se o titular, o emissor da ordem de pagamento, ou seu beneficiário.

Nesse ambiente, para reduzir o risco de fraudes nas transações eletrónicas e melhorar a proteção dos dados do cliente na União Europeia, a DSPII prevê o estabelecimento de medidas de *autenticação forte de clientes*[263], baseadas em pelo menos dois dos três elementos: conhecimento, posse e inerência e a exigência de requisitos adicionais para transações de pagamento eletrónico à distância como o código de autenticação exclusivo com ligação dinâmica, gerado para cada transação de pagamento e específico para cada valor e beneficiário, de modo que o utilizador esteja sempre a par do montante e do beneficiário da operação.

---

[260] GUIMARÃES, Maria – Separata Infrações Económicas e Financeiras. Estudos de Criminologia e Direito. p.588

[261] A engenheira social, refere-se ao conjunto de atividades ou enganos que os atacantes usam para obter informações ou ativos das organizações através da manipulação de usuários legítimos, a fim de ter acesso a sistemas ou informações úteis e posteriormente para realizar fraudes ou instruções para uma rede de dados eletrónicos.

[262] Cit. por BARRETO, Ricardo – op. cit., p.167

[263] No art. 2.º núm. 30 da Diretiva (UE) 2015/2366 a «Autenticação forte do cliente», é "uma autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece, posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação."

No entanto, é obrigação do utilizador de serviços de pagamento fazer usos dos instrumentos de pagamentos de acordo com as condições que regem a sua emissão e utilização, à vez, de comunicar sem demora ao prestador de pagamento ou à entidade indicada por este último, o furto, a perda, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento. Por outro lado, a lei manda o utilizador preservar com o devido resguardo as *credenciais de segurança personalizadas*[264] fornecidas pelo prestador de serviços de pagamento para efeitos de autenticação do utilizador.

Tome-se em conta, que o prestador de serviços de pagamento vai suportar o risco do envio do instrumento de pagamento ou das respetivas credenciais de segurança personalizadas ao utilizador de serviços de pagamento[265]. O que significa que corre por conta do prestador de serviços de pagamento ou da instituição emissora do cartão de pagamento, as perdas resultantes da interceção ou extravio dum cartão enviado ao titular.

Na ocorrência de uma operação de pagamento não autorizada ou incorretamente executada, que não seja produto do furto, a perda, ou a apropriação abusiva do instrumento de pagamento, o utilizador uma vez que tenha conhecimento da operação já realizada, deve comunicar esses factos sem demora indevida, e dentro de um prazo até 13 meses a contar da data do débito, ao prestador de serviços de pagamento para que este possa realizar a retificação da operação não autorizada ou incorretamente executada.[266]

No que respeita à prova de autenticação e execução das operações de pagamento, caso um utilizador de serviços de pagamento alegue que uma operação não foi corretamente executada ou negue ter autorizado a referida operação, o prestador de serviços de pagamento deverá, neste caso, fazer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada, e que não foi afetada por qualquer avaria técnica ou por outra deficiência do serviço prestado.[267]

No caso de uma operação de pagamento não autorizada, o prestador de serviços de pagamento deve reembolsar imediatamente o ordenante do montante dessa operação e, se for caso, repor a conta

[264] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 69.º
[265] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 70.º núm. 2
[266] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 71.º núm. 1
[267] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 72.º

de pagamento debitada na situação em que estaria se a operação de pagamento não autorizada não houvesse sido executada, exceto se o prestador de serviços tiver motivos razoáveis para suspeitar de fraude e comunicar por escrito esses motivos à autoridade nacional relevante."[268]

O ordenante pode suportar até 50€, as perdas relativas às operações de pagamento não autorizadas resultantes da utilização de um instrumento de pagamento perdido, furtado ou da apropriação abusiva de um instrumento de pagamento, salvo se: i) a perda, o furto ou a apropriação abusiva não pudesse ser detetada pelo ordenante antes da realização de um pagamento, sempre que o ordenante não tiver atuado fraudulentamente; ou ii) a perda tiver sido causada por atos ou omissões de um agente, de um trabalhador ou de uma sucursal do prestador de serviços de pagamento ou de uma entidade à qual as suas atividades tenham sido expostas[269].

O ordenante vai suportar todas as perdas até ao limite do seu saldo disponível ou da linha de crédito associada à conta ou ao instrumento de pagamento, relativas a operações de pagamento não autorizadas se nelas tiver incorrido devido ao incumprimento com dolo ou por negligência grosseira ou a atuação fraudulenta.[270] No entanto, o ordenante não suporta as consequências financeiras resultantes da utilização de um instrumento de pagamento perdido, furtado ou da apropriação abusiva após ter procedido à comunicar esses factos ao prestador de serviços de pagamento.[271] Pois que, realizada esta comunicação, é a instituição de pagamento que dispõe de todos os meios para impedir a sua utilização não autorizada[272], portanto, sobre ela recai as responsabilidades das perdidas financeiras produzidas despois da comunicação feita pelo titular. Não obstante, a demora da comunicação será comummente imputável ao utilizador do serviço, pelo menos a título de negligência, sempre que o prestador de serviços de pagamento tenha disponibilizado os meios necessários à sua realização[273]

---

[268] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 73.º

[269] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 74.º

[270] Por exemplo, no ato de *phishing* (vem da palavra inglesa "fishing" (pesca), aludindo à tentativa de fazer os usuários morderem o gancho), se o utilizador tiver fornecido os seus dados com negligência (leve), haverá apropriação abusiva dos dados pessoais de pagamento com quebra da confidencialidade dos dispositivos de segurança personalizados imputável ao ordenante, devendo entender-se que cabe ao titular suportar o risco até um máximo de 50 euros, a menos que haja um comportamento com dolo, gravemente negligente, incumprimento deliberado das suas obrigações ou comportamento fraudulento. Nos demais casos, não responderá.

[271] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 74.º

[272] GUIMARÃES, Maria – Op. cit. p.590

[273] GUIMARÃES, Maria – Op. cit. p.593

Se o prestador de serviços de pagamento não exige a *autenticação forte do cliente*, o ordenante só suporta as perdas financeiras se tiver atuado fraudulentamente. Caso o beneficiário ou o seu prestador de serviços de pagamento não aceite a *autenticação forte do cliente*, deve reembolsar os prejuízos financeiros causados ao prestador de serviços de pagamento do ordenante.[274]

No evento de uma operação de pagamento baseada em cartão e o montante não seja previamente conhecido (por exemplo, reservas de hotel ou contratos de aluguer de automóveis), o prestador de serviços de pagamento só pode bloquear fundos na conta do ordenante se este tiver informado imediatamente após a receção da ordem de pagamento o montante exato dos fundos a bloquear. Nesse caso, o prestador de serviços de pagamento liberta, sem demora indevida, os fundos bloqueados na conta de pagamento do ordenante.[275]

Entretanto, uma operação de pagamento autorizada iniciada pelo beneficiário ou através deste, se a autorização da operação de pagamento não especifica o montante exato no momento em que foi concedida, ou se o montante da operação de pagamento excede o montante que o ordenante poderia razoavelmente esperar tendo em conta o seu perfil de despesas anterior, o ordenante tem direito ao reembolso do montante integral da operação de pagamento executada. Ainda que, o ordenante não pode basear-se em razões relacionadas com a taxa de câmbio.[276]

Os prestadores de serviços de pagamento passam a estar obrigados a aplicar procedimentos de *autenticação forte do cliente*, para aumentar a proteção dos dados pessoais de pagamento, no cenário que o ordenante aceda em linha à sua conta de pagamentos, ou quando inicie uma operação de pagamento eletrónico, ou quando realize uma operação através de um canal remoto que possa implicar uma atividade fraudulenta.[277]

Da mesma forma, também é preciso considerar o Regulamento Delegado (UE) 2018/389 de 27 de novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à *autenticação forte do cliente*

---

[274] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 74.º

[275] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 75.º

[276] Diretiva (UE) 2015/2366 relativa aos serviços de pagamento no mercado interno, art. 76.º núm. 1

[277] BASTO, Inés – A nova Diretiva de Serviços de Pagamento. Revista "Actualidade Jurídica Uría Menéndez", p. 122

e às normas abertas de comunicação comuns e seguras, mesmo que, entro em vigor no dia 13 de março de 2018, mas é aplicável a partir de 14 de setembro de 2019, com exceção do artigo 30º, n.ºs 3 e 5 (Obrigações gerais para as interfaces de acesso), que são aplicáveis a partir de 14 de março de 2019.[278]

É assim, que o Regulamento Delegado (UE) 2018/389, com o objeto de implementar medidas de segurança, estabelece os requisitos a cumprir pelos prestadores de serviços de pagamento que lhes permitam: i) Aplicar o procedimento da autenticação forte do cliente nos termos do artigo 97.º da Diretiva (UE) 2015/2366[279]; ii) Isentar da aplicação dos requisitos de segurança da autenticação forte do cliente, tendo por base o nível de risco, o montante e a recorrência da operação de pagamento e o canal de pagamento utilizado; iii) Proteger a integridade e a confidencialidade das credenciais de segurança personalizadas do utilizador; iv) Estabelecer normas para as comunicações entre os prestadores de serviços de pagamento relativamente à prestação e utilização de serviços de pagamento em aplicação do título IV[280] da Diretiva (UE) 2015/2366.[281]

No que respeita às medidas de segurança para a aplicação da *autenticação forte do cliente*, o Regulamento Delegado citado estabelece no seu art.º 4 que a autenticação deve basear-se em dois ou mais elementos pertencentes às categorias de conhecimento, posse e inerência e resultar na geração de um código de autenticação que só deve ser aceite uma vez pelo prestador de serviços de pagamento. Com o código de autenticação: i) Não é possível obter informação sobre os elementos pertencentes às categorias; ii) Não é possível gerar um novo código a partir dele; iii) O código não pode ser falsificado; iv) Não devem ser possíveis mais de cinco tentativas de autenticação falhadas consecutivamente num

---

[278] COMISSÃO EUROPEIA - **Regulamento Delegado (UE) 2018/389** da Comissão de 27 de novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras. Art.º 38

[279] COMISSÃO EUROPEIA - Regulamento Delegado (UE) 2018/389, op. cit. Art.º 97.- Autenticação:
1. Os Estados-Membros asseguram que os prestadores de serviços de pagamento apliquem a autenticação forte do cliente caso o ordenante:
a) Aceda em linha à sua conta de pagamento; b) Inicie uma operação de pagamento eletrónico; c) Realize uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou outros abusos.
2. No que diz respeito à iniciação de operações de pagamento eletrónico a que se refere o n.º 1, alínea b), os Estados-Membros asseguram que, em caso de operações de pagamento remotas, os prestadores de serviços de pagamento apliquem uma autenticação forte do cliente que inclua elementos que associem de forma dinâmica a operação a um montante específico e a um beneficiário específico.
3. No que diz respeito ao n.º 1, os Estados-Membros asseguram que os prestadores de serviços de pagamento disponham de medidas de segurança suficientes para proteger a confidencialidade e a integridade das credenciais de segurança personalizadas dos utilizadores de serviços de pagamento.
4. Os n.ºs 2 e 3 são igualmente aplicáveis caso os pagamentos sejam iniciados através de um prestador do serviço de iniciação do pagamento. Os n.ºs 1 e 3 são igualmente aplicáveis quando as informações forem solicitadas através de um prestador de serviços de informação sobre contas.
5. Os Estados-Membros asseguram que o prestador de serviços de pagamento que gere a conta permita que o prestador do serviço de iniciação do pagamento e o prestador de serviços de informação sobre contas se baseiem nos procedimentos de autenticação facultados pelo prestador de serviços de pagamento que gere a conta ao utilizador de serviços de pagamento, nos termos dos n.ºs 1 e 3, e, em caso de intervenção do prestador do serviço de iniciação do pagamento, nos termos dos n.ºs 1, 2 e 3.

[280] DIREITOS E OBRIGAÇÕES RELATIVAMENTE À PRESTAÇÃO E UTILIZAÇÃO DE SERVIÇOS DE PAGAMENTO

[281] COMISSÃO EUROPEIA - Regulamento Delegado (UE) 2018/389, op. cit. Art.º 1

determinado período de tempo; e v) Não deve exceder 5 minutos o tempo máximo de inatividade após o ordenante ser autenticado.

Do ponto de vista pagamentos celebrados à distância ou fora do estabelecimento comercial, quando o pagador é um consumidor nos termos do art.º 3 do Decreto – lei N.º 24/2014,[282] ele têm o direito fundamental[283] de receber informações amplas, suficientes e claras na fase pré-contratual pelo vendedor ou fornecedor do produto ou serviço, que é geralmente o beneficiário do pagamento; Informação obrigatória que é detalhada no art.º 4 do Decreto – lei N.º 24/2014, e que por extravasar o objeto desta dissertação fazemos referência só de aquelas que podem ser de interesse à proteção jurídica em pagamentos, tais como:

i) Identidade do fornecedor incluindo endereço e dados de contacto;
ii) Preço total do bem o serviço, incluindo taxas e impostos ou quaisquer outros encargos ou custos[284];
iii) O modo de cálculo de preços e os recargos quando não se poda realizar em momento anterior à celebração do contrato;
iv) A indicação de que podem ser devidos encargos suplementares posteriores ou outros custos;
v) As Modalidades de pagamento, de entrega, de execução, a data limite de entrega do bem ou serviço, e, se for o caso, o sistema de tratamento de reclamações.[285]

Bem assim, consoante com o art.º 19 no.º 2 e 3 do DL 24/2014, o fornecedor de bens ou prestador de serviços deve informar ao consumidor o incumprimento do contrato devido a indisponibilidade do bem ou serviço encomendado e reembolsá-lo dos montantes pagos no prazo máximo de 30 dias a contar do momento de ter informado a indisponibilidade. Se o reembolso não fora feito dentro do prazo indicado, o fornecedor fica obrigado a devolver em dobro os montantes pagos pelo

[282] Decreto – lei N.º 24/2014 relativa aos direitos dos consumidores e os contratos à distância, art.º 3 letra c) «Consumidor», a pessoa singular que atue com fins que não se integrem no âmbito da sua atividade comercial, industrial, artesanal ou profissional; (A relação jurídica de consumo dá-se quando á um fornecedor profissional de bens ou prestador de serviços, e um consumidor. Fora de este campo não há relação jurídica de consumo.)

[283] Desde 1989, a Constituição de Portugal, elevou os direitos dos consumidores à categoria de direitos fundamentais no capítulo relativo aos direitos e deveres económicos do Titulo III parte I. (BARBIERI, Diovanna – A PROTEÇÃO DO CONSUMIDOR NO COMÉRCIO ELETRÓNICO.p 24)

[284] O preço total, que deve incluir os custos totais, por período de faturação, no caso de um contrato periódico.

[285] Decreto – lei N.º 24/2014 relativa aos direitos dos consumidores e os contratos à distância, art.º 4. N.º 7: Incumbe ao fornecedor de bens ou prestador de serviços a prova do cumprimento dos deveres de informação estabelecidos no presente artigo.

consumidor, no prazo de 15 dias úteis, sem prejuízo do direito do consumidor de demandar à indemnização[286] por danos que possa ter lugar.[287]

A violação das normas presentes no Decreto-Lei n.º 24/2014 constitui a prática de contraordenação punível pela ASAE[288] com coimas que variam para as violações do art.º 4 do DL entre os € 400,00 e os € 2.000,00 para pessoas singulares; e os € 2.500,00 e os € 25.000,00 para pessoas coletivas. Em quanto às coimas no caso de violações do art.º 19 núm. 2 e 3 do DL antes citado, estas variam entre os € 500,00 e os € 3.700,00 para pessoas singulares; e os € 3.500,00 e os € 35.000,00 para pessoas coletivas.[289]

Conjuntamente ao aparato normativo, existe, como política de defesa do consumidor, o quadro institucional de promoção e tutela de direitos, formado por:

i. Associações e Cooperativas de Consumo[290];
ii. Centro Europeu do Consumidor;
iii. Centro de Informação Autárquica ao Consumidor;
iv. Centros de Arbitragem de Conflitos de Consumo;
v. Conselho Nacional do Consumo[291];
vi. Comissão de Segurança[292];
vii. Direção-Geral Consumidor;
viii. Instituto do Consumidor;
ix. Ministério Público;

[286] A indemnização pode ser por danos patrimoniais e não patrimoniais concordo ao art.º 562 (Indemnização) do Código Civil português, art.º 566 (Indemnização em dinheiro) do mesmo corpo legal, assim como do art.º 899 (Indemnização, não havendo dolo nem culpa) ibidem.

[287] Decreto – lei N.º 24/2014 relativa aos direitos dos consumidores e os contratos à distância, art.º 19

[288] Compete à ASAE, a fiscalização do cumprimento do disposto no Decreto-Lei n. º 24/2014 e a instrução dos respetivos processos de contraordenação, coimas e sanções. (Decreto – lei N.º 24/2014, art.º 30)

[289] Decreto – lei N.º 24/2014 relativa aos direitos dos consumidores e os contratos à distância, art.º 31

[290] Por exemplo, a Associação Portuguesa para a Defesa do Consumidor

[291] É um órgão consultivo do governo onde estão representadas a maiorias das entidades do Sistema de defensa do consumidor

[292] Por exemplo, a Autoridade de Segurança Alimentar e Económica, e o Instituto Português da Qualidade

CAPITULO IV

OS DADOS PESSOAIS DE PAGAMENTO E A SUA RELAÇÃO COM O CRIME INFORMÁTICO

4.1. O CRIME INFORMÁTICO

Do que foi desenvolvido até agora na presente investigação, podemos expressar que a Internet é o instrumento que permitiu moldar o conceito de globalização, uma vez que é uma tecnologia que tem colocado a informação, a cultura e a ciência ao alcance de todas as pessoas do mundo, até mesmo os criminosos que encontraram as fraquezas da rede, para atacá-la e, pior ainda, ficar impunes. De tal forma que o desenvolvimento das TIC's permitiu também, a execução de comportamentos antissociais que violam ou infringem a lei, através de atos criminosos tradicionais, de formas não tradicionais, conhecidos como crimes informáticos, cibercrimes, ou *computer crimen* de acordo com o seu termo anglo-saxão.

Na proposta de Rodriguez, Alonso e Lascuraín, os crimes Informáticos são:

> *"...todas aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad, y/o disponibilidad de los datos y sistemas informáticos, y ello sin perjuicio de que, además, pueden suponer una puesta en peligro o lesión de bienes jurídicos distintos"*[293]

Para Miguel Davara Rodríguez, o cibercrime é:

> *"...la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software."*[294]

Do acima exposto podemos inferir que o crime informático implica qualquer atividade ilegal que se enquadre em figuras tradicionais já conhecidas como roubo, furto, fraude, falsificação, prejuízo, burla e sabotagem, mas sempre que envolva o computador ou a informática como meio para cometer a ilegalidade, ou fim da própria ilegalidade.

---

[293] RODRIGUEZ, ALONSO e LASCURAÍN - DERECHO PENAL E INTERNET. Régimen Jurídico de Internet, pag. 504 "...todas aquelas condutas que põem em perigo ou danifiquem a integridade, confidencialidade e/ou disponibilidade de dados e sistemas informáticos, e isto sem prejuízo de que, além disso, podem acarretar um perigo ou prejuízo a diferentes bens jurídicos." (tradução minha)

[294] DAVARA RODRÍGUEZ., Miguel Á. – Manual de Derecho informático.P. 389 "...a execução de uma ação, que reunindo as características que definem o conceito de crime [ou delito], seja realizada utilizando um elemento de informático e/ou telemático, ou violando os direitos do titular de um elemento informático, seja *hardware* o *software*." (tradução minha)

Portanto, os interesses ou bens lesados por violações no uso da informática poderão ser de diferente ordem, dependendo da finalidade de cada sistema informático ou, se preferir, dependendo do conteúdo de seus programas. Assim, temos lesões de ordem moral como a manipulação indevida de dados pessoais que violam a privacidade, lesões que podem acarrar consequências económicas como a violação ou a manipulação de secretos industriais ou comerciais ou roubo de quantias em dinheiro, chegando até a violação ou manipulação de dados políticos ou militares com resultados negativos para a paz, imprevisíveis ou verdadeiramente catastróficos.[295]

Os crimes informáticos são caracterizados por:

i. Ser Crimes Ocupacionais quando são cometidos por pessoas que trabalham com um sistema informático e, principalmente, quando é praticado contra o proprietário do referido sistema ou, pelo menos, indiretamente, ao ser este prejudicado;
ii. São Crimes de Oportunidade Especial porque a sua comissão será levada a cabo no momento mais favorável para isto;
iii. São considerados de "Colarinho Branco"[296], por exigir de uma preparação e conhecimento, além dum nível cultural e econômico. [297]
iv. É transnacional, porque o cibercrime, não se detém pelas fronteiras físicas ou temporais, ou seja é transfronteiriço ou extraterritorial, quer dizer, que o ato punível pode atingir dois ou mais Estados. Temos a questão de saber que lei vai ser aplicada, caso no qual, o princípio básico é da territorialidade (aplicação da lei penal no espaço), se os factos ocorrem em Portugal aplica-se a lei penal portuguesa.[298]
v. Têm temporalidade, o que faz referencia no momento que inicia o ato ilícito e quando este se materializa ou causa o prejuízo. Portanto, pode haver um desfasamento temporal entre o momento em que o agente atua, e o momento em que um *software* produz um determinado resultado. Isto coloca problemas ao nível da determinação do momento da prática do facto, porque a sua atuação está fragmentada.

---

[295] VILARIÑO PINTOS, Eduardo - El delito informático, p. 808.

[296] Término cunhado em 1924 por Edwin Sutherland (1883-1950), sociólogo americano considerado um dos criminologistas mais influentes do século XX.

[297] VILARIÑO PINTOS, Eduardo – Op. Cit., p. 812.

[298] O legislador português considera que o relevante é o local da atuação do agente, mas também é relevante o local onde o resultado se produziu, ou se devia ter produzido no caso de tentativa. Basta que um desses elementos tenha conexão com o território português, a lei penal portuguesa considera se competente para julgar os agentes do crime.

vi. Facilidade de Repetição, ao considerar que a função principal de um computador é a repetição de tarefas, isto pode facilitar os ataques informáticos ao ser repetida sem grande esforço dos atacantes contra a mesma vítima ou contra vítimas distintas;
vii. A automação, a qual esta associada ao sistema e os aparelhos informáticos;
viii. O anonimato, porque o rasto pode ser apagado, ou é possível usar programas que escondem a identidade dos atacantes;
ix. A complexidade, pela sofisticação dos ataques de computador, sem precisar ter grandes conceitos informáticos, e pela necessidade de criação de equipas de investigação que sejam multidisciplinares, com conhecimentos do direito e da informática.
x. Ser crimes danoso, ao abranger um número muito grande de vítimas, o que pode gerar sentimentos de insegurança.

Com base na conceção do crime no direito penal, toda ação ou omissão requer que os seguintes 4 elementos básicos estarem presentes: um comportamento humano Típico, Antijurídico (ilegal), Culpável e Punível, assim temos:

i. Facto típico (elemento material). Quer dizer, que descreva um comportamento que lesa ou cause danos ao bem jurídico protegido. O conforma a ação que é desenvolvida pelo autor; portanto é o resultado da ação, e a relação de causalidade que deve existir entre a ação do autor e o resultado.
ii. Facto ilegal (elemento jurídico). Isto é, que o comportamento está descrito em uma lei devidamente emitida pela autoridade competente cujo incumprimento é objeto de violação ou transgressão.
iii. Facto culpável (elemento moral). O constitui a imputabilidade. Que há responsabilidade pela infração, seja por descuido, negligência, imperícia ou por agir com dolo por ser cometida com consciência e vontade.
iv. Facto punível (elemento jurídico). Significa, que a lei penal ou especial criminal, prescreve uma pena privativa de liberdade e/ou económica.

A doutrina normalmente diz que um facto típico se divide, em tipo incriminador e tipo justificador. Temos o tipo incriminador que se preenchido estabelece a culpa a uma pessoa por cometer o crime, e

temos o tipo justificador que legitima o comportamento dessa pessoa, exemplo: a legítima defesa, o direito de necessidade ou o conflito de deveres. O tipo incriminador está formado pelo tipo objetivo de ilícito e o tipo subjetivo de ilícito.

O tipo subjetivo de ilícito liga-se à componente interna do agente, que pode ser dolosa ou negligente. Assim, o art.º 14 do Código Penal português estabelece o dolo (direto, necessário e eventual), o art.º 15 letra a) ibidem trata da negligência consciente, e letra b) sobre negligência inconsciente. "O dolo, como elemento subjetivo geral, resume-se à consciência e vontade do agente direcionadas à realização da conduta descrita em um tipo penal objetivo".[299]

Ao nível do tipo objetivo de ilícito o compõem os seguintes elementos: Sujeito ativo[300], responsável de uma ação ou uma omissão, um resultado, com um nexo causal e uma imputação objetiva. No cibercrime é importante sublinhar que o nível do tipo objetivo de ilícito, a conduta ou o bem jurídico, um deles, tem de ser digital ou informático para ser considerado um crime informático.

O sujeito ativo do crime informático é o homem singularmente considerado responsável duma infração criminal,[301] também conhecido como autor, réu possível[302], criminoso,[303] agente[304] ou arguido[305] que possui conhecimentos gerais sobre a informática. No entanto, deve-se notar que difere do criminoso comum, pela capacidade que ele tem de operar os sistemas informáticos ou computacionais, é por isso, que são comumente chamados *Hackers*,[306] *Crakers*[307] ou pirata informático. Pelo geral, o sujeito ativo do crime é uma pessoa de certo *status* socioeconómico, pelo que a sua comissão não pode ser explicada

[299] FLORENTINO, Bruno - Tipo e tipicidade, tipo objetivo e tipo subjetivo. Dolo e culpa. [Em linha]. [Consult. 21 Junho 2018]. Disponível na internet: https://brunoflorentinosilva.jusbrasil.com.br/artigos/183249818/tipo-e-tipicidade-tipo-objetivo-e-tipo-subjetivo-dolo-e-culpa

[300] Ao nível do tipo objetivo de ilícito temos este pormenor importante sobre o sujeito ativo ou autor. Começa-se a falar se de um terceiro autor, quando falamos da responsabilidade dos *agentes de software*, há já discussão no parlamento europeu sobre esta questão embora no âmbito civil.

[301] SANTOS, Manuel e LEAL-HENRIQUES, Manuel – Noções Elementares de Direito Penal, p. 69

[302] DA MATTA, Caeiro – Direito Criminal Português. II, p.214

[303] DA MATTA, Caeiro – Op. Cit., p 215

[304] DECRETO-LEI nº 400/82 Código Penal Português, art.º 3

[305] DECRETO-LEI nº 400/82 Código Penal Português, art.º43 núm.3.

[306] Pessoa com grandes conhecimentos de informática e programação, que se dedica a encontrar falhas em sistemas e redes computacionais. = CIBERPIRATA, PIRATA INFORMÁTICO "hacker", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://priberam.pt/dlpo/hacker [consultado em 04-09-2018].

[307] Pirata informático especializado em penetrar sistemas de segurança ou descodificar programas ou códigos informáticos. "cracker", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://priberam.pt/dlpo/cracker [consultado em 04-09-2018].

pela pobreza, ou pela falta de recreação, ou baixa escolaridade, nem pela baixa inteligência ou instabilidade emocional.[308]

Assim, com os casos condenados, observou-se que o perfil do sujeito ativo varia de acordo com o tipo de crime cometido, desde empregados ou ex-funcionários, terceiros em conveniência, usuários insatisfeitos, espiões profissionais ou industriais, investigadores privados, empresas de marketing, agências de qualificação de crédito ou solvência patrimonial, que geralmente baseiam os seus atos por uma motivação: Ideológica ao fazer ataques contra organizações políticas ou Estados; Económica quando eles procuram lucrar; Sociais quando procuram ser aceitos e reconhecidos pelo seu círculo social; De conhecimento quando procuram demonstrar as suas habilidades, violando os sistemas de segurança informáticos. Da mesma forma, há aqueles que cometem esses crimes, apenas por diversão.

Em oposição ao sujeito ativo temos o sujeito passivo, que é a vítima da infração[309], aliás, qualquer pessoa particular, entidade legal ou organização pública ou privada titular do bem jurídico lesado[310] sobre a qual recai a ação maliciosa feita pelo sujeito ativo[311], podendo diferir da parte prejudicada.

Consequentemente, para que qualquer ato poda ser considerado um crime, são necessárias a concordância dos seguintes elementos integrados:

i. Um agente, ou autor isto é, um indivíduo que viola o Estado de direito e, portanto, ao ser imputável incorre nas condições punitivas determinada pelo legislador.
ii. Um objeto que é determinado pelo direito violado se eles pertencem às pessoas singulares ou coletivas, normalmente entendidos no campo jurídico como o bem jurídico protegido.
iii. A vítima, em outras palavras, a pessoa que sofre a lesão;
iv. O fim, dizendo, a perturbação da ordem legal.

[308] PAEZ, Juan; ACURIO, Santiago, DERECHO Y NUEVAS TECNOLOGÍAS. 1ª. p. 186

[309] DA MATTA, Caeiro – Direito Criminal Português. II p.213

[310] Por exemplo programas ou sistemas eletrónicos onde a informação requerida é encontrada.

[311] DA MATTA, Caeiro – Op. Cit., p. 222

O Direito Penal português, embora esteja em grande parte no código penal português, abarca também as leis penais extravagantes ou diplomas que se ocupam de determinados setores da vida na sociedade. O caso clássico é a Lei n.º 109/2009, conhecida como a Lei do Cibercrime, que prevê crimes informáticos em sentido estrito, ao ser crimes cuja descrição típica ou valor tutelado seja informático ou digital.

Em contraposição ao conceito de crime informático ou cibercrime em sentido estrito. Temos o crime informático em sentido amplo, que diz respeito aos comportamentos que não implicam o uso de tecnologias mas que podem ser realizados ou consumados através das novas tecnologias, e que podem ser crimes informáticos. Exemplo: A injúria e a difamação, determinada nos arts.º 180 e 181 do Código Penal português. A injúria e a difamação podem ser considerados crimes informáticos em sentido amplo, porque não precisa ser realizados através de meios informáticos mas podem sê-lo. Nesses casos a prova pode ser digital, e podemos aplicar isto a crimes informáticos em sentido amplo.

No Código Penal há um princípio básico que é a legalidade (*Nullum crimen, nulla pœna sine lege*), para cumprir com este princípio o legislador europeu e português não criminalizam os ataques informáticos específicos como o *ransomware*[312] enquanto uma realidade completa, já que eles ficariam rapidamente ultrapassados, produto do desenvolvimento tecnológico. A abordagem do legislador foi de segmentar os comportamentos, não punimos o *ransomware*, mas punimos o acesso ilegítimo. Da mesma forma, a componente de danificação dos dados por encriptação, já está coberto por um outro tipo legal.

A vantagem desta técnica é que permite ao julgador e legislador ter uma lei cuja vigência e atualidade seja mais prolongada, independentemente do tipo de ataque, se houver destruição ou alteração dos dados há sempre uma solução legal para isso. Mas essa perenidade da lei penal é feita à custa de uma certa abstração dos termos utilizados, que por muitas vesses torna difícil a compreensão do alcance do tipo legal.

[312] é um tipo de software nocivo (*malware*) que vai encriptar os dados informáticos, tornar inacessíveis os dados informáticos. É um bloqueio/encriptação dos ficheiros a não ser que se pague o resgate. Os meios de difusão são vários, através de *sites*, explorando o JAVA e o Flash, que apresentam vulnerabilidades para instalação de malware. Também através do *email*, através de docs, ou qualquer outro ficheiro executável. Há agora a criação de *ransomware* adequado às necessidades dos clientes, quem cria recebe uma parte e quem distribui recebe outra.

Deste jeito, partindo da segmentação de comportamentos, na perspetiva de EDUARDO VILARIÑO PINTOS[313], as infrações através da informática podem ocorrer em qualquer uma das quatro áreas ou fases fundamentais das operações informáticas que, em geral, são realizadas num sistema de processamento eletrónico de dados. Além disso, cada uma dessas áreas ou fases responderá a tipos específicos de infrações:

i. Na primeira fase, a entrada ou *input*, em que a informação é transferida para uma linguagem inteligível para o computador, é fácil de inserir dados falsos, alterar a informação ou excluir a entrada dos documentos-chave; Esta é uma das formas mais comuns dos crimes informáticos. Em geral, os crimes financeiros começam nesta fase.
ii. Na segunda fase, da programação, onde são fornecidos ao computador a sequência lógica de operações para resolver problemas, onde as violações ocorrem quando são introduzidas ordens que levam sistematicamente a uma alteração dos resultados do programa; geralmente é a base das infrações mais graves.
iii. Na terceira fase, é da saída conhecida como *output*, na qual a informação que provém da memória do computador é transferida para a linguagem inteligível do homem, as infrações mais frequentes são do tipo de furto de informação privada.
iv. Na quarta e última fase é das operações, a comunicação de informações que envolve o uso de circuitos telefónicos (ou através de um ponto de acesso de rede sem fio) para transmitir informações do computador para o terminal e vice-versa, e a partir de um computador para outro, as violações são feitas pela interceção dos dados dada a possibilidade de unir um terminal não autorizado para conhecer os dados privados e possivelmente manipulá-los.

Desse jeito, vemos que o crescimento do crime informático na última década tem sido uma constante em todo o mundo, por exemplo, estima-se que o impacto económico dessa atividade esta cerca de USD $ 3 trilhões no planeta, um número ainda maior do que o tráfico ilegal de drogas (USD$ 1 trilhão), onde as regiões mais afetadas, cujo mercado movimenta cerca de USD $ 12.500 milhões por ano, são Ásia (49% dos ataques), Europa (28%), América do Norte e do Sul (19%). Só a Indonésia, tem um 14% do tráfego malicioso mundial, e com um total de 6.600.000 ataques cibernéticos por dia; O setor mais

[313] VILARIÑO PINTOS, Eduardo – Op. Cit., p.810

afetado por esse crime é o financeiro (75,29% dos ataques), o segundo é o Governo (10,56%), seguido pelas indústrias de comunicações (8,41%), energia (3,71%), indústria (1,98%) e do comércio com apenas um 0,05%[314].

Por outro lado, vemos casos como de Evaldas Rimasauskas de 48 anos, quem tem sido demandado por engano contra Facebook e Google em uma quantia de mais de 100 milhões de dólares, por utilizar um esquema de *Phishing*[315] desde o ano 2013, pelo qual foi acusado de fraude, roubo agravado de identidade e lavagem de dinheiro. As duas empresas confirmaram que alguns dos seus empregados foram enganados pelo suspeito.[316]

Os ciber ataques com o uso de *Malware*[317] são muito variados. Dentro deste grupo podemos encontrar termos como: *Worms*, Vírus, *Trojans*, *Spyware*, *Botnets*, etc.:

i. ***Worm*** (Minhoca): A caraterística principal deste *software* é a sua capacidade de auto replicação sem intervenção humana. Estamos a falar normalmente de *emails* com anexos que vem com informações apelativas, com duas extensões. Este tipo de ataque não destrói os dados, mas a sua capacidade de replicação é tal que vai enchendo os discos de memória de forma que o sistema não consegue correr por falta de espaço ou saturação nas redes. A forma de atuação dos *worms* é levar a um maior consumo. O seu potencial nocivo vai mais pelo consumo de recursos.
ii. **Vírus**: A sua caraterística comum é a possibilidade de eliminação de dados informáticos, por essa caraterística são mais perigosos do que os *worms*. Estão num patamar acima dos *worms*, porque tem essa capacidade de multiplicação mas para alem disso, associa uma capacidade

[314] DINERO.COM - El cibercrimen es un delito más rentable que el narcotráfico. 28/09/2015 [Consult. 01 jul 2018]. Disponível na internet: https://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-**colombia**/213988

[315] A palavra Phishing, foi "batizada em 1996, aquando a sua menção teve lugar num *newsgroup* denominado como *alt.onlineservice.america-online*" e é um acrónimo de origem inglês que guarda relação com o ato de pescar, (em inglês "Fishing"), que aplicado na ciência da informática, exemplifica a pesca de informação. (AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação.p. 67) Assim, o phishing é um ataque que visa obter dados sensíveis, exemplo dados pessoais bancários o de pagamento e é um tipo de ataque que pode utilizar vários meios. Há por ex. o envio de *email* com um link onde se tem de preencher e dessa forma há recolha de dados de formas ilegal. O tipo de phishing não tem um tipo legal exclusivo para ele.

[316] ALVES, LAURINDA - FACEBOOK E GOOGLE VÍTIMAS DE ESQUEMA DE 'PHISHING' DE MAIS DE 100 MILHÕES.

[317] É a abreviação de "Software mal-intencionado", um termo que engloba todos os tipos de *software* mal-intencionado ou código de computador cuja função é danificar um sistema ou causar um mau funcionamento. Programa concebido para causar danos ou para aceder ilegalmente a informação em sistemas informáticos "Malware", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://priberam.pt/dlpo/Malware [consultado em 04-09-2018].

de apagar dados informáticos. Temos diferentes classificações de vírus consoante a sua atuação. Há vírus que atuam com o arranque e há outros que atuam dentro do sistema operativo. Há vírus polimórficos, que mudam o seu código para não ser detetados. Podem vir associados aos jogos, aos programas, aos documentos, ou podem estar em outros ficheiros.

iii. ***Trojan***: O cavalo de troia. Há diferentes tipos de *trojan.* É um *software* que tem uma aparência legítima mas que no seu interior tem *software* malicioso que vai afetar o sistema. Isto vai permitir uma serie de possibilidades, desde *keyloggers*[318], o qual já foi mais utilizado no caso de acesso às contas bancarias. Outra possibilidade é a de controlar os microfones e camara dos computadores.

iv. ***Spyware*:** Programa informático que espia o utilizador, coleta informação digitada pelo utilizador (texto digitado, passwords, números de cartões de crédito, etc...), pode ainda ser utilizado para coletar o tempo de utilização de determinados *sites*, isto é informação com valor para determinadas empresas.

Um dos ataques mais comuns atualmente é chamado **DDOS** (também conhecido como *DoS Attack)*[319] que é um ataque de negação de serviço com a utilização de *malwares*, refere-se à tentativa de tornar os recursos dum sistema, indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na *WWW.*

Baseado em isto, um estudo realizado na França refletiu as seguintes causas do crime informático:

i. Descentralização de sistemas, o que faz com que o usuário tenha um papel mais importante e maior acesso aos recursos do sistema de informático.
ii. A conexão dos sistemas informáticos entre si. Isso ocorre dentro da mesma empresa e entre diferentes empresas ao nível nacional e internacionalmente. O exemplo mais atual é a Internet, uma rede de computadores que liga milhares de computadores e mais de cem milhões de usuários em todo o mundo.

[318] "Consiste num programa do Tipo *spyware* de vigilância, que tem como objetivo captar, registar e armazenar tudo o que se digita (como números de cartão bancário e senhas), ou seja, reconhece os caracteres introduzidos pelo utilizador." AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação. P.88

[319] É um acrônimo em inglês para *Denial of Service*

iii. O desenvolvimento dos meios de pagamento eletrónico, que permite a sua transferência e gestão sem a presença física do titular. Nesse sentido, é muito mais fácil e discreto pegar dinheiro de um banco por computador do que entrar com armas. Assim, o monto da defraudação nesses assuntos são muito maiores do que os crimes tradicionais.[320]

Como resultado desses factos, podemos observar que as atividades criminosas realizadas por qualquer pessoa que faz um uso indevido dos meios eletrónicos e informatizados, podem causar grande perda económica para as pessoas, empresas e até mesmo para o governo.

4.2. A CLASSIFICAÇÃO DO CRIME INFORMÁTICO.

As várias atividades criminosas relativas com a informática apresenta diferentes ações para consumar a lesão, o que tem motivado a necessidade de uma classificação aberta[321] do cibercrime, tendo em conta os elementos que as constituem e os bens juridicamente protegidos e, dentro dessas categorias, procuramos distinguir as ações típicas que a vida cotidiana ou a experiência nacional ou internacional manifestam.

Nesse âmbito, JULIO TÉLLEZ VALDÉS[322] classifica o cibercrime com base em dois critérios: A) como *instrumento ou Meio*, ou B) como *Fim ou Objetivo*:

A. Instrumento ou Meio: Nesta categoria temos comportamentos criminogênicos que utilizam computadores como método ou meio na prática do crime, por exemplo:

i. Falsificação de documentos através da informática (cartões de crédito, débito, etc.).
ii. Variação de ativos e passivos na contabilidade das empresas.
iii. Simulação ou planeamento de crimes convencionais (fraude, roubo, homicídio, etc.).
iv. Roubo de tempo dum computador.

---

[320] PALAZZI, Pablo - DELITOS INFORMATICOS. 1ra. Buenos Aires, p.60

[321] O modo de cometer um crime, e as múltiplas facetas que o uso da informação oferece, impossibilita uma classificação fechada para que possa compreender todas as possibilidades que existem, no entanto, certas características concorrem, comuns a todos os comportamentos catalogadas como crimes informáticos.

[322] TÉLLEZ Valdés, Julio - Derecho Informático. 4ta, p.190

v. Leitura, cópia ou subtração dos dados confidenciais.
vi. Modificação dos dados, na entrada ou na saída.
vii. Uso indevido ou violação de um código para entrar num sistema, (Cavalo de Tróia).
viii. Variação quanto ao destino de pequenas quantias de dinheiro para uma conta bancária falsa (técnica de salame)[323].
ix. Uso não autorizado de programas informáticos.
x. Introdução de instruções que causem interrupções na lógica interna dos programas, a fim de obter benefícios.
xi. Alteração no funcionamento dos sistemas.
xii. Obtenção de informações residuais impressas em papel ou fita magnética após a execução dum trabalho.
xiii. Acesso às áreas informatizadas de forma não autorizada.
xiv. Intervenção nas comunicações dos dados.

B. Fim ou Objetivo[324]: Nesta categoria, enquadramos comportamentos criminogênicos que são direcionados contra o computador, acessórios ou programas como uma entidade física. Alguns exemplos são os seguintes:

i. Programação de instruções que produzem um bloqueio total ao sistema.
ii. Destruição de programas por qualquer método.
iii. Danos à memória.
iv. Ataque físico contra a máquina ou seus periféricos.
v. Sabotagem política ou terrorismo onde são controlados ou destruídos os centros nervosos informatizados.
vi. Sequestro de suportes magnéticos contendo informações valiosas para fins de chantagem, pagamento de resgate, etc.

[323] Furto de pequenas quantias de dinheiro quási imperceível de um grande número de titulares.
[324] TÉLLEZ Valdés, Julio - Derecho Informático. 4ta, p.190

Partindo da perspetiva de MIGUEL DAVARA RODRIGUEZ,[325] as ações criminais relacionadas com a informática centram as suas atividades no acesso e/ou manipulação de dados que se encontram em suportes informáticos ou em programas do computador. O doutrinário aponta que a manipulação através da informática pode vir de dois aspetos diferentes: **a)** acesso e manipulação dos dados e **b)** Manipulação dos programas. Assim, faz uma classificação baseada em seis ações de acordo com o propósito que elas buscam:

i. Manipulação dos dados e informações contidas nos arquivos ou suportes informáticos sim autorização do titular.
ii. Acesso e uso de dados por aqueles que não estão autorizados a fazê-lo.
iii. Introdução de programas ou rotinas em outros computadores para destruir informações, dados ou programas.
iv. Uso do computador e/ou programas de outra pessoa sem autorização, a fim de obter seus próprios benefícios e em detrimento de outro.
v. Utilização do computador para fins fraudulentos.
vi. Agressão à privacidade através do uso e processamento de dados pessoais para fins diferentes dos autorizados.

Na opinião de CORREA[326], este autor cita uma antiga classificação de *Ulrich Sieber* e distingue as seguintes categorias:

i. Fraude por manipulações de um computador contra um sistema de processamento de dados.
ii. Espionagem computacional e roubo de *software*.
iii. Sabotagem informático.
iv. Roubo de serviços.
v. Acesso não autorizado aos sistemas de processamento de dados.
vi. Ofensas tradicionais em negócios assistidos por computador.

[325] DAVARA RODRÍGUEZ., Miguel Á. op. cit., p. 393
[326] PALAZZI, Pablo - DELITOS INFORMATICOS. 1ra., p.40

Além do mais, as Nações Unidas[327] reconhecem como crimes informáticos os seguintes:

i. Fraudes cometidas por manipulação de computadores: **a)** manipulação de dados de entrada [também conhecida como subtração de dados]; **b)** manipulação de programas; **c)** manipulação dos dados de saída.
ii. Falsificações informáticas: **a)** quando os dados informatizados dos documentos armazenados são alterados; **b)** quando os computadores são usados para falsificar documentos de uso comercial.
iii. Danos ou modificações de programas ou dados informatizados: **a)** sabotagem informática por meio de vírus, *worms*, bombas lógicas ou cronológicas.
iv. Acesso não autorizado aos serviços e sistemas de informática**: a)** piratas informáticos ou *hackers*; **b)** reprodução não autorizada de *software* protegido legalmente; e **c)** o estipulado nas legislações internacionais.

Em 1989, o Departamento de Justiça dos EUA, no seu Manual de Recursos da Justiça Penal sobre os crimes "*Computer Crime: Criminal Justice Resource Manual",* parte da ideia que as comissões das infrações são realizadas através de diferentes "Técnicas", entre as quais se destacam como as mais comuns até agora detetadas, as seguintes:

i. **Fraude de dados** *(data didling):* É a técnica mais simples, segura e utilizada para a prática de infrações informáticas; inclui a alteração de dados antes ou durante a sua incorporação no computador.
ii. **Cavalo de Tróia** *(Trojan horse):* Definido no subcapítulo 4.1 *(O CRIME INFORMÁTICO)* como um *Malware*, e que consiste em colocar sub-repticiamente instruções num computador, a fim de executar funções não autorizadas; É a técnica mais comum para fraude e sabotagem de programas.
iii. **Técnicas de Salame** *(rounding down)*: É o nome dado ao furto de pequenas quantias de dinheiro de um grande número de titulares, de modo que, em cada caso, a subtração é praticamente impercetível.

[327] TORRES CHAVES, Efraín - Breves Comentarios a la ley de Comércio Electrónico, Firmas Electrónicas y Mensajes de Datos, pag. 89.

iv. **Armadilhas** *(trap down)*: É prática dos programadores para produzir quebras no código informático por meio da inserção de um código adicional ou sua modificação.

v. **Bombas Lógicas** *(logia bombs)*: É a execução de um programa num determinado momento ou periodicamente num computador para a perpetração de um ato malicioso não autorizado.

vi. **Limpeza** *(scavenging):* É a técnica para obter as informações que podem permanecer dentro ou em torno de um sistema informático após a execução de um trabalho.

vii. **Vazamento de dados** *(data leakage):* consiste na transferência de dados ou cópias de dados de um sistema informático para outro.

viii. **Carregar e Personificar a identidade** *(piggybacking and impersonation)*: Carregar significa ter acesso a áreas controladas e Personificar a Identidade significa aceder sob a identidade de outra pessoa que tenha acesso ao sistema; Em ambos os casos, pode ser feito física ou eletronicamente.

ix. **Intercetação** (*wire tapping*): Consiste em uma conexão nos fios de comunicação entre o computador e um Terminal.

x. **Simulação e Modelagem** (*simulation and modeling*): Neste caso, o computador será utilizado não só como instrumento para cometer a infração, mas também para planejá-la ou controlá-la; A sofisticação dessa técnica é que ela precisa do uso dum computador com uma adequada capacidade de elaboração.

xi. **Ataques assíncronos** (*Asynchronous Attacks*): Aproveitando uma característica do sistema operacional que permite renderização dinâmica das funções executadas. A maioria dos sistemas operacionais de computadores funciona de forma assíncrona com base nos serviços que devem ser executados para os vários programas de computador executados no computador. Os programadores ou operadores de computador podem obter acesso à cópia de reinicialização do ponto de verificação do programa, dados e parâmetros do sistema.

xii. ***Superzapping*** (denominação derivada do programa utilitário chamado superzap): Consiste no uso não autorizado dum programa utilitário para alterar, apagar, copiar, inserir dados ou usar de forma não autorizada aqueles armazenados num computador ou em meio magnético.

Do que está exposto, vemos como: doutrinários, organizações internacionais e juristas, emitiram classificações de cibercrime com base em ações típicas de criminalidade informática, das quais é possível inferir que as principais atividades criminosas orientadas para: Um lucro; apropriação ilícita de

fundos; causar danos a terceiros; agir sem autorização ou de forma dolosa ou fraudulenta; violar o sigilo, a segurança, a confidencialidade, a privacidade ou a intimidade; ou apenas a sabotagem, podem ser resumidos nos seguintes atos:

- **i.** A falsificação de documentos ou informações através de um sistema informático;
- **ii.** A modificação ou alteração de dados armazenados ou processados num sistema de informação ou em redes eletrónicas;
- **iii.** A supressão, eliminação ou apagado dos dados armazenados ou processados num sistema de informação ou redes eletrónicas;
- **iv.** A subtração, a obtenção, a cópia, a transferência, a apropriação ou o sequestro de dados armazenados ou processados num sistema de informação ou em redes eletrónicas;
- **v.** A reprodução, a difusão ou a divulgação de dados armazenados ou processados num sistema de informação ou redes eletrónicas;
- **vi.** O acesso ou uso não autorizado de informações, serviços ou dados armazenados ou processados num sistema de informação ou redes eletrónicas;
- **vii.** O acesso ou a utilização fraudulenta ou não autorizada dum computador ou *hardware*;
- **viii.** O dano, a rutura ou a destruição da unidade física de processamento de dados ou *hardware*.
- **ix.** O dano, a perturbação ou a destruição de dados, programas de computador ou *software*;

4.3. OS TRATADOS E AS CONVENÇÕES INTERNACIONAIS.

Partindo da relevância dos princípios da legalidade e da territorialidade no domínio criminal, de onde resultaria uma fragmentação generalizada para os regimes nacionais, surge a necessidade, de olhar pontos de referência normativos acima das leis dos estados soberanos, em matéria penal substantiva e ao mesmo tempo de cooperação entre as polícias e entre as autoridades judiciais nacionais[328]. Dessa maneira, considerando como antecedente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (Conselho da Europa) em 1950[329], assim como as

[328] Em 1983, a **OCDE** apresentou um estudo sobre a possibilidade de aplicar e harmonizar leis penais a nível internacional contra o uso indevido de programas de computador. Posteriormente, em 1986, publicou um relatório sobre Crimes da informática, onde foram feitas propostas de reformas legislativas para vários Estados-Membros e recomendou uma lista mínima de exemplos de usos indevidos que os países poderiam proibir e sancionar em leis criminais.

[329] Citada no Capitulo I, Subcapítulo 1.2.2.

Recomendações do Comité dos Ministros[330] e as Resoluções adotadas pelos Ministros europeus da Justiça[331], foram desenvolvidas as seguintes normas:

4.3.1. Convenção N.º 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, do Conselho de Europa, em 1981.

A convenção n.º 108 do conselho da europa, de 28 de janeiro de 1981 ocupou-se já também de matérias de crime quando no seu art.º 7 decreta que, "Para a proteção dos dados de carácter pessoal registados em ficheiros automatizados devem ser tomadas medidas de segurança apropriadas contra a destruição (...) não autorizada, (...) e também contra o acesso, a modificação ou a difusão não autorizados,"[332] devindo as partes "estabelecer sanções e vias de recurso apropriadas em face da violação das disposições do direito interno que confiram eficácia aos princípios básicos para a proteção dos dados"[333]

4.3.2. Convenção sobre Cibercrime, do Conselho da Europa em 2001.

Adotada pelo Comité de Ministros do Conselho da Europa na sessão n.º 109 de 8 de novembro de 2001 e assinada em Budapeste em 23 de novembro de 2001 entrou em vigor em 1º de julho de 2004, decorrente da "Necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional"[334]

---

[330] Também serviram de antecedentes "as Recomendações do Comité de Ministros N.º **R (85)** 10 relativa à aplicação prática da Convenção Europeia de Auxílio Judiciário Mútuo em matéria penal no tocante às cartas rogatórias para interceção de telecomunicações, N.º **R (88)** 2 sobre as medidas destinadas a combater a pirataria no domínio dos direitos de autor e direitos conexos, N.º **R (87)** 15 que regulamenta a utilização de dados pessoais no sector da polícia, N.º **R (95)** 4 sobre a proteção de dados de carácter pessoal no sector das telecomunicações, designadamente os serviços telefónicos, e **R (89)** 9 sobre a criminalidade informática que estabelece diretrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos, e ainda a **R (95)** 13 relativa a problemas da lei processual penal ligados às tecnologias da informação" (CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Preâmbulo)

[331] "A Resolução n.º 1 adotada (...) na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), (...) recomenda ao Comité de Ministros o apoio ao trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) no domínio do cibercrime, a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios eficazes para investigar esses crimes (...) [e] a Resolução n.º 3 adotada na 23.ª Conferência (...) (Londres, 8 e 9 de Junho de 2000), que encoraja as partes intervenientes nas negociações a prosseguirem os seus esforços para encontrar soluções adequadas que permitam ao maior número possível de Estados tornarem-se partes da Convenção, e reconhece a necessidade de haver um sistema de cooperação internacional rápido e eficaz que tenha devidamente em conta as exigências específicas da luta contra o cibercrime" (CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Preâmbulo)

[332] CONSELHO DA EUROPA - Convenção 108 para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, art.º 7.

[333] CONSELHO DA EUROPA - Convenção 108, Op. Cit., art.º 10.

[334] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Preâmbulo.

Busca "Impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de *(sic.)* desses sistemas, redes e dados, assegurando a incriminação desses comportamentos"[335], bem como, "a adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a deteção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto a nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável"[336]

A Convenção sobre Cibercrime tem 3 partes: O direito penal substantivo; O direito processual penal e; A cooperação internacional. No seu Capitulo II sobre Medidas a adotar a nível nacional, na Seção 1 das normas de Direito Penal (substantivo), tipifica no Título 1, as infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, no seguinte sentido:

> **"Artigo 2.º – Acesso ilícito:** (...) quando praticado intencionalmente, o acesso ilícito a um sistema informático no seu todo ou a parte dele. Para que se verifique a infração penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático."[337]
>
> **"Artigo 3.º – Intercepção ilícita:** (...), quando praticada intencionalmente, a intercepção não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos, para, de ou dentro de um sistema informático, incluindo as radiações electromagnéticas emitidas por um sistema informático que transporte esses dados informáticos. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático."[338]
>
> **"Artigo 4.º – Dano provocado nos dados:** 1. (...), quando praticados intencionalmente, a danificação[339], o apagamento, a deterioração, a alteração ou supressão não autorizados de dados informáticos..."[340]

[335] Ibidem

[336] Ibidem

[337] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º 2

[338] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º 3

[339] Só há dano a partir do momento em que o dado se torna irrecuperável.

[340] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º 4

"Artigo 5.º – Sabotagem[341] **informática:** (...) quando praticada intencionalmente, a perturbação grave, não autorizada, do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados informáticos."[342]

"Artigo 6.º – Utilização indevida de dispositivos[343]
1. (...), quando praticadas intencional e ilicitamente:
a) A produção, venda, aquisição para efeitos de utilização, importação, distribuição, ou outras formas de disponibilização de:
i) Um dispositivo, incluindo um programa informático, concebido ou adaptado antes de mais para permitir a prática de uma das infracções previstas nos artigos 2.º a 5.º supra;
ii) Uma palavra-passe, um código de acesso ou dados similares que permitem aceder, no todo ou em parte, a um sistema informático, com a intenção de os utilizar para cometer qualquer uma das infracções previstas nos artigos 2.º a 5.º supra; e
b) A posse de um dos elementos referidos na alínea a) (i) ou (ii), desde que utilizados com a intenção de cometer qualquer uma das infracções previstas nos artigos 2.º a 5.º. (...)
2. O presente artigo não pode ser interpretado no sentido de determinar que existe responsabilidade criminal nos casos em que a finalidade da produção, venda, obtenção para utilização, importação, distribuição ou outras formas de disponibilização referidas no n.º 1 do presente artigo não é a prática de uma das infracções previstas nos artigos 2.º a 5.º da presente Convenção, mas antes a realização de testes autorizados ou a protecção de um sistema informático..."[344]

O título 2 sobre as infrações relacionadas com as computadoras específica:

"Artigo 7.º – Falsificação informática: (...), quando praticadas intencional e ilicitamente, a introdução, a alteração, o apagamento ou a supressão de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis..."[345]

"Artigo 8.º - Burla informática: (...), quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de:
a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos;
b) Qualquer interferência no funcionamento de um sistema informático, com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo."[346]

---

[341] No Sabotagem há inoperabilidade ou redução do desempenho. É também o que acontece com o *Worm* e o *Randsomware* não destrói os dados, apenas os encripta.

[342] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º 5

[343] Quando se fala em dispositivo não tem de ser dispositivo físico tangível necessariamente.

[344] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º. 6

[345] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º. 7

[346] CONSELHO DA EUROPA - Convenção sobre o Cibercrime, Art.º. 8

O Título 3 trata sobre Infrações relacionadas com o conteúdo, onde o seu art.º 9 designa as Infrações relativas à pornografia infantil, e o Título 4 ocupa-se das Infrações respeitantes à violações do direito de autor e direitos conexos, especificadas no seu art.º 10.

Sobre o que precede, pode-se determinar que na comunidade internacional, a proteção do direito à intimidade, à privacidade e à identidade tenha sido objeto de preocupação como um direito fundamental do ser humano, pelo que o seu tratamento tem sido regulado, definindo formas de proteção.

4.3.3. Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adotado em Estrasburgo, o dia 28 de Janeiro de 2003.

O protocolo tem por objetivo completar, as disposições da Convenção sobre Cibercriminalidade aprovado em Budapeste em 23 de novembro de 2001, no que respeita à criminalização de atos de natureza racista e xenófoba, cometidos por meio de sistemas informatizados. Para tal efeito, desenvolve diferentes preceitos que buscam garantir um equilíbrio ideal entre a liberdade de expressão e a luta eficaz contra os atos dessa natureza e, assim, harmonizar eficazmente as disposições jurídicas substantivas relacionadas com a luta contra a propaganda racista e xenófoba.

Sob o título "Medidas a adotar a nível nacional", os artigos 3º a 6º contêm uma série de normas de marcado carácter penal, que impõem aos Estados a obrigação de classificar como infração penal, segundo o seu direito interno, as seguintes condutas quando se comentem intencionalmente:

> **Art.º 3** "Difusão de material racista e xenófobo através de sistemas informáticos".- O objectivo é criminalizar a divulgação ou disponibilização ao público de qualquer outra forma material racista e xenófobo através dum sistema informático.
>
> **Art.º4** "Ameaça por motivos racistas e xenófobos".- O Protocolo insta aos Estados Partes a definir o ato de ameaçar por meio de um sistema de computador, como a prática de um crime grave conforme definido na legislação nacional; assim, as pessoas em razão de pertencerem a um grupo caracterizado por a raça, a cor, a descendência ou origem nacional ou étnica, bem

como religião, na medida em que é usada como pretexto para qualquer um desses fatores; ou para um grupo de pessoas que se distingue por qualquer uma dessas características.

Art.º 5 "Insulto por motivos racistas e xenófobos".- O instrumento comentado considera que merece reproche criminoso insultar em público, por meio dum sistema informático, a uma pessoa ou grupos de pessoas.

Art.º 6 "Negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade".- Os comportamentos que o protocolo pretende incluir no direito penal dos Estados Partes com o presente artigo são distribuir ou tornar disponível ao público ou de outra forma através de um sistema de computador, material que negue, minimize grosseiramente, toleram ou justificam atos constitutivos de genocídio ou crimes contra a humanidade, conforme definido no direito internacional e reconhecido como tal por uma decisão final e vinculativa do Tribunal Militar Internacional, ou de qualquer outro tribunal internacional estipulado pelos instrumentos internacionais pertinentes e cuja jurisdição tenha sido reconhecida por essa parte.

4.3.4. Comunicação da Comissão (COM (2005) 184 final: "Programa de Haia: dez prioridades para os próximos cinco anos. Parceria para a renovação europeia no domínio da liberdade, da segurança e da justiça"), de 10 de maio de 2005.

O Programa Plurianual da Haia inclui as 10 prioridades da União destinadas a reforçar o espaço de liberdade, segurança e justiça, considerando concentrar os esforços em 10 prioridades:

i. Fortalecer os direitos fundamentais e a cidadania. A União quer controlar e promover o respeito pelos direitos fundamentais nas políticas europeias. Quer também lutar contra qualquer forma de discriminação e garantir a proteção dos dados pessoais.

ii. Luta contra o terrorismo. Apoiar aos Estados-Membros na sua luta contra o terrorismo, concentrando-se nos aspetos relacionados com a captura de terroristas e o financiamento, a prevenção, a análise de risco, a proteção de infraestruturas sensíveis e a gestão das consequências. As medidas tomadas pela Comissão para alcançar estes objetivos incluem:

melhorar o intercâmbio de informações; Um quadro europeu para a proteção dos dados relacionados; E uma comunicação sobre a proteção de infraestruturas críticas.

iii. Definir uma abordagem equilibrada para a imigração.

iv. Desenvolver uma gestão integrada das fronteiras externas da União. Uma das prioridades de curto prazo é a inserção de identificadores biométricos em documentos de identidade e viagem que aumentem a segurança dos documentos.

v. Ordenar um procedimento comum de asilo.

vi. Maximizar o impacto positivo da imigração.

vii. Encontrar o equilíbrio entre a proteção da privacidade e a segurança ao compartilhar informações. Apoiar um diálogo construtivo entre todas as partes interessadas, a fim de encontrar soluções que equilibrem a disponibilidade de informações e o respeito pelos direitos fundamentais, como a proteção da privacidade e a proteção dos dados.

viii. Desenvolver um conceito estratégico relacionado com o crime organizado. O desenvolvimento de um modelo europeu de informação no domínio penal é uma prioridade.

ix. Garantir um verdadeiro espaço europeu de justiça. A União deve tomar medidas para assegurar uma confiança recíproca entre os Estados-Membros, criando regras processuais mínimas que garantam, por exemplo, os direitos da defesa, e

x. Compartilhar responsabilidades e garantir a solidariedade.[347]

4.3.5. Comunicação da Comissão ao Conselho e ao Parlamento Europeu - "Elaboração de um conceito estratégico para combater a criminalidade organizada" {SEC (2005) 724}, de 02 de junho de 2005.

Recomenda melhorar os conhecimentos da criminalidade organizada e reforçar a recolha e análise de informações, por exemplo, na conservação dos dados para serviços de comunicações eletrónicas na investigação de infrações penais que envolvem o uso da tecnologia da informação. Ainda mais, considera necessário encontrar um equilíbrio entre a aplicação da lei eficaz, a proteção

[347] COMISSÃO DAS COMUNIDADES EUROPEIAS – COM (2005) 184 final, Comunicação da Comissão ao Conselho e ao Parlamento Europeu, de 10 de Maio de 2005: "Programa de Haia: dez prioridades para os próximos cinco anos. Parceria para a renovação europeia no domínio da liberdade, da segurança e da justiça

dos direitos fundamentais e as obrigações dos prestadores de serviços; Também aconselha melhorar o acesso aos dados e as informações e intensificar o intercâmbio entre os corpos de segurança.[348]

4.3.6. Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais, assinada em Lanzarote em 25 de outubro de 2007.

A proteção de menores é o núcleo essencial desta convenção, que se concentra principalmente no respeito pelos direitos dos menores, garantindo o seu bem-estar, tendo em conta as suas opiniões, necessidades e preocupações, e agindo em todos os momentos no melhor interesse da criança, com especial atenção na prevenção de crimes de natureza sexual. Tal é assim, que garante proteção abrangente para crianças contra exploração e abuso sexual, e também lida com processos judiciais contra os supostos autores desses crimes.

A convenção tipifica a conduta que constitui exploração e abuso sexual nos artigos 18º a 23º. Nos casos em que um adulto tem relações sexuais com uma criança, particularmente quando a força ou ameaça é usada, o ato é criminalizado com base no art.º 18 (Abusos sexuais). Também tipifica crimes relacionados com a prostituição infantil (Art.º19), e crimes relacionados com a pornografia infantil (Art.º20) onde inclui a produção, fornecimento, disseminação e posse de pornografia infantil, bem como a utilização de tecnologias informáticas e da comunicação para aceder à pornografia infantil.

Combinada ainda, infrações penais relativas à participação de uma criança em espetáculos pornográficos (Art.º 21), a Corrupção de menores (Art.º 22), e o Abordagem de crianças para fins sexuais (Art.º 23), sendo a primeira vez, que o assédio infantil (*'grooming'*)[349] foi incluído num tratado internacional, refletindo a crescente preocupação com o fenômeno do abuso em menores citados com adultos com quem entraram em contato anteriormente no ciberespaço, especialmente em *chats* na Internet ou em páginas de jogos *on-line*.

---

[348] COMISSÃO DAS COMUNIDADES EUROPEIAS – COM (2005) 232 final, Comunicação da Comissão ao Conselho e ao Parlamento Europeu - "Elaboração de um conceito estratégico para combater a criminalidade organizada" {SEC (2005) 724}

[349] O termo "*grooming*" significa fazer propostas para um menor, a fim de abusar dele e obter uma gratificação sexual.

A cumplicidade e tentativa e tratada no art.º 24, e com o fim de prevenir e julgar a exploração e abuso sexual de crianças, a Convenção estipula que os dados relativos à identidade e ao perfil genético das pessoas condenadas podem ser registrados, armazenados e, se necessário, enviados para autoridades competentes de outros Estados (Registo e armazenamento de dados nacionais sobre pessoas condenadas por infrações penais de natureza sexual - art.º 37)

4.3.7. A Decisão-quadro 2008/913/JAI relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia adotada o dia 28 de Novembro de 2008.

O Conselho da União Europeia aprovou a Decisão-quadro 2008/913/JAI relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia adotada o dia 28 de Novembro de 2008, na qual compromete aos Estados-Membros tomar as medidas necessárias para assegurar que sejam puníveis como infrações penais os atos de incitação pública à violência ou ao ódio dirigido contra uma pessoa ou grupo de pessoas, com base na cor da pele, raça, ascendência, crença religiosa ou origem étnica ou nacional, assim como também seja penado a difusão por qualquer meio, de imagens texto ou outro material com conteúdo racista ou xenófobo, negação ou banalização grosseira pública de crimes de genocídio ou contra a humanidade e crimes de guerra, quando tais comportamentos puderem incitar à violência ou ódio contra essa pessoa ou grupo cometidos no território da UE, incluindo através dum sistema de informação.[350]

4.3.8. Tratado sobre o Funcionamento da União Europeia - TFUE, de 2009.[351]

No âmbito dos delitos informáticos estipula-se:

> **Art. 83** n.º1 "O Parlamento Europeu e o Conselho, por meio de directivas adoptadas de acordo com o processo legislativo ordinário, podem estabelecer regras mínimas relativas à definição das infracções penais e das sanções em domínios de criminalidade particularmente grave com dimensão transfronteiriça que resulte da natureza ou das incidências dessas infracções, ou ainda da especial necessidade de as combater, assente em bases comuns.

[350] CONSELHO DA UNIÃO EUROPEIA - DECISÃO-QUADRO 2008/913/JAI relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia

[351] Citado no Capitulo I, subcapitulo 1.2.18 do presente trabalho.

São os seguintes os domínios de criminalidade em causa: terrorismo, tráfico de seres humanos e exploração sexual de mulheres e crianças, tráfico de droga e de armas branqueamento de capitais, corrupção, contrafação de meios de pagamento, criminalidade informática e criminalidade organizada..."[352]

Art.º 325 n.º1. "A União e os Estados-Membros combaterão as fraudes e quaisquer outras actividades ilegais lesivas dos interesses financeiros da União, por meio de medidas a tomar ao abrigo do presente artigo, que tenham um efeito dissuasor e proporcionem uma protecção efectiva nos Estados- -Membros, bem como nas instituições, órgãos e organismos da União."[353]

4.3.9 Programa de Estocolmo do Conselho Europeu "Uma Europa Aberta e Segura que Sirva e Proteja os Cidadãos" (2010/C 115/01)

O Programa de Estocolmo regula as prioridades da UE para fortalecer ainda mais o espaço de liberdade, segurança e justiça para o período 2010-2014, e tem por objetivo abordar os desafios do futuro com medidas centradas nos interesses e necessidades dos cidadãos considerando entre as suas prioridades que:

i. A cidadania europeia deve conferir aos nacionais os direitos e liberdades fundamentais consagrados na Carta dos Direitos Fundamentais da UE e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Os cidadãos da UE devem poder exercer estes direitos dentro e fora da UE, sabendo que a sua privacidade é respeitada, especialmente no que diz respeito à proteção de dados pessoais.

ii. Recomenda o desenvolvimento de uma estratégia de segurança interna para a UE destinada a melhorar a proteção dos cidadãos e a luta contra o crime organizado e o terrorismo. Centrar-se-á na luta contra a criminalidade transfronteiriça, tais como: tráfico de seres humanos; abuso sexual, exploração sexual de menores, pornografia infantil; e crime cibernético;

iii. Reforçar os controlos fronteiriços para impedir a imigração ilegal e a criminalidade transfronteiriça.[354]

[352] TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA. Art.º 83, núm. 1

[353] TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA. Art.º 325, núm. 1

[354] CONSELHO EUROPEU (2010 /C 115/01), - Programa de Estocolmo "Uma Europa aberta e segura que sirva e proteja os cidadãos ".

4.3.10. Diretiva 2011/92/UE do parlamento Europeu e do Conselho, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho, de 13 de Dezembro de 2011.

Com a presente diretiva a UE adotou a legislação destinada a combater as ofensas sexuais contra menores para o qual considera aspetos como: sanções e prevenção, incluindo assistência às vítimas, e estão previstas disposições específicas para a pornografia infantil através da Internet e do turismo sexual.

Neste contexto, os Estados-Membros farão o que for necessário para garantir que os sítios Web que contenham pornografia infantil alojados no seu território sejam removidos e realizarão esforços para também remover os sítios *Web* hospedados noutros países. Poderão também, sem prejuízo de certos requisitos de transparência e informação para os usuários da Internet, bloquear o acesso a tais *sites* no seu território. A diretiva define infrações penais de acordo com as seguintes categorias:

i. Os Abusos sexuais, tais como a realização de atos de natureza sexual com um menor que não tenha atingido a maioridade sexual ou que o obrigue a participar de tais atos com um terceiro;

ii. A exploração sexual, consistindo, por exemplo, em coagir um menor a prostituir-se ou participar em espetáculos pornográficos;

iii. A pornografia infantil: possuir, acessar, distribuir, fornecer e produzir pornografia infantil;

iv. O aliciamento de crianças para fins sexuais através da Internet: propor através da Internet um encontro com um menor para cometer abuso sexual ou incitar-lhe pelos mesmos meios, que forneça material pornográfico que o represente.[355]

4.3.11. Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, do Parlamento Europeu e do Conselho, de 2013

[355] PARLAMENTO EUROPEU E DO CONSELHO - DIRETIVA 2011/92/UE, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho.

A Diretiva **2013/40/UE** do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, substitui a Decisão-Quadro 2005/222/JAI (DM) do Conselho da Europa, numa ação para unificar as legislações nacionais na luta contra a pirataria, a propagação de vírus e ataques de negação de serviço.

Do mesmo modo, a Diretiva reflita a preocupação pelos crimes que são importantes pela sua evolução, crescimento e desenvolvimento contínuo, tais como:

i. Os ataques ligados ao crime organizado. Ataques massivos ou em larga escala contra qualquer objetivo.
ii. Ataques às infraestruturas críticas com impacto global.
iii. Roubo, bloqueio ou usurpação da identidade.
iv. Intrusão ilegal nos sistemas informáticos.
v. Intercetação, obtenção do conteúdo da informação.
vi. A responsabilidade das pessoas jurídicas quando elas propiciam e se beneficiam do acesso ilegal a terceiros.
vii. Os meios e programas utilizados para a comissão criminal, a sua criação e a sua comercialização.

As normas incluem a proibição do uso dos chamados "*botnets*": programas prejudiciais projetados para assumir o controlo remoto das redes de computadores. Além disso, insta os países da UE a utilizar os mesmos pontos de contacto que o Conselho da Europa e o G8[356] para reagirem prontamente às ameaças que envolvem tecnologia avançada.[357]

4.3.12. DIRETIVA (UE) 2016/681 do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, de 2016.[358]

[356] O Grupo dos Oito ou G8 é um grupo de países industrializados que têm grande importância política, econômica e militar no mundo. É composto por Alemanha, Canadá, Estados Unidos, França, Itália, Japão, Reino Unido e Rússia.

[357] PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2013/40/EU - Relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho

[358] A Diretiva 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, citada no subcapítulo 1.2.19. deste trabalho, completa o novo regulamento europeu sobre proteção de dados definido pelo Regulamento 2016/679 (o Regulamento Geral de Dados de Proteção - citado no subcapítulo 1.2.20.) e desta Diretiva 2016/681, definindo as garantias e os princípios que devem reger o tratamento automatizado e / ou manuais, de dados pessoais relativos a pessoas singulares, identificados ou identificáveis, sempre que tal seja feito para fins de "prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais," incluindo proteção e prevenção contra ameaças contra segurança pública.

A Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, tem por intenção regular a transferência de dados de Registo de Identificação de Passageiros Aéreos (*Passenger Name Record* – PNR), tais como: nome, morada, número de passaporte, número de cartão de crédito, telefone, bagagem, número do assento, itinerário, preferências de refeição, dados dos voos comerciais internacionais de entrada ou saída do espaço da União Europeia, das companhias aéreas, etc. Também regula o processamento desses dados pelas autoridades competentes dos países da EU, com o objeto de prevenir, detetar, investigar e reprimir as infrações terroristas ou da criminalidade grave.[359]

4.4. LEGISLACÃO COMPARADA DOS CIBERCRIMES RELACIONADOS COM OS DADOS PESSOAIS DE PAGAMENTO

O aumento da tecnologia disponível, tanto para o infrator quanto para as vítimas, combinado com o escasso conhecimento sobre como se proteger dos possíveis crimes que se podem padecer por meio das novas tecnologias, fornece aos infratores as facilidades de possíveis ataques, sem respeitar as barreiras geográficas ou jurisdicionais. A partir daí, surge a necessidade dos Estados de combatir com medidas jurídico-penais alguns casos de abusos relacionados à tecnologia da informação, visando proteger a privacidade, os dados pessoais e a correspondência, direitos que, como resultado do *boom* tecnológico nas telecomunicações, foram vulnerados.

Nesse quadro, as seguintes legislações estrangeiras são brevemente analisadas, a fim de fornecer uma visão global da maneira como o legislador está lutando contra o cibercrime:

4.4.1. Argentina

Somente após à promulgação da Lei de Proteção de Dados Pessoais, conhecida como habeas data (Lei n.º 25.326 de 2000), que incluiu os artigos do Código Penal 117 bis e 157 bis se forneceu

[359] PARLAMENTO EUROPEU E DO CONSELHO - DIRETIVA (UE) 2016/681 relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

proteção penal às informações pessoais entendidas como intangíveis. Existem outras leis especiais que também dão tutela a certos bens intangíveis, que a título de exemplo mencionamos:[360]

> A Lei 24.766, chamada de Confidencialidade da Informação, que a protege apenas quando um segredo comercial é importante;
> A Lei 24.769, de Crimes Fiscais, que prevê proteção penal às informações do Tesouro Nacional, a fim de evitar a sua supressão ou alteração.
> A Lei 11.723 estendeu a proteção penal ao *software*.

Em junho de 2008, a Lei 26.388 conhecida como "Lei de Crimes de Informática" fez uma série de modificações no Código Penal argentino, substituindo e incorporando figuras típicas em vários artigos. Assim, os seguintes artigos foram modificados ou adicionados:[361]

> Art.º 128.- Pornografia infantil pela Internet ou por outros meios eletrónicos;
> Art.º 153 núm. 1.- Violação, apreensão e desvio de comunicação eletrónica;
> Art.º 153 núm. 2.- Intercetação ou captura de comunicações eletrónicas ou telecomunicações;
> Art.º 153 bis.- Acesso a um sistema informático ou dados;
> Art.º 155.- Publicação duma comunicação eletrónica;
> Art.º 157 bis, núm. 1.- Acesso a um banco de dados pessoais;
> Art.º 157 bis inciso 2.- Divulgação de informação registada num banco de dados pessoais;
> Art.º 157 bis inciso 2.- Inserção de dados falsos em arquivo de dados pessoais (previamente regulado no artigo 117 bis, parágrafo 1º, incorporado pela Lei Habeas Data);
> Art.º 173 inciso 16.- Fraude informática;
> Art.º 183 e 184, incisos 5 e 6.- Dano ou sabotagem informático.

---

[360] GALEON.COM HISPAVISTA - Delitos informáticos en el derecho comparado. [Em linha]. Disponível na internet: http://derela.galeon.com/enlaces2303544.html

[361] ABOGADOS PORTALEY - La incorporación de los delitos informáticos al Código Penal argentino. [Em linha]. 2008 Disponível na internet: HTTPS://DELITOSINFORMATICOS.COM/06/2008/NOTICIAS/LA-INCORPORACION-DE-LOS-DELITOS-INFORMATICOS-AL-CODIGO-PENAL-ARGENTINO

4.4.2. Alemanha

Na República Federal da Alemanha, para lidar com crimes relacionados à informática, em 15 de maio de 1986, foi adotada a Segunda Lei sobre o Combate ao Crime Económico. Esta lei reforma o Código Penal alemão (*Strafgesetzbuch – StGB)* no seu artigo 148º de 22 de dezembro de 1987, para contemplar os seguintes crimes:[362]

§ 202a. Espionagem de dados. Assim, incrimina o ato de acessar dolosamente aos dados para os quais não se está autorizado, entendido como tais: os armazenados, transmitidos eletronicamente, magneticamente ou imediatamente acessíveis.

§ 263a. Burla Informática. De acordo com a redação do preceito, o prejuízo patrimonial cometido consiste em influenciar o resultado da elaboração de dados por meio da manipulação da informática, ou pelo uso de dados incorretos ou incompletos, ou por uso não autorizado ou intrusão ilegítima num sistema ou rede eletrónica que fornece acesso a dados reais.

§ 266b. Uso abusivo de cheques ou cartões de crédito.

§ 269. A falsificação de provas, juntamente com modificações complementares do resto das falsidades documentárias, tais como o engano no tráfego legal através da elaboração de dados, falsidade ideológica, ou o uso de documentos falsos (**§** 270, 271 e 273).

§ 303a. Alteração de dados (303a), é ilícito cancelar, desativar ou alterar dados e até mesmo a tentativa é punível.

§ 303b. Sabotagem informático (303b). Destruição de dados de significado especial por meio de estrago, inutilização, eliminação ou alteração dum sistema de dados.

4.4.3. Áustria

Com a Lei de reforma de 22 de dezembro de 1987 (Lei sobre crimes informáticos), o Código Penal de Áustria contempla os seguintes crimes:[363]

[362] DE LA CUESTA ARZAMENDI, José L. (Dir.) [et al.] – Derecho Penal Informático, p 149

[363] CONSELHO NACIONAL DA ÁUSTRIA - Penal Code (Strafgesetzbuch - StGB) [Em linha]. [Austria], 1 January 1975, [Consult. 30 Julho 2018]

O artigo art.º 118 trata sobre o acesso ilícito a um sistema de computador. O Artigo 126a faz referência à destruição de dados, que é processada num sistema automatizado, seja por eliminação, modificação ou supressão. O Artigo 126b versa da interrupção da operação dum sistema informático, afetando a sua funcionalidade, impedindo a entrada ou transmissão de dados.

A intercetação abusiva dos dados do art.º 119a indica que a pessoa que intercepta de maneira não autorizada, por meio dum sistema informático, certos dados, buscando uma vantagem pecuniária ou causando danos a um dispositivo que estava conectado ao sistema informático utilizando os campos de radiação eletromagnética, serão punidos.

O artigo 148ª sobre a utilização fraudulenta do tratamento de dados decreta que aqueles que, com a intenção de enriquecerem-se ou a terceiros de forma ilegal, danifiquem o sistema de processamento automatizado de dados através da conceção dos programas ou através da introdução, modificação ou supressão de dados, será punido.

4.4.4. Brasil

A Lei n.º 11.829 de 25 de novembro de 2008 regulamenta o Estatuto da Criança e do Adolescente, para melhorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e posse de tais materiais e outros comportamentos relacionados à pedofilia na Internet.[364]

Por sua parte, a Lei n.º 12.735 de 30 de novembro de 2012, altera o Código Penal, e o Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrónico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares.[365]

A Lei n.º 12.737 de 30 de novembro de 2012 prevê a criminalização de crimes informáticos e outras medidas. Em seu regulamento incorpora emendas aos artigos 154-A e 154-B sobre invasão de dispositivo informático; O artigo 266º que trata sobre Crime de Interrupção de serviço telegráfico,

[364] CONGRESSO NACIONAL DE BRASIL - LEI Nº 11.829, DE 25 DE NOVEMBRO DE 2008, (Lei Azeredo).
[365] CONGRESSO NACIONAL DE BRASIL - LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012,

telefônico, informático, telemático ou de informação de utilidade pública, e o art.º 298 de falsificação de documento particular do Código Penal que visam proteger a segurança dos sistemas informáticos. Assim temos, que a produção e distribuição de aparelhos que permitem a invasão de *smartphones* ou *tablets* também serão punidos com penas de prisão, assim como, a obtenção ilegal de dados bancários por meios eletrónicos também será punida, com penas que variam de um a cinco anos de prisão.[366]

Por outro lado, a Lei nº 12.965 de 23 de abril de 2014, que trata sobre o Marco Civil da Internet,[367] indica sanções pelo incumprimento da Proteção aos *Registros, aos Dados Pessoais e às Comunicações Privadas* prescritos nos artigos 10º e 11º, aplicadas de forma isolada ou cumulativa, nomeadamente: **i.** Advertência, com indicação de prazo para adoção de medidas corretivas; **ii.** Multa de até 10% (dez por cento) do faturamento do grupo económico no Brasil, **iii.** Suspensão temporária das atividades, e **iv.** Proibição de exercício das atividades.[368]

4.4.5. Colômbia

A Lei 1.273 de 2009, que altera o Código Penal, criando um novo bem jurídico conhecido como *a Proteção da Informação e dos Dados*, com o qual se preserva integralmente os sistemas que utilizam a tecnologia da informação e a comunicação.

Assim, o Capítulo I, que trata sobre os ataques contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos, regula:[369]

Art.º 269A: Acesso abusivo a um sistema informático.
Art.º 269B: Obstrução ilegítima de sistema informático ou rede de telecomunicações.
Art.º 269C: Intercetação de dados informáticos.
Art.º 269D: Dano informático.
Art.º 269E: Utilização de *software* malicioso.
Art.º 269F: Violação de dados pessoais.
Art.º 269G: Falsificação de *websites* para captura de dados pessoais.
Art.º 269H: Circunstâncias do agravamento punitivo.

[366] CONGRESSO NACIONAL DE BRASIL - LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012, (Lei Carolina Dieckmann; Lei de Crimes Cibernéticos)
[367] Lei citada no subcapítulo 1.3 do presente trabalho e que trata da Legislação Comparada.
[368] CONGRESSO NACIONAL DE BRASIL- MARCO CIVIL DA INTERNET. [Em linha]. LEI Nº 12.965, DE 23 DE ABRIL DE 2014, art.º 12
[369] CONGRESO DE COLOMBIA – LEY 1273 DE 2009.

E o Capítulo II que se refere aos ataques informáticos e outras infrações institui:[370]

Art.º 269I: Furto de meios informáticos e similares
Art.º 269J: Transferência não consentida de ativos.

Além disso é incorporado o artigo 58º que considera como um agravante geral se realizar qualquer um dos factos puníveis, utilizando meios informáticos, eletrónicos ou telemáticos.

4.4.6. Costa Rica

A Lei n.º 9048 de 10 de julho de 2012, modifica diversos artigos da seção VIII ("delitos informáticos" e conexos) do Título VII do Código Penal, ao reformar os artigos 167º (corrupção de uma pessoa menor ou incapaz), 196º (Violação de correspondência ou comunicações), 196ºbis (Violação de dados pessoais), 214º (extorsão), 217ºbis (burla informática), 229ºbis (danos no computador) e 288º (Espionagem) da Lei nº 4.573. Por outro lado, acrescenta a subseção 6) ao artigo 229º (Dano agravado) e um artigo 229ºter (Sabotagem informático)[371].

Finalmente modifica de forma abrangente a seção VIII do Título VII do Código Penal ao acrescentar uma quantidade significativa de crimes informáticos, intitulada Delitos informáticos e conexos, onde regula:[372]

Artigo 230º.- Suplantação de identidade
Artigo 231º.- Espionagem informático
Artigo 232º.- Instalação ou propagação de programas informáticos maliciosos
Artigo 233º.- Suplantação de páginas eletrónicas
Artigo 234º.- Facilitação do crime informático
Artigo 235º.- Tráfico de drogas e crime organizado
Artigo 236º.- Divulgação de informação falsa

[370] Ibidem.
[371] ASSEMBLEIA LEGISLATIVA DA REPÚBLICA DA COSTA RICA – Lei N.º 9048.
[372] Ibidem.

4.4.7. Equador

Os Crimes informáticos foram introduzidos na legislação equatoriana através das emendas ao Código Penal, primeiramente com o estabelecido na Lei de Comércio Eletrónico, Assinaturas Eletrónicas e Mensagens de Dados, Lei n.º 2002-67 publicada no Diário Oficial Nº 557-S, 17-IV -2002, que tem como objeto, regular os mensagens de dados, a assinatura eletrónica, os serviços de certificação, a contratação eletrónica e telemática, a prestação de serviços eletrónicos através de redes de informação incluindo o comércio eletrónico, e a proteção dos utilizadores desses sistemas.[373]

O art.º 40 da LCElec estabelece infrações administrativas que são classificadas como leves e graves.[374] Posteriormente, com as reformas do Código Penal realizadas em 2014, são tipificados os seguintes atos criminosos relacionados à tecnologia da informação:[375]

> Art. 103.- Pornografia com o uso de crianças ou adolescentes.- (A pessoa que fotografar, filmar, gravar, produzir, transmitir ou editar materiais visuais, audiovisuais, informáticos, eletrónicos ou qualquer outro suporte ou formato contendo o representação visual de nus ou semi-nus reais ou simulados de crianças ou adolescentes em uma atitude sexual, são sancionados)
> Art. 173.- Contacto com propósito sexual com menores de dezoito anos por meio eletrónico.-
> Art. 174.- Oferta de serviços sexuais com menores de dezoito anos por meios eletrónicos.-
> Art. 178.- Violação de privacidade.-
> Art. 186.- Burla.-
> Art. 190.- Apropriação fraudulenta por meios eletrónicos.-
> Art. 191.- Reprogramação ou modificação das informações do telemóvel.- (A pessoa que reprograma ou modifica as informações de identificação do equipamento terminal móvel)
> Art. 192.- Intercâmbio, comercialização ou compra de informações do telemóvel.- (A pessoa que troca, comercializa ou compra bancos de dados é sancionada)
> Art. 211.- Supressão, alteração ou suposição da identidade e estado civil.-
> Art. 229.- Revelação ilegal de bases de dados.-
> Art. 230.- Intercetação ilegal de dados.-
> Art. 231.- Transferência eletrónica de ativos

---

[373] CONGRESO NACIONAL DE ECUADOR - Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Ley No. 67, art.° 1

[374] CONGRESO NACIONAL DE ECUADOR - Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Ley No. 67, art.° 40
Infrações leves:
i) O atraso no cumprimento de uma instrução ou na entrega de informações exigidas pelo órgão de controlo; e
ii) Qualquer outra violação das obrigações impostas por esta Lei e seus regulamentos às entidades certificadoras credenciadas.
Infrações graves:
1. Uso indevido do certificado de assinatura eletrónica por omissões atribuíveis à entidade certificadora de informações credenciada;
2. A falta de notificação ao organismo de controlo da existência de atividades presuntivamente ilícitas levadas a cabo pelo destinatário do serviço;
3. Não cumprir a petição do organismo de inspeção de suspender a prestação de serviços de certificação para impedir a prática de uma infração;
4. Incumprimento das resoluções emanadas pelas Autoridades de Autorização, Registo, Regulação e Controlo; e
5. Não permitir ou obstruir a realização de auditorias técnicas pelo órgão de controlo.

[375] ASAMBLEA NACIONAL DE LA REPÚBLICA DEL ECUADOR - CODIGO ORGANICO INTEGRAL PENAL, COIP,

Art. 232.- Ataque à integridade dos sistemas da informática.-
Art. 233.- Crimes contra informação pública legalmente reservada.-
Art. 234.- Acesso não consentido a um sistema informático, telemático ou de telecomunicações.
Art. 476.- Intercetação de comunicações ou dados informáticos.-

4.4.8. Espanha

Ao longo do Código Penal espanhol (Lei O. 10/1995 de 23 de novembro), e especialmente após a reforma de 2015[376], aparecem amostras de crimes de informática, quando se refere aos meios utilizados para a comissão. Assim, por exemplo, seguindo a ordem sistemática do código penal, crimes desse tipo são:[377]

i. Abusos e agressões sexuais em crianças menores de dezasseis anos de idade (art.º 183 ter)[378]
ii. Crimes contra a intimidade e o direito da própria imagem (arts.º 197 a 201)
iii. Crimes contra o patrimônio e contra a ordem socioeconômica:
a) Dos furtos (arts.º 234 a 236)
b) Dos roubos (arts.º 237 a 242)
c) Das defraudações:
- Das burlas (arts.º 248 a 251);
- Da apropriação indevida (arts.º 252 a 254)
d) Dos danos (arts.º 263 a 267)
e) Crimes contra a propriedade intelectual e industrial, ao mercado e aos consumidores:
- Dos crimes contra a propriedade intelectual (arts.º 270 a 272);
- Dos crimes contra a propriedade industrial (arts.º 273 a 277);
- Dos crimes contra o mercado e aos consumidores (arts.º 278 a 286)
f) Das falsidades documentais (arts.º 390 a 399)
g) Outras referências indiretas:
- Das defraudações de fluido elétrico e análogo (arts.º 255, 256);
- Os crimes corporativos (art.º 290);
- Os estragos (art.º 346);
- Da infidelidade na custódia de documentos e violação de segredos (arts.º 413 a 417);
- Das desordens públicas (art.º 560)

[376] A última atualização publicada corresponde a 28 de abril de 2015. Nela se revoga o Livro III, são adicionados, apagados e modificados certos preceitos e referências indicados e o caráter da Lei ordinária é declarado ao artigo 128 pela Lei Orgânica 1/2015, de 30 de março, que modifica a Lei Orgânica 10/1995, de 23 de novembro, do Código Penal.

[377] DAVARA RODRÍGUEZ., Miguel Á. – Manual de Derecho informático.P. 407

[378] Por exemplo: Cyberbullying, ou cyber acosso, refere-se, em termos gerais, ao assédio. O grooming (o aliciamento de crianças)

4.4.9. Estados Unidos da América

No entendimento de PAEZ e ACURIO[379], no Estados Unidos da Norte América existe legislação abundante e variada em relação à prevenção e punição dos crimes cibernéticos, sendo capaz de mencionar a Lei Federal de Proteção de Sistemas (1985), a Lei de Fraude e Abuso de Computador (1986), Lei de Fraude e atividade relacionada em conexão com computadores (1994, 18 USC Sec. 1030)[380] e a Lei da Privacidade *(The Privacy Act)* de 1992.

A Lei Federal sobre de Proteção de Sistemas de 1985 foi a base para a Flórida, Michigan, Colorado, Rhode Island e Arizona, sejam constituídos nos primeiros estados com legislação específica, antecipando um ano para a promulgação da Lei de Fraude e Abuso do Computador 1986 (*Computer Fraud and Abuse Act)*. Este último refere-se a crimes de abuso ou fraude contra casas financeiras, registros médicos, computadores de instituições financeiras ou envolvidos em crimes interestaduais. Também especifica penalidades para o tráfego de senhas com intenção de cometer fraudes e declara ilegal o uso de senhas próprias ou de terceiros de forma inapropriada.[381]

Em 1994, foi adotada a Lei de Fraude e atividade relacionada em conexão com computadores (18 USC Sec.1030), que alterou a Lei de Fraude e Abuso do Computador de 1986, a fim de eliminar argumentos híper-técnicos sobre o que é e não é um vírus, um verme ou um cavalo de Tróia.

A nova Lei de 1994 proíbe a transmissão de um programa, informações, códigos ou comandos que causem danos ao *hardware*, ao *software*, às redes, ou às informações (18 U.S.C.: Sec. 1030), e define dois níveis para o tratamento daqueles que criam vírus definindo sanções mais severas para aqueles que intencionalmente causam danos pela transmissão de um vírus e sanções menos severas para aqueles que o transmitem de forma imprudente. Esta lei não define vírus, mas descreve o ato de criá-lo para dar espaço no futuro à nova era de ataques tecnológicos nos sistemas informáticos, seja qual for a forma que eles tomem.[382]

---

[379] PAEZ, Juan; ACURIO, Santiago, DERECHO Y NUEVAS TECNOLOGÍAS. 1ª. Equador, p. 236

[380] 1994 Código dos EUA, Título 18 - Crimes e Procedimentos Penais, Parte I - Crimes, Capítulo 47 - Fraude e Declarações Falsas, Sec. 1030 - Fraude e atividade relacionada em conexão com computadores

[381] PAEZ, Juan; ACURIO, Santiago, Op. Cit. p. 237

[382] PAEZ, Juan; ACURIO, Santiago, Op. Cit. p. 238

No estado da Califórnia, em 1992, foi adotada a Lei de Privacidade, na qual são contemplados os crimes informáticos, mas em grau menor que os crimes relacionados à intimidade, que constituem o objetivo principal desta Lei. As emendas feitas à Seção 502 do Código Penal relacionado aos crimes de informática estende aos sujeitos suscetíveis de serem afetados por esses crimes, especificando sanções pecuniárias para cada pessoa afetada.[383]

4.4.10. França

Na França, com a Lei n.º 88/19 sobre fraude informática de 5 de janeiro de 1988 (*Lei Godfrain*), optou-se pela modalidade de criminalização do acesso ilegítimo, a alteração (introdução ou destruição) de dados e, a falsificação dos mesmos, mas não uma forma de "furto digital". No entanto, ao tipificar o acesso fraudulento aos sistemas informáticos, eles estão prevendo qualquer roubo de produtos digitais.[384]

Assim mesmo, antes da Convenção de 2001 sobre Cibercrime, já tinham artigos no Código Penal referentes à espionagem industrial e comercial, sancionando para tal efeito: A alteração de dados (art.º 321-1); A intrusão num sistema informático para conhecer dados confidenciais (art.º 323-1), e os ataques a um sistema informático (art.º 323-2), todos cometidos sem autorização, e usando como meio uma rede eletrónica de dados.[385]

Após a ratificação da Convenção, duas grandes categorias de infrações foram criadas. Uma diretamente relacionada às TIC's, onde estão localizados os ataques ao sistema de processamento automático de dados, a difusão de programas que permitem atacar o sistema de processamento automático de dados, as infrações à lei informática e à liberdade sobre a proteção de dados pessoais, assim como infrações relativas aos cheques, como por exemplo fazer cheques falsos, e também inclui infrações sobre criptologia. [386] A outra categoria está relacionada com a comissão de atos ilícitos prejudiciais aos bens jurídicos tradicionalmente protegidos, através da rede de dados, como por exemplo,

[383] PAEZ, Juan; ACURIO, Santiago, Op. Cit. p. 238

[384] PALAZZI, Pablo - Delitos Informáticos. 1ra. Buenos Aires. Pag. 96

[385] DE LA CUESTA ARZAMENDI, José L. (Dir.) [et al.] – Derecho Penal Informático, p 147

[386] DE LA CUESTA ARZAMENDI, José L. (Dir.) [et al.] – Derecho Penal Informático, p 148

a disseminação de conteúdo ilegal, a pornografia infantil e os comportamentos de ódio, racismo e antissemitismo, e finalmente as burlas informáticas.[387]

4.4.11. Holanda

A lei de Cibercrime de 1 de Março de 1993 na Holanda estabelece artigos específicos para as técnicas de *hacking*[388] e *Phreacking*[389]. Declara que o simples facto de entrar em um computador que não tem acesso legal é considerado um crime; O mesmo que, publicar a informação obtida é ilegal se eles são dados que devem permanecer em segredo.[390]

Da mesma forma, o dano à informação ou a um sistema de comunicação pode ser punido com prisão, assim como, alterar, adicionar ou excluir dados, se isso for feito remotamente sem autorização.

Os vírus são considerados especialmente na lei se forem distribuídos com a intenção de causar problemas. Enquanto à prática do *Phreacking*, o agente pode ser penado até com três (3) anos de prisão; Também, e punida com pena de prisão a pessoa que venda os elementos que permitam fazer essa prática.

A norma contempla que o receber dados de satélite é legal, desde que não seja necessário nenhum esforço especial para obtê-los e, finalmente, observa que a falsificação de cartões de crédito ou débito para obter benefícios nas transações eletrónicas como se fossem originais, é punido com privação de liberdade.[391]

A Convenção sobre Cibercriminalidade de 2001 entrou em vigor para os Países Baixos em 1 de março de 2007. Em simultâneo com esta lei foi adotado pelo Senado em 30 de Maio de 2006 a Lei Cibercrime II (26.671) para implementar as disposições da Convenção e ajustar a legislação existente

---

[387] Ibídem.

[388] É o conjunto de técnicas pelas quais uma pessoa sem autorização acessa um sistema informático, violando as medidas de segurança estabelecidas originalmente.

[389] Utilizar o serviço de telefonia por meio de um truque técnico com o objetivo de não pagá-lo

[390] SEGU.INFO - Legislación y Delitos Informáticos – Holanda. [Em linha]. Argentina [Consult. 16 junho 2018]. Disponível na internet: https://www.segu-info.com.ar/delitos/holanda.htm.

[391] Ibídem

com penalidades mais altas para crimes cibernéticos, estendendo a criminalização de várias ofensas e apertando os poderes do judiciário e da polícia.[392]

4.4.12. Venezuela

Tem uma Lei especial sobre o Cibercrime de 30 de outubro de 2001, publicada no Diário Oficial n.º 37.313 (2001), que visa proteger os sistemas que usam tecnologias de informação, assim como prevenir e punir os crimes cometidos contra ou pelo uso de tais tecnologias. A lei contempla os seguintes crimes:[393]

i. Crimes contra sistemas que usam tecnologia da informação:
a) Acesso indevido a um sistema;
b) A sabotagem ou dano aos sistemas, incluindo qualquer ato que altere o seu funcionamento;
c) Posse de equipamentos ou prestação de serviços para atividades de sabotagem;
d) Espionagem informático, que inclui a obtenção, disseminação e divulgação de informações, factos ou conceitos contidos num sistema; e
e) A falsificação de documentos através do uso de tecnologias de informação ou a criação, modificação ou alteração de dados em um documento.

ii. Crimes contra a propriedade: Esta classe inclui:
a) O roubo, através do acesso, interceção, interferência, manipulação ou utilização de um sistema que utilize tecnologias da informação;
b) Fraude causada pelo uso indevido das tecnologias de informação;
c) A obtenção indevida dos bens ou serviços através da utilização de cartões inteligentes (cartões de crédito, débito ou de identificação);
d) A manipulação fraudulenta de cartões inteligentes, ou a criação, duplicação ou incorporação indevida de dados em registros, listas de consumo ou similares;
e) A apropriação indébita de cartões inteligentes;
f) Provisão inadequada dos bens ou serviços usando um cartão inteligente; e
g) Posse de equipamentos para falsificações.

iii. Crimes contra a privacidade de pessoas e comunicações são:
a) Violação da privacidade dos dados ou informações pessoais
b) Violação da privacidade das comunicações; e
c) A revelação indevida de dados ou informações obtidas pelos meios descritos nas alíneas a) ou b) acima.

---

[392] EERSTE KAMER - Goedkeuring Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerke. [Em linha]. [Consult. 28 feb 2018]. Disponível na internet: https://www.eerstekamer.nl/wetsvoorstel/30036_goedkeuring_verdrag_inzake

[393] ASAMBLEA NACIONAL DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA - Ley Especial Contra los Delitos Informáticos, 2001

iv. Crimes contra crianças e adolescentes são:

a) A divulgação ou exibição de material pornográfico sem aviso prévio para restringir o acesso a menores; e

b) A exibição pornográfica de crianças ou adolescentes.

v. Crimes contra a ordem económica:

a) A apropriação indevida de propriedade intelectual através da reprodução, divulgação, modificação ou cópia de *software*, e

b) A oferta enganosa de bens ou serviços através do uso de tecnologias da informação.

Na legislação comparada observa-se a inclusão de diferentes crimes em harmonia com à realidade nacional de cada país, tratando a existência de tipos penais tradicionais, tais como: sabotagem, fraude, espionagem, falsificação, dano ou destruição, abuso de propriedade intelectual e roubo, mas feitos no ambiente informático ou no campo da tecnologia da informação, dando origem a crimes como: Acesso não autorizado para um sistema de processamento de dados; Danos ou destruição de dados; Alteração, modificação ou eliminação de dados; Uso ou divulgação, revelação, publicação ou difusão de dados; Impedir ou falsificar o funcionamento de um sistema; e o Espionagem e sabotagem de dados. Da mesma forma, novas figuras criminosas são observadas, tais como: vírus informáticos, técnicas de *hacking* e violação ou intercetação de comunicações.

Na Venezuela destaca-se como um dos países que têm crimes mais qualificados, seguido por Espanha e Colômbia, onde são observados vários tipos de delitos que vão desde delitos contra os sistemas que usam tecnologias computacionais, contra a propriedade, contra a privacidade dos indivíduos e das comunicações e contra a ordem econômica, e até o acesso abusivo, o uso de *software* malicioso, o furto de meios informáticos, etc.

4.5. OS CRIMES INFORMÁTICOS COM UM ENFOQUE NOS DADOS PESSOAIS DE PAGAMENTO EM PORTUGAL.

Em Portugal, a Lei n.º 109/2009 identificada como Lei do Cibercrime, foi promulgada a 15 de Setembro de 2009, e tem por objetivo adaptar o direito interno à Convenção sobre Cibercrime do Conselho da Europa que foi aprovada por Resolução da Assembleia da República n.º 88/2009, em DR I Série de 15.09.2009, marcando assim, "as disposições penais materiais e processuais, bem como as

disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, [394] do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação."[395]

A Lei n.º 109/2009 contem no capítulo I, o seu objetivo e as definições, e depois, tem uma componente de criminalização no capítulo II com a tipificação de vários crimes informáticos materiais (componente Substantiva), uma parte processual no seu capítulo III sobre meios de obtenção de prova digital (componente Adjetiva). Também conta com uma parte sobre a cooperação internacional no capítulo IV, daí que a sua estrutura é muito semelhante à da Convenção de Budapeste de 2001, e finalmente, o capítulo V trata da aplicação da lei penal portuguesa no espaço e da competência dos tribunais portugueses, além de abordar disposições de natureza transitória.

No art.º 2 da Lei do Cibercrime encontramos as definições referenciadas na Convenção de Budapeste que são: Sistema informático, Dados informáticos, Dados de tráfego, Fornecedor de serviço, Interceção, Topografia, e Produto semicondutor, o que permitem ampliar o âmbito das possíveis atividades que podem ser punidas pela lei em Portugal.[396]

Em quanto aos delitos informáticos materiais em sentido estrito, que estabelece a Lei do Cibercrime, por ter um elemento necessariamente informático encontramos:

Artigo 3º - Falsidade informática;
Artigo 4º - Dano relativo a programas ou outros dados informáticos;
Artigo 5º - Sabotagem informática;
Artigo 6º - Acesso ilegítimo;
Artigo 7º - Interceção ilegítima;
Artigo 8º - Reprodução ilegítima de programa protegido.

4.5.1. Falsidade informática (art.º 3 da Lei n.º 109/2009)

[394] A Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, substitui a Decisão-Quadro 2005/222/JAI (DM) do Conselho da Europa, numa ação para unificar as legislações nacionais na luta contra a pirataria, a propagação de vírus e ataques de negação de serviço.

[395] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime., [Em linha]. Art.º 1

[396] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime., [Em linha]. Art.º 2

"1 - Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2 - Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 - Quem, actuando 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 objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.

4 - Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista 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."[397]

Ao ser a falsidade informática um crime público, não precisa necessariamente de queixa para iniciar o procedimento criminal de acordo com o art.º 48 do Código de Processo Penal de Portugal,[398] além disto, é um tipo de crime em sentido estrito porque os atos de falsificação incidirem sobre dados ou programas informáticos.[399]

O crime é punível com pena até 5 anos de prisão ou multa até 600 dias, e a situação agrava-se com pena de prisão de 1 a 5 anos de acordo com os números 2 e 4, quando as ações afetarem dados registados ou incorporados em cartão bancário de pagamento ou qualquer dispositivo que permita o acesso aos sistemas de pagamento, assim como, quem importar, distribuir, vender ou detiver para fins comerciais os dispositivos que permitam o acesso aos dados referidos. Se o ato e praticado por um sujeito no exercício das suas funções, este será punido com 2 a 5 anos de prisão. Nestes casos, o bem

[397] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 3

[398] CPP Art.º 48 - O Ministério Público tem legitimidade para promover o processo penal, com as restrições constantes dos artigos 49.º a 52.º (Excetuando-se os casos em que o procedimento dependa de acusação particular ou de queixa.)

[399] VENÂNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 38

jurídico que se protege não é o património, quer dizer, que o prejuízo não é patrimonial, o que se protege é a confidencialidade, integridade e a disponibilidade dos dados e dos sistemas informáticos.[400]

Na circunstância, no n.º 1 o crime é consumado do ponto de vista objetivo, apenas com a produção de dados ou documentos não genuínos.[401] Do ponto de vista subjetivo, é a "intenção de provocar engano nas relações jurídicas" [402] aquando esses dados ou documentos sejam considerados ou utilizados para fines legais.

A clonagem de cartões bancários será um dos comportamentos previstos no n.º 2. O próprio Código Penal já prevê a contrafação de cartões de crédito ou de outros meios de pagamento nos arts.º 262, 266 e 267.[403] O art.º 267, nº 1, alínea c) abrange apenas a parte gráfica do cartão, a sua aparência. Agora bem, no Ac. Trib. da Relação de Lisboa de 30 de junho de 2011 reconhece-se que:

> "O bem jurídico protegido pelo crime de contrafação de moeda é a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfego monetário; o bem jurídico protegido pelo crime de falsificação informática é a integridade dos sistemas de informação. Se a ação consiste em duplicar e utilizar cartões bancários, com acesso a dados que neles se encontravam, produzindo com estes dados documentos não genuínos para os utilizar no levantamento de dinheiro ou pagamento de bens, ocorrem, em concurso efetivo, aqueles dois crimes."[404]

---

[400] Cit. por. ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 3 - Ac. TRP de 24-04-2013, sumário retirado da CJ, 2013, T2, pág.223 (jurisprudência)

[401] Cit. por. ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 3 - Ac. TRE de 19-05-2015 (jurisprudência)

[402] VENÁNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 38

[403] **CP Art.º 262.** *Contrafacção de moeda*
1 - Quem praticar contrafracção de moeda, com intenção de a pôr em circulação como legítima, é punido com pena de prisão de 3 a 12 anos.
2 - Quem, com a intenção de a pôr em circulação, falsificar ou alterar o valor facial de moeda legítima para valor superior é punido com pena de prisão de 2 a 8 anos.
CP Art.º 266. Aquisição de moeda falsa para ser posta em circulação:
1 - Quem adquirir, receber em depósito, transportar, exportar, importar ou por outro modo introduzir em território português, para si ou para outra pessoa, com intenção de, por qualquer meio, incluindo a exposição à venda, a passar ou pôr em circulação:
a) Como legítima ou intacta, moeda falsa, falsificada, fabricada sem autorização legal ou em desrespeito pelas condições em que as autoridades competentes podem emitir moeda; ou
b) Moeda metálica depreciada, pelo seu pleno valor; ou
c) (Revogada.)
é punido, no caso da alínea a), com pena de prisão até 5 anos e, no caso da alínea b), com pena de prisão até 6 meses ou com pena de multa até 60 dias.
2 - A tentativa é punível.
CP Art.º 267. Títulos equiparados a moeda
1 - Para efeitos do disposto nos artigos 262.º a 266.º, são equiparados a moeda:
a) Os títulos de crédito nacionais e estrangeiros constantes, por força da lei, de um tipo de papel e de impressão especialmente destinados a garanti-los contra o perigo de imitações e que, pela sua natureza e finalidade, não possam, só por si, deixar de incorporar um valor patrimonial;
b) Os bilhetes ou fracções da lotaria nacional; e
c) Os cartões de garantia ou de crédito.
2 - O disposto no número anterior não abrange a falsificação relativamente a elementos a cuja garantia e identificação especialmente se não destine o uso do papel ou da impressão.

[404] Cit. por. ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 3 - Ac. Trib. da Relação de Lisboa, de 30/06/2011 (jurisprudência)

A justificação para o concurso[405] efetivo destes crimes foi o facto de estes dois tipos legais tutelarem bens jurídicos distintos; Temos aqui varias aproximações que podem ser feitas, quer pelo bem jurídico, quer pela conduta em si. Ainda mais, entre os crimes de falsidade informática no especial no n.º 2 e o crime de burla informática (art.º 221.º CP), pode existir concurso efetivo (real) de infrações, no caso em que o agente da falsidade informática seja também da burla informática.[406]

No número 3 deste artigo, a penalização do utilizador do documento falseado, seja no caso no n.º 1 ou n.º 2 do art.º 3, requer estabelecer o dolo específico da "intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro."[407] A sanção será a prevista no nº1 ou n.º 2 do mesmo artigo, respetivamente.

O previsto no n.º4 neste artigo, pune-se as condutas de "*importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2,"* do diploma objeto de análise[408]. Chama a atenção a conjugação verbal *"tenha sido"* o que implica que, primeiro deve consumar-se os factos típicos designados no n.º2, para poder aplicar as disposições do n.º 4, o que contraria a logica da previsão do crime. PEDRO VENÁNCIO, sobre isso entende, que existe um lapso de escrita do legislador e por isso urge retificar a previsão legal deste n.º 4 do art.º 3 para que o crime consuma-se com as condutas de importação, distribuição ou detenção dos referidos dispositivos, mas sem precisar da efetiva utilização dos mesmos.[409]

Por outro lado, há sobreposição parcial entre o crime de "falsidade informática" (art.º 3) e o crime de "dano dos dados informáticos" (art.º 4). A diferencia está no dolo específico de "falsidade

---

[405] **Concurso de normas**: quando a conduta do agente realiza (preenche) o tipo de várias normas incriminadoras – O Concurso pode ser **Efetivo** o qual divide-se em **Real** (quando o agente pratica vários factos que preenchem autonomamente vários crimes ou várias vezes o mesmo crime) e **Ideal** (o agente comete vários crimes através da prática de uma só ação); Ou pode ser Concurso **Aparente** (impuro) quando a conduta criminal é exclusiva e totalmente absorvida por um só tipo, de modo tal que todos os demais devem ceder.

[406] Cit. por. ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 3 - Ac. TRP, de 14.09.2016 (jurisprudência)

[407] Cit. por VENÁNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 40

[408] O n.º 4 do Art. 3 da Lei 109/2009 corresponde ao previsto no art.º 6 da Convenção sobre o Cibercrime, sob a epígrafe "Utilização indevida de dispositivos"

[409] VENÁNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 40

informática" que como foi indicado é "a intenção de provocar engano nas relações jurídicas"[410]. À partida preenchendo este art.º 3, não se aplica o art.º 4.

As práticas de *phishing*[411] e *pharming*[412] cumprem os princípios factuais, para que possam ser sancionados de acordo com as disposições deste diploma.

4.5.2. Dano relativo a programas ou outros dados informáticos (art.º 4 da Lei n.º 109/2009)

> "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.
> 2 - A tentativa é punível.
> 3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.
> 4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.
> 5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.
> 6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa."[413]

O objetivo do legislador com este artigo foi o de defender "a integridade e o bom funcionamento ou o bom uso de dados e programas informáticos"[414]. Portanto, neste art.4º o legislador pretendeu tutelar situações em que a conduta do sujeito ativo simplesmente preenche o tipo objetivo de crime de dano relativo aos programas ou outros dados informáticos, ao "apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios"[415], sem autorização, de forma negligente ou ilegítima, pelo qual não requerer de dolo específico

---

[410] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 3, n.º 1

[411] Tipo de Ataque informático descrito no subcapítulo 4.1. O CRIME INFORMÁTICO nota de rodapé n.º 315

[412] Tipo de Ataque informático que consiste em redirecionar o nome de domínio (DNS) de uma entidade confiável para uma página da Web, aparentemente idêntica, mas que na verdade foi criada pelo agente para obter dados privados do usuário, geralmente dados bancários.

[413] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 4

[414] VERDELHO, Pedro; BRAVO, Rogeiro; e LOPES ROCHA, Manuel – LEIS DO CIBERCRIME. Vol. I. p. 253

[415] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 4 núm. 1

ou especial intenção para acusar ou punir ao sujeito com pena de multa ou prisão até 3 anos, mas se o dano causado for de "valor elevado"[416] a pena é de prisão até 5 anos ou de multa[417] até 600 dias, e se o dano "for de valor consideravelmente elevado"[418] a pena é de prisão de 1 a 10 anos.

Dessa maneira, pretende-se assegurar o bom funcionamento dos sistemas informáticos através da penalização das ações que efetivamente danificam esses sistemas assim como das tentativas, sempre que não existem causas que excluem a culpa ou justificam a ilicitude, e seja presentada a queixa por parte do lesado.

Com o n.º 3 do art.º 4, criminaliza-se quem ilegitimamente produz, vende, distribui, dissemina ou introduz dispositivos, sistemas ou programas informáticos como por exemplo os chamados *malwares*,[419] e os *spam*,[420] com vista a praticar o crime de dano previsto no n.º 1 do art.º 4, e portanto, não se exigindo a consumação do dano ou sequer de tentativa dos mesmos, pelo que, o tipo legal, torna-se num crime de risco ou de perigo.[421] Nestes casos, o Ministério Público pode agir, sem requerer de queixa. Com efeito, trata-se de um crime semipúblico.[422]

O Código Penal também concebe no art.º 212[423] o crime de Dano, mas este é considerado um dano comum às coisas, onde o bem jurídico protegido é o património, quando o agente destrói, desfigura, danifica, ou torna inacessível coisa alheia; Este diploma visa proteger os bens corpóreos. Enquanto que, o art.º 4 da Lei 109/2009 é um pouco mais abrangente, não só por ser um crime informático em sentido

---

[416] Concorde ao art.º 202 do CP "Definições legais: Para efeito do disposto nos artigos seguintes considera-se: a) Valor elevado: aquele que exceder 50 unidades de conta avaliadas no momento da prática do facto;"

[417] Concorde ao art.º 47 do CP, Pena de multa, núm. 1 - A pena de multa é fixada em dias, de acordo com os critérios estabelecidos no n.º 1 do artigo 71.º, sendo, em regra, o limite mínimo de 10 dias e o máximo de 360, e **art.º 70 CP**, "Critério de escolha da pena: Se ao crime forem aplicáveis, em alternativa, pena privativa e pena não privativa da liberdade, o tribunal dá preferência à segunda sempre que esta realizar de forma adequada e suficiente as finalidades da punição."

[418] Concorde ao art.º 202 do CP Definições legais: Para efeito do disposto nos artigos seguintes considera-se: (...) b) Valor consideravelmente elevado: aquele que exceder 200 unidades de conta avaliadas no momento da prática do facto;..."

[419] Descrito no Ver Capitulo IV, Subcapítulo 4.1. O CRIME INFORMATICO. Nota de rodapé n.º 317

[420] SPAM (Sending and Posting Advertisement in Mass) são mensagens eletrónicas não solicitadas enviadas para uma grande quantidade de pessoas. Ou seja, é o ato de enviar e postar publicidade em massa. Geralmente, a propaganda é o tipo de SPAM mais conhecido e o *e-mail* é a maneira mais usual de enviá-las". SANTOS, Barbara - SPAM: o que é e como evitar essa prática.

[421] VENÁNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 46

[422] PEDRO VENÁNCIO, excetua o n.º 5 (valor consideravelmente elevado) por ser um crime público e agravado, pela perturbação da paz social e a fiabilidade dos meios eletrónicos. (Lei Do Cibercrime. Anotada e Comentada, p. 45)

[423] CP Art.º 212.- Dano:
1- Quem destruir, no todo ou em parte, danificar, desfigurar ou tornar não utilizável coisa alheia, é punido com pena de prisão até 3 anos ou com pena de multa.
2 - A tentativa é punível.
3 - O procedimento criminal depende de queixa.
4 - É correspondentemente aplicável o disposto nos artigos 206º e 207º

estrito, au tutelar a integridade, a fiabilidade e a correta funcionalidade dos dados ou programas informáticos em concordância com o art.º 35 da Constituição da República Portuguesa,[424] senão, por ser um crime de risco ou de perigo, como foi comentado.

É importante considerar o disposto no art.º 45 sobre "Viciação ou destruição de dados pessoais" da Lei n.º 67/98[425] de Proteção Dados Pessoais, que sanciona com prisão até 2 anos ou multa até 240 dias a conduta de "apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afetando a sua capacidade de uso"[426] sem a devida autorização; Sendo um crime público, punível por dolo e por negligência, onde a pena pode ser agravada se o dano for particularmente grave.

Por quanto a norma invocada é específica para tutelar os dados pessoais, "a sua fidedignidade e segurança, independentemente do seu suporte,"[427] e que em nosso caso de estudo poderiam ser os dados pessoais de pagamento; Esta norma prevaleceria sobre as disposições do art.º 4 da Lei n.º 109/2009 Lei do Cibercrime, sempre que o ilícito recaia sobre dados "pessoais". Deve-se notar, que a sanção prevista na Lei de Proteção Dados Pessoais é menos gravosa, que a prescrita na Lei do Cibercrime.

Da mesma maneira, Benjamim Silva Rodrigues[428] afirma que em relação ao crime previsto no art.º 45 sobre "Viciação ou destruição de dados pessoais" da Lei n.º 67/98 que: "Este tipo de crime complementa os artigos 5.º e 6.º da LCI [agora Lei de Cibercrime] respeitantes aos crimes de "Dano Relativo a Dados ou Programas Informáticos" e à "Sabotagem Informática." A especificidade resulta no tipo legal de crime em estudo, se identificarem 'dados pessoais' que podem ainda, caber nos artigos 5.º e 6.º da LCI [agora Lei de Cibercrime], na fórmula legal genérica «'dados' ou programas». Verifica-se uma 'zona de coincidência' ao nível de certo tipo de dados a tutelar." É por isso que Benjamim Silva

[424] Citado no Capitulo I, Subcapítulo 1.4.- A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS EM PORTUGAL.

[425] "Enquanto não for aprovada legislação nacional que complemente o RGPD e que venha a revogar a Lei n.º 67/98, de 26 de outubro, esta lei manter-se-á em vigor em tudo o que não contrarie aquele diploma europeu. No que diz respeito aos tratamentos de dados pessoais relativos à prevenção, investigação e repressão criminal, a Lei n.º 67/98 tem integral aplicação, sem qualquer alteração, até à transposição da Diretiva 2016/680." (COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – Comunicado da CNPD Aplicação do novo quadro legal de proteção de dados. [Em linha]: Lisboa, 25 de maio de 2018, [Consult. 18 agosto 2018]. Disponível na internet https://dre.pt/documents/10184/826042/Comunicacao+CNPD_25_5_2018.pdf/87e28703-4e8c-4439-9ba9-f0f7b75ceab1)

[426] Lei n.º 67/98 Lei de Proteção de Dados Pessoais. Art.º 45

[427] VENÁNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 48

[428] Cit. por VENÁNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 49

Rodrigues "defende a prevalência do crime da LPDP sobre os crimes da LCI (agora Lei de Cibercrime), nas situações em que os bens atingidos no ambiente digital sejam dados pessoais."[429]

4.5.3. Sabotagem informática (art.º 5 da Lei n.º 109/2009)

> "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.
> 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
> 3 - Nos casos previstos no número anterior, a tentativa não é punível.
> 4 - A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.
> 5 - A pena é de prisão de 1 a 10 anos se:
> a) O dano emergente da perturbação for de valor consideravelmente elevado;
> b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos."[430]

Este artigo tutela o normal funcionamento dos sistemas informáticos e das comunicações eletrónicas que garantam os serviços básicos dos cidadãos, como os de acesso à banca *on-line* ou *homebanking*;[431] transferências de dinheiro na rede, compras on-line ou pagamentos à distância, pelo que se tratar de um crime público, e portanto, no procedimento criminal não depende de queixa.[432]

Preenche o tipo objetivo do crime na sua forma simples: "quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele,

---

[429] VENÂNCIO, Pedro – Lei Do Cibercrime. Anotada e Comentada, p. 48

[430] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 5

[431] "Através da emissão de cartões bancários é possível realizar uma imensidão de operações nomeadamente através dos serviços de homebanking, sendo possível, para o efeito, aceder a uma variedade de operações bancária em linha, tudo através de um simples dispositivo, o computador.(...) Destarte, a abertura de conta pressupõe a possibilidade de aceder a um serviço proporcionado pela instituição bancária de efetuarmos operações através da Internet. Para tanto é outorgado um contrato de adesão entre a instituição bancária e o cliente". AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação. P.96

[432] VENÂNCIO, Pedro – Op. cit., p. 53

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."[433]

A lei, só exige que o sujeito ativo atue sem autorização, pelo que não se requer de uma especial intenção, o que alarga o seu âmbito de aplicação e facilita a prova e punição[434] com prisão até 5 anos ou com multa até 600 dias, e com a possibilidade de ser aumentada de 1 a 5 anos de prisão no caso de dano elevado, e de 1 a 10 anos caso o dano seja de valor consideravelmente elevado ou se os danos graves ou duradouros for para um sistema informático que apoie funções sociais críticas.

No caso dos atos descritos no n.º 2 do artigo, estes consistem na difusão das condutas descritas no tipo objetivo do crime na sua forma simples (nº 1 ibidem), pelo que, se pretende punir os atos preparatórios da prática do Sabotagem Informática, e ao contrário dos artigos 3º e 4º da Lei n.º 109/2009, a sua tentativa não é punível. No entanto, o crime na sua forma simples, a tentativa e punível conforme o disposto no art.º 23[435] do Código Penal.[436]

A diferencia entro o crime de Sabotagem Informática e o crime de Dano Relativo a Programas ou Dados Informáticos, é o objeto do crime. Assim o crime de Sabotagem Informático pune os atos que perturbem gravemente o funcionamento de todo o sistema informático ou a comunicação dos dados, e o crime de Dano Relativo a Programas ou Dados Informáticos, pune os atos relacionados de um qualquer dado informático ou programa, sem que seja necessário que o dano caia em todo o sistema informático.

---

[433] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 5

[434] VENÁNCIO, Pedro – Op. cit., p. 53. Na LCI (lei anterior à Lei do Cibercrime n.º 109/2009) o crime de Sabotagem Informática continha o elemento subjetivo específico do tipo legal previsto no seu art.º 6 com a "intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância" ibidem.

[435] CP Art.º 23 - Punibilidade da tentativa:
"1 - Salvo disposição em contrário, a tentativa só é punível se ao crime consumado respectivo corresponder pena superior a 3 anos de prisão.
2 - A tentativa é punível com a pena aplicável ao crime consumado, especialmente atenuada.
3 - A tentativa não é punível quando for manifesta a inaptidão do meio empregado pelo agente ou a inexistência do objecto essencial à consumação do crime."

[436] VENÁNCIO, Pedro – Op. cit., p. 53

No que respeita ao artº. 329[437] do Código Penal relativo ao Sabotagem, preocupa-se com a natureza do crime, dimensão e importância económica.[438] Sobre isto, PEDRO VENÁNCIO[439] reconhece, que este crime não consume o crime de Sabotagem Informática da Lei n.º 109/2009 em determinas situações, porque o crime de Sabotagem Informática não depende da sua natureza pública ou privada, nem da sua dimensão ou importância económica. Mas se, por exemplo o ataque afeta o sistema informático de uma grande empresa de telecomunicações em Portugal como "Altice", que ponha em causa o funcionamento da rede de telecomunicações a nível nacional, por mais que cumpra com o tipo de crime de Sabotagem Informática, não deixa de se integrar o crime de Sabotagem do Código Penal no seu art.º 329 pela dimensão do dano e importância económica que pode implicar.[440]

A prática de DDOS[441], ou controlo de redes informáticas através de *botnets*[442] poderão preencher uma forma de sabotagem informática, na medida que interfere no sistema de informação.[443]

4.5.4. Acesso ilegítimo (art.º 6 da Lei n.º 109/2009)

> "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
> 2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.
> 3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.
> 4 - 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.

---

[437] CP Art.º 329. Sabotagem: "Quem destruir, impossibilitar o funcionamento ou desviar dos seus fins normais, definitiva ou temporariamente, total ou parcialmente, meios ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população, infra-estruturas de relevante valor para a economia, a segurança ou a defesa nacional, com intenção de destruir, alterar ou subverter o Estado de direito constitucionalmente estabelecido, é punido com pena de prisão de três a dez anos."

[438] ACÓRDÃO DO TRIBUNAL DA RELAÇÃO DE COIMBRA de 15-10-2008, Processo nº 368/07.8TAFIG.C1, relatora Alice Santos [Em linha]

[439] VENÁNCIO, Pedro – Op. cit., p. 53

[440] Ibidem.

[441] Descrito no subcapítulo 4.1. O CRIME INFORMÁTICO. Ver nota de rodapé n.º 319

[442] "As redes botnet, são as responsáveis pela maior parte do *spam* enviado (...) botnet consiste num conjunto de computadores controlados por atacantes através de, por exemplo, vírus, cavalos de Troia no computador completamente incauto. A execução de um ataque de botnet processa-se da seguinte forma: o botnet quando quiser enviar ataques de phishing envia mensagem aos milhares de computadores que controla para o fazerem em vez dele." (AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação. P.67)

[443] Em Portugal o *spam* é punido com pena de multa, mas que não está no CP, é uma contraordenação. Mas não é crime.

5 - A tentativa é punível, salvo nos casos previstos no n.º 2.
6 - Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa."[444]

Este artigo abrange as infrações relativas à segurança e ameaças contra a intimidade, integridade e disponibilidade[445] da informação das pessoas públicas ou privadas contidas num sistema ou nas redes informáticas, portanto, salvaguarda assim, os dados eletrónicos no ciberespaço. A segurança do sistema informático é o bem jurídico protegido,[446] no entanto, para Pedro Venáncio, acresce-se ainda, a proteção ao património do lesado[447]. Em nosso entender, o tipo penal criminaliza o ato de aceder sem autorização a um sistema informático, pelo que, não é necessário que o agente pretenda obter um benefício patrimonial, basta que aceda ilegitimamente.

O tipo objetivo de crime é: "sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele"[448], e "de qualquer modo aceder a um sistema informático."[449] Em quanto ao elemento subjetivo específico do crime, este não esta presente, ou melhor, não é exigida uma especial intenção por parte do sujeito ativo; Em vista disso, só há um dolo genérico que alarga o âmbito do crime e simplifica a sua prova e punição[450], quem simplesmente preenche o tipo objetivo de aceder num qualquer sistema informático sem autorização.

No caso dos atos descritos no n.º 2 do artigo, estes consistem na difusão das condutas descritas no tipo objetivo do crime na sua forma simples (nº1 ibidem), pelo que, se pretende punir os atos preparatórios para a obtenção ilegítima de dados nos sistemas informáticos. Neste caso o crime é punível na sua forma consumada e não a tentativa.[451] Sendo assim, a tentativa de acesso ilegítimo e punível, só nos casos nº1, nº3 e 4º deste artigo n.º 6.

Na sua forma simples, é um crime considerado de pouca repressão, com prisão de 1 mês a 1 ano, ou multa de 10 a 120 dias. Na sua forma qualificada, se a execução do delito implica a violação de regras de segurança a pena agrava-se com prisão até 3 anos ou multa, e se com o acesso ilegítimo "o

---

[444] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 6
[445] VENÁNCIO, Pedro – Op. cit., p. 59
[446] Acórdão do Tribunal da Relação do Porto de 08-01-2014 Processo nº: 1170/09.8JAPRT.P2
[447] VENÁNCIO, Pedro – Op. cit., p. 59
[448] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 6
[449] Ibidem.
[450] VENÁNCIO, Pedro – Op. cit., p. 60
[451] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 6 núm. 5

agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei" ou se obtiver benefício de valor consideravelmente elevado, a pena é ainda agravada com prisão de 1 a 5 anos.

O procedimento penal depende de queixa, com exceção nos casos previstos no n.º 2 deste artigo (difusão das condutas descritas no tipo objetivo), e no n.º 4 (na sua forma qualificada); Em vista disso, é considerado um crime semipúblico, pelo qual, o Ministério Público tem legitimidade para seguir com o procedimento criminal nos caos dos n.os 2 e 4 do art.º 6.

Finalmente, o acesso ilegítimo, normalmente designado por *hacking*,[452] acaba por ser um meio para outros tipos de crimes. Assim sustenta Pedro Venáncio, quando diz que a prática de Sabotagem Informática trata-se de um crime de dano que envolve a prática do Acesso Ilegítimo, pelo que se considera que o consome.[453] De modo igual, o Tribunal de Relação de Guimarães, no Acórdão de 17-11-2008, exprime que "entre os crimes de sabotagem informática e acesso ilegítimo existem concurso de infrações"[454]

4.5.5. Intercepção ilegítima (art.º 7 da Lei n.º 109/2009)

> "1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.
> 2 - A tentativa é punível.
> 3 - Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número"[455]

---

[452] É o conjunto de técnicas pelas quais uma pessoa sem autorização acessa um sistema informático, violando as medidas de segurança estabelecidas originalmente.

[453] Cit. por VENÁNCIO, Pedro – Op. cit., p. 58 (Sentença da 9.ª Vara Criminal do Circulo de Lisboa, 3ª. Secção de 19-6-1997, processo n.º 1/97, Ref.ª JusNet 10510/1997)

[454] Cit. por VENÁNCIO, Pedro – Op. cit., p. 65 Processo n.º 2233/07, publicado na CJ, ano XXXIII, Tomo V/2008, a pp. 289 a 292, com sumário de António Geraldes (Ref.ª CJ online 7922/2008)

[455] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 7

Similar ao tipo de crime de Acesso Ilegítimo, a Intercetação Ilegítima, visa tutelar a segurança nas comunicações informáticas de dados privados, como os dados pessoais de pagamento utilizados no comércio eletrónico, a sua intimidade, privacidade e confidencialidade.

À vista disso, a segurança das comunicações informáticas e a sua privacidade é o bem jurídico protegido. Para tanto, criminaliza o simples ato de intercetar sem autorização transmissões de dados informáticos, inclusive meta-dados[456] não-públicos, seja por telefone, ficheiro ou correio eletrónico[457], quer dizer, que não é necessário que o agente pretenda obter um benefício patrimonial, basta que intercete ilegitimamente os dados eletrónicos.

O tipo objetivo de crime é: intercetar ilegitimamente "transmissões de dados informáticos que se processem no interior de um sistema informático, a ele destinado ou dele proveniente"[458] através de meios técnicos. Neste crime, não requer qualquer especial intenção ou dolo específico que tenha de ser provado, deste modo, estamos perante um dolo genérico do agente criminoso, quando este intercete ilegitimamente transmissões de dados informáticos, o qual pode ser sancionado com uma pena de prisão até 3 anos ou pena de multa.

O nº3 pune os atos preparatórios que permitam intercetar dados informáticos, ou fazer outros tipos de crime; Estes atos são: a produção, distribuição, venda, disseminação ou introdução num sistema informático destinados a produzir as ações não autorizadas do n.º 1 deste artigo 7º.

A tentativa deste crime na sua forma simples mesmo sem obter resultado é punível, assim como os atos preparatórios já comentados.

O crime é público pela importância do bem jurídico protegido, consequentemente, o procedimento criminal não precisa de queixa.

---

[456] "Descrição ou conjunto de características de um dado ou de um item, especialmente em relação a informação processada por computador, como, por exemplo, o tamanho ou o tipo de um ficheiro, ou ainda a data da última alteração" "metadado", em Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, https://priberam.pt/dlpo/metadado [consultado em 26-08-2018].

[457] VENÂNCIO, Pedro – Op. cit., p. 68

[458] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Art.º 7 núm. 1.

Este artigo tem semelhança com o previsto no art.º 192[459] n.º 1 do Código Penal relativo à "Devassa da vida privada" ao proteger a privacidade das pessoas, embora, a diferença esta no tipo objetivo[460] do crime, porque no caso da Devassa da vida privada é "Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa," especificamente da "comunicação telefónica, mensagens de correio electrónico ou facturação detalhada." Também varia o elemento subjetivo, dado que, na Intercetação Ilegítima o dolo é genérico, enquanto que, na Devassa da vida privada, o dolo é específico quando requer de uma especial "intenção de devassar a vida privada das pessoas."

Similarmente, o art.º 194[461] nº2 do Código Penal sobre "Violação de correspondência ou telecomunicações", encontra paralelo com a Intercetação ilegítima no que tange às comunicações eletrónicas. PEDRO VENÁNCIO explica que pode "existir sobreposição quanto à Intercetação da mensagem escrita ou comunicação de áudio ou vídeo em ambiente digital, já não haverá quando se trata da intercetação de transmissão de dados informáticos de natureza diversa"[462] porque os dados informáticos abarca todo tipo de dados informáticos como se observa na definição da alínea b) do art.º 2[463] da Lei n.º 109/2009 Lei do Cibercrime, o que extravasa a natureza dos dados protegidos no art.º 194[464] nº2 do Código Penal.[465] Outra diferença, é que no art.º 194 do CP tem de se chegar ao conteúdo das telecomunicações, enquanto o art.º 7 da Lei n.º 109/2009 basta ter acesso aos meta-dados.

Entre as ações ou práticas que concorrem com o disposto do presente artigo, temos o ciber-espionagem, entre elas as técnicas que utilizam ondas eletromagnéticas que permitem intercetar todas

---

[459] CP 192.º Devassa da vida privada:
"1 - Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:
a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada;
b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos;
c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa;
é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias...."

[460] No caso do art.º 7 da Lei n.º 109/2009 Lei do Cibercrime, sobre a Intercetação Ilegítima, como já vimos, o tipo objetivo de crime é: intercetar ilegitimamente "transmissões de dados informáticos que se processem no interior de um sistema informático, a ele destinado ou dele proveniente"

[461] CP art.º 194. Violação de correspondência ou de telecomunicações
"1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.
2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento..."

[462] VENÁNCIO, Pedro – Op. cit., p. 68

[463] "b) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;"

[464] CP art.º 194. Violação de correspondência ou de telecomunicações
"1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.
2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento..."

[465] VENÁNCIO, Pedro – Op. cit., p. 68

as informações que entram em um computador, por exemplo, as antenas do Echelon[466] podem captar ondas eletromagnéticas e transmiti-las a um lugar central para o seu processamento. Existe também uma técnica acústica, que a partir do som captura a informação. Também, as comunicações que são transmitidas por cabo, seja telefone, fax ou dados, podem ser intercetadas com acesso físico ao cabo nas suas extremidades, ou é possível fazer um corte ao cabo ou aceder a partir de um ponto intermediário usando correntes indutivas, sem alterar fisicamente o cabo. No caso de cabos coaxiais de comprimentos longos, existem estações intermediárias que amplificam a sinal, e é nesses pontos que é possível acessar ao interior do cabo.[467]

4.5.6. Reprodução ilegítima de programa protegido (art.º 8 da Lei n.º 109/2009)

> "1 - Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.
> 2 - Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.
> 3 - A tentativa é punível."[468]

Seguindo a linha de crimes estabelecidos na Lei n.º 109/2009, encontramos o art.º 8 que trata de "Reprodução ilegítima de programa protegido", o qual, apesar de não estar orientado para crimes relacionados ao objeto de estudo da presente dissertação, ou seja, não é voltado para os dados pessoais de pagamentos no comércio eletrónico, fizemos apenas algumas referências deste crime.

Sendo assim, o art.º 8 protege o Direito de propriedade intelectual, ao tutelar as violações dos direitos de autor relativos aos programas informáticos, em analogia com o disposto no Código dos Direitos de Autor e Direitos Conexos, onde o tipo objetivo do crime na sua forma simples é "...quem ilegitimamente reproduzir divulgar ou comunicar ao público um programa informático protegido por lei", pelo qual pode ser "punindo com pena de prisão até 3 anos ou com pena"

---

[466] ECHELON é considerada a maior rede de espionagem e análise para intercetar comunicações eletrónicas, controlado pela comunidade UKUSA (Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia)

[467] EXPRESIONBINARIA - Espionaje e Interceptación de las comunicaciones [Em linha]. PUBLICADO EN CIENCIA Y TECNOLOGÍA, NOTICIAS, 10 NOVIEMBRE, 2011. [Consult. 25 Ago 2018]. Disponível na internet https://www.expresionbinaria.com/espionaje-e-interceptacion-de-las-comunicaciones/

[468] ASSEMBLEIA DA REPÚBLICA - Lei n.º 109/2009 Lei do Cibercrime. [Em linha]. Artº. 8

Da mesma forma, o n.º 2 pune com pena de prisão até 3 anos ou com pena, "...quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia." Para estes dois casos, não é exigido dolo específico, em outras palavras, o dolo é genérico, e a tentativa é igualmente punível concorde ao n.º 3 deste artigo.

Ainda que estamos perante à proteção de um direito privado, o crime não depende de queixa, por isto é considerado um crime público, pelo qual o Ministério Público é legitimado para seguir com o procedimento criminal.[469]

4.5.7. Burla informática e nas comunicações (CP art.º 221):

> "1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.
> 2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.
> 3 - A tentativa é punível.
> 4 - O procedimento criminal depende de queixa.
> 5 - Se o prejuízo for:
> a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;
> b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.
> 6 - É correspondentemente aplicável o disposto no artigo 206.º"[470]

A burla informática está no Código Penal e não na Lei n.º 109/2009, e trata, de uma forma de causar prejuízo ao património com a utilização de sistemas informáticos. A fraude informática é uma concretização de um crime que já tínhamos (burla tradicional) mas agora aplicado à parte informática,

[469] VENÂNCIO, Pedro – Op. cit., p. 71

[470] DECRETO-LEI nº 400/82 Código Penal Português. Art.º 221

quando o agente obtém para si ou para terceiro um enriquecimento ou um beneficio ilegítimo, sem precisar "a mediação do ofendido ou da pessoa enganada",[471] ou melhor prescindindo do erro ou engano em relação à pessoa lesada,[472] mas causando-lhe um prejuízo patrimonial por meios informáticos para o cometimento do facto criminoso.

Na senda do pensamento de Pedro Correia e Inês De Jesus,[473] a burla informática não é uma verdadeira burla em sentido próprio e técnico, uma vez que não segue o *iter criminis* da burla clássica, pois, não contempla a astúcia, o erro ou engano e a prática de atos pelo burlado, exigidos na burla tradicional.

Este art.º 221 do Código Penal prevê dois crimes diferentes, porém, equiparáveis, onde o n.º 1 é o crime de burla informática e no n.º 2 é o crime de burla nas telecomunicações.

O bem jurídico protegido é de natureza patrimonial e a fiabilidade dos dados assim como o funcionamento dos sistemas e das redes informáticas, mas o lesado é a pessoa que sofre o prejuízo patrimonial, e portanto, não é necessariamente o proprietário dos dados ou programas informáticos.[474] Os elementos de "enriquecimento ilegítimo" no caso da burla informática e "benefício ilegítimo" no caso da burla nas comunicações ajudam a diferenciar os dois tipos de crime, por quanto "benefício" não é necessariamente o mesmo que um "enriquecimento". O enriquecimento "pode traduzir-se num aumento patrimonial, na diminuição de débitos ou na poupança de despesas,"[475] entretanto o beneficio, pode no só ser de forma patrimonial, senão, "a utilização imediata pelo agente de sistemas de comunicações, sem para isso ter que suportar o respetivo custo,"[476] ainda o bem jurídico protegido no tipo penal da burla nas comunicações é o "normal funcionamento ou exploração de serviços de comunicações".

---

[471] Cit. por AZEVEDO, Ana - Burlas Informáticas: Modos de Manifestação. Braga: Universidade do Minho, 2016. Dissertação de Mestrado. P. 40

[472] ACÓRDÃO DO TRIBUNAL DA RELAÇÃO DE COIMBRA de 15-10-2008, processo nº 368/07.8TAFIG.C1, relatora Alice Santos [Em linha] Coimbra [Consult. 19 Agosto 2018]

[473] CORREIA, Pedro; DE JESUS, Inês - Combate às transferências bancárias ilegítimas pela Internet no direito português:entre as experiências domésticas e políticas globais concertadas. Scientific Electronic Library Online – SCIELO. [Em linha]. Rev. direito GV vol.12 no.2 São Paulo May/Aug. 2016 [Consult. 17 Ago. 2018]. Disponível na internet: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322016000200542

[474] AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação. P. 36

[475] Cit. por. CORREIA, Pedro; DE JESUS, Inês – op. cit.

[476] Cit. por AZEVEDO, Ana - Burlas Informáticas: Modos de Manifestação. Braga: Universidade do Minho, 2016. Dissertação de Mestrado. P.43

O tipo objetivo do crime no caso da burla informática é "causar a outra pessoa prejuízo patrimonial interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento,"[477] e no caso da burla nas comunicações é quem "com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações".[478]

O elemento subjetivo decorre da "intenção de obter para si ou para terceiro enriquecimento ilegítimo" para o caso da burla informática ou "obter para si ou para terceiro um benefício ilegítimo" no caso da burla nas comunicações, pelo que estamos perante a um delito de ação dolosa, e por conseguinte é necessário que o agente da infração tenha uma atuação positiva, com consciência e vontade de causar a outrem um dano ou prejuízo patrimonial.

Para a consumação do crime é exigida a produção de uma perda patrimonial da vítima, pelo que pode ser considerado um tipo de crime de resultado ou material, mas para efetiva consumação do crime não terá que ocorrer necessariamente um enriquecimento por parte do agente ou de terceiro.

A tentativa é igualmente punível de acordo ao n.º 3 deste artigo, e a pena pode ser agravada com prisão até 5 anos ou com pena de multa até 600 dias se o prejuízo for de valor elevado, e com pena de prisão de 2 a 8 anos, se o prejuízo for de valor consideravelmente elevado,[479] Em vista disso, em princípio, o crime é semipúblico, e portanto, o procedimento criminal depende de queixa na sua forma simples. Contudo, nos casos previstos no n.º 5 deste articulo (gravação da pena) pela forma qualificada, o crime torna-se público, pelo que, o Ministério Público pode promover o processo penal.[480]

Este tipo de crime abrange "a utilização indevida de máquinas automáticas de pagamento (ATM), incluindo os casos de manipulação ou utilização indevida no sentido de utilização sem a vontade do

[477] DECRETO-LEI nº 400/82 Código Penal Português. Art.º 221 n.º 1
[478] DECRETO-LEI nº 400/82 Código Penal Português. Art.º 221 n.º 2
[479] DECRETO-LEI nº 400/82 Código Penal Português. Art.º 221 n.º 5
[480] CORREIA, Pedro; DE JESUS, Inês – op. cit.

titular"[481], assim, se o agente furta o cartão de débito ou de crédito e levanta dinheiro em ATM indevidamente ou faz pagamentos num terminal POS[482], há burla informática.[483] Paulo Pinto de Albuquerque adiciona a estes factos "o carregamento não autorizado de cartão de moeda eletrónica (*smart card*, *pay before card*) com o PIN de outrem"[484] pode constituir também a conduta típica prevista no art.º 221 do Código Penal.

Se, a pratica do atos como o *phishing*,[485] permite ao atacante obter para si ou para terceiro enriquecimento ilegítimo bem seja, por ter acesso à conta bancaria e extrair desta o dinheiro do titular, causando "a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento"[486], tem-se preenchido o tipo objetivo na sua forma simples do crime de *Burla Informática e nas Comunicações* previsto no art.º 221 n.º 1 do Código Penal.

Não obstante, no caso acima referido, poderá haver concurso de penas com a tipificação de Acesso ilegítimo estabelecido no Art.º 6 da Lei de Cibercrime, se o atacante acede ao sistema informático do titular do direito sem estar autorizado. Em todo caso, o delito de Burla Informática abrange o delito de Aceso Ilegítimo, por ser o acesso ao sistema informático só uma parte da infração necessária hasta consumar por completo o crime, que é com a obtenção de lucro. Nesse sentido, "essas parcelas apenas deverão ser consideradas atos preparatórios do crime de burla informática e que não deverão ser individualmente punidas".[487]

Além disso, no caso de *pharming* por medio da reprodução de uma página de uma instituição bancária com elementos em tudo semelhantes aos da página oficial, ademais de configurar-se o crime de falsidade informática prescrita no art.º 3 da Lei n.º 109/2009 pelo conteúdo enganoso, com indicação

---

[481] ACÓRDÃO DO TRIBUNAL DA RELAÇÃO DE COIMBRA de 15-10-2008, processo nº 368/07.8TAFIG.C1, relatora Alice Santos [Em linha] Coimbra [Consult. 19 Agosto 2018]

[482] Máquina de ponto de venda (do inglês: Point of Sale ou Point of Service).

[483] AZEVEDO, Ana – Op. cit. P.38

[484] Cit. por AZEVEDO, Ana – Op. cit. P.38

[485] Tipo de ataque informático descrito no subcapítulo 4.1. O CRIME INFORMÁTICO nota de rodapé n.º 315

[486] Assembleia da República - CÓDIGO PENAL, Art.º 221

[487] AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação. P. 69

falsa do remetente, cujo ato esta sancionado com pena de prisão até 5 anos ou multa de 120 a 600 dias, os agentes do crime incorrem na prática de contrafação, imitação e uso ilegal de marca, constante das alíneas a), b) e c) do art.º 322 do Código de Propriedade Industrial[488], já que a marca é uma sinal distintiva sempre que este devidamente registrada, encontra-se protegida pela lei. No entanto, se os atos cometidos permitiram a extração dos recursos monetários da vítima, é possível indicar que se tem consumado o crime de burla informática, tratando-se de uma "relação de concurso aparente de consumação, onde o crime de burla informática absorve o crime de contrafação, imitação e uso ilegal de marca"[489] e o crime de falsidade informática, "a menos que, atendendo à diversidade dos bens jurídicos protegidos, se entenda verificar-se um concurso efetivo de crimes." [490]

Importa, ainda, distinguir o crime de burla informática previsto no art.º 221 n.º2 do Código Penal, com o crime de "Dano relativo a programas ou outros dados informáticos" previsto no art.º 4 da Lei n.º 109/2009, onde a principal diferença é que no crime de burla tem que existir o benefício ilegítimo, causado pelo prejuízo patrimonial.[491]

[488] **CÓDIGO DA PROPRIEDADE INDUSTRIAL** Art.º 322.- **Violação dos direitos exclusivos relativos a desenhos ou modelos.-** É punido com pena de prisão até 3 anos ou com pena de multa até 360 dias quem, sem consentimento do titular do direito:
a) Reproduzir ou imitar, totalmente ou em alguma das suas partes características, um desenho ou modelo registado;
b) Explorar um desenho ou modelo registado, mas pertencente a outrem;
c) Importar ou distribuir desenhos ou modelos obtidos por qualquer dos modos referidos nas alíneas anteriores. Assembleia da República -

[489] AZEVEDO, Ana – Burlas Informáticas: Modos de Manifestação

[490] SANTOS, Rita, O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos.p. 288

[491] SIMAS, Diana – O CIBERCRIME. Lisboa: Universidade Lusófona de Humanidades e Tecnologias, 2014, Dissertação de Mestrado.

4.6. OS PROBLEMAS DE PERSECUÇÃO DO CRIME INFORMÁTICO.

O cibercrime, para mais ser relativamente novo para as nossas sociedades, evolui de forma rápida ao igual que a tecnologia, e como o direito penal precisa de lei prévia, este não consegue acompanhar o desenvolvimento tecnológico, para lidar com toda a amplitude legal dos crimes informáticos.

Além disso, a complexidade da investigação é sentida em vários níveis e por várias razões, uma é que as instituições dedicadas a sua perseguição não têm as ferramentas adequadas que lhes permitam ser eficazes, dificultando assim, a sua investigação; Da mesma forma que a polícia e os tribunais não estão devidamente treinados na ciência da informática, e no caso de obter provas eletrónicas, é difícil fazer com que os juízes as entendam e considerem a sua validade. Do mesmo modo, há dificuldade na compreensão das leis relativas ao crime informático, a sua interpretação e aplicação, isto leva à necessidade de criação de equipas de investigação que sejam multidisciplinares.

Podemos acrescentar que o direito penal relacionado com o crime informático não contém regras claras quando as pessoas coletivas estão envolvidas como autores desses crimes, é dizer, as responsabilidades jurídicas das empresas não estão devidamente determinadas, o que na prática torna necessária procurar de outras normas que permitam estabelecer sanções.

Outrossim, é a facilidade com que qualquer pessoa possa executar um crime informático, faz com que o número de crimes seja maior em comparação com a forma tradicional de crime, assim acontece com a injúria ou o acesso a determinados dados informáticos. Vemos também que o facto de uma pessoa esteja frente um monitor e fisicamente distanciada da vítima acaba por ser um promotor do crime informático, já que este distanciamento pode levar a que haja uma maior flexibilidade moral e ética dos agentes.

Além de tudo, o facto de que a Internet não é governada, isto é, não há uma autoridade pública, de modo que é mantido o seu princípio de liberdade sem limites e total descentralização, sem barreiras geográficas, tem originado uma discussão sobre o assunto da territorialidade com o fim de conhecer qual lei é aplicável. A regra pelo geral é o lugar "fisico onde o ato foi cometido" (o sitio em que foi

provocado o ato delictuoso *Lex Loci Delicti)*,"[492] mas resulta difícil pelo critério expansivo que tem a lei, que inclui, e a localização do agente como a residencia habitual ou o domicilio *(Lex Loci Delicti Commissi)*.[493] As leis dos estados, especialmente o Direito Internacional Privado, abrangem para mais, o sitio de localização ou lugar do bem lesado *(Lex Rei Sitae*).[494]

Ainda, os criminosos têm ferramentas para não deixar vestígios, como o uso da rede informáticas Tor,[495] que possibilita que se mascare o IP para que seja muito difícil identifica-lo corretamente, e a dificuldade de identificação do agente acresce quando aquele utiliza terminais públicos ou sistemas pré-pagos.[496] Mesmo que, estes vestígios existirem é muito difícil imputá-los a uma determinada pessoa. É fácil para o atacante se passar por outra pessoa.

Contudo, em base no princípio da transnacionalidade, o Estado é forçado a ter uma atitude de colaboração permanente e atual com outros Estados através de autoridades judiciárias e criminais, mais, a falta de harmonização dos regímenes penais entre os Estados soberanos sobre o que são crimes informáticos e os tipos criminosos existentes e traduzi-los em acordos de extradição, contribui à impunidade na persecução do cibercrime.

A própria ONU resume os problemas que envolvem a cooperação internacional na área do cibercrime: [497]

i. Falta de acordos globais sobre que tipo de comportamento deve constituir o cibercrime.
ii. Ausência de acordos globais na definição legal dos comportamentos criminosos.
iii. Falta de especialização entre as diferentes leis processuais nacionais em matéria de investigação de crimes informáticos.
iv. Caráter transnacional de muitos crimes cometidos através do uso de computadores.

---

[492] ROBERTO, Wilson – DANO TRANSNACIONAL E INTERNET. Direito Aplicável e Competência Internacional: alguns aspectos. Lisboa: Jurua, 2010, p. 49

[493] Todavia, se um desses elementos está relacionado com Portugal, a lei portuguesa é considerada competente para julgar o crime. A Lei n.º 109/2009 do Cibercrime tem um critério expansivo, de criação do maior número possível de critérios para aplicarmos a lei portuguesa. De facto, basta que o agente este domiciliado em um dos paises membros da EU "para que esse país se declare competente internacionalmente para conhecer da demanda, de acordo com a leitura do art. 2º do Regulamento de Bruxelas I, pouco importando onde esteja situado o servidor ou a partir de onde o demando acedeu à rede se compudadores" (ROBERTO, Wilson – DANO TRANSNACIONAL E INTERNET. Direito Aplicável e Competência Internacional: alguns aspectos. Lisboa: Jurua, 2010, p. 81)

[494] ROBERTO, Wilson – Op. cit., p.50

[495] Rede gerida a partir do seu próprio pacote de *software* e que permite o acesso à Internet anonimamente. Mais especificamente, o Tor esconde a origem e o destino do tráfego da Internet, fazendo com que os outros não descubram quem você é e o que está vendo *online*.

[496] SIMAS, Diana – O CIBERCRIME, p. 156 "Face a esta situação muitos países passaram a exigir que nestes locais seja obrigatória a identificação do utilizador."

[497] PAEZ, Juan; ACURIO, Santiago, DERECHO Y NUEVAS TECNOLOGÍAS, p. 230

v. Ausência de tratados de extradição, acordos de ajuda mútua e mecanismos sincronizados que permitam a implementação da cooperação internacional.

Pode ainda haver um desfasamento temporal entre o momento em que o agente atua, e o momento em que um *software* produz um determinado resultado. Isto coloca problemas ao nível da determinação do momento da prática do facto, porque a sua atuação está fragmentada. Isto acontece com os ataques de Bombas Lógicas ou cronológicas,[498] o que precisa que o ataque seja planeado antes, e é até possível que o agente que está cometendo o ataque esteja realizando outra atividade diferente e incompatível com o ataque no momento em que é executado[499], por isso, dizemos que o crime informático ultrapassa as fronteiras físicas, e também as temporais.

Uma outra questão do crime informático é a sua facilidade de repetição. Isto tem a ver com o próprio surgimento de informática, que surgiu para a execução de tarefas repetitivas ou automaticamente pela própria máquina muitas vezes sem um *input* humano. E aqui não estamos a falar em sistemas inteligentes com certo grau de autonomia, estamos a falar daquilo que é mais comum nos computadores, podemos pôr um alarme a todos os dias e tentar aceder ao *email* de uma pessoa com uma senha nova.

É possível que o agente modifique um programa informático para realizar uma atividade ilegal em benefício de ele ou de terceiros e estabelecer uma rotina com o *software,* para o programa se possa modificar automaticamente, deixando o programa como foi no começo, uma vez que o ataque tenha sido realizado. Desta forma, nem visualmente, nem com a análise do programa, nem com estudos do processo, seria possível detetar o que aconteceu e como o ato foi cometido.[500]

É claro que em todos os casos a que estamos nos referindo, há um ataque a um bem jurídico protegido, sem embargo, a questão se concentra em saber se há ou não responsabilidade criminal, se a ação mal-intencionada pode ser identificada ou não.

---

[498] (*logia bombs*) Definido no subcapítulo 4.2. A CLASIFICAÇÃO DO CRIME INFORMÁTICO. "...É a execução de um programa em um determinado momento ou periodicamente num computador para a perpetração de um ato malicioso não autorizado."

[499] DAVARA RODRÍGUEZ., Miguel Á. – Manual de Derecho informático. 11ª, p. 400

[500] DAVARA RODRÍGUEZ., Miguel Á. – Manual de Derecho informático. 11ª, p. 401

CAPITULO V

VALOR PROBATORIO NO CRIME INFORMÁTICO

Não vale a pena criminalizar determinados atos se depois não houver formas possíveis de provar a ocorrência dos mesmos, isto pressupõe um regime processual que no caso português está contido na Lei n.º 109/2009 o qual instaurou novos meios de investigação e produção de prova no Capitulo III, com os arts.º 11 a 19 ao considerar disposições processuais que indicam em que situações e de que forma os dados informáticos devem ser utilizados para facilitar as investigações criminais, pelo que instaura os limites para o acesso de entidades públicas ou privadas às informações pessoais ou sensíveis e determina o tipo de dados que podem ser usados na prossecução dum processo legal. Assim temos:

Art. 11º- Âmbito de aplicação das disposições processuais
Art. 12º - Preservação expedita de dados;
Art. 13º - Revelação expedita de dados de tráfego;
Art. 14º - Injunção para apresentação ou concessão de acesso a dados;
Art. 15º - Pesquisa de dados informáticos;
Art. 16º - Apreensão dos dados informáticos;
Art. 17º - Apreensão de correio eletrónico e registos de comunicações de natureza semelhante;
Art. 18º - Interceção de comunicações;
Art. 19º - Ações encobertas.

Aliás, encontraremos preceitos assentes em outras legislações para a investigação do crime e a prova como é a Lei respeito à obtenção da prova, a Lei da Cooperação Judiciária Internacional em matéria penal, a Lei da Proteção Dados Pessoais, a Lei de conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas, e o Código de Processo Penal de Portugal.[501]

Nesse sentido, para utilizar convenientemente as provas, é necessário obter de maneira adequada os indícios e as evidências necessárias que serviram de base para o cometimento do delito, por isso, será importante observar a função que o sistema informático cumpriu, com a intenção de identificar onde deve ser localizado e como a prova deve ser usada. Isso, por sua vez, dependerá, se for um elemento material de um sistema informático como o *hardware*, ou as informações nelas contidas.

[501] Em particular os art.º 187 (Admissibilidade), 188 (Formalidades das operações), e 189 (Extensão) do Código de Processo Penal de Portugal.

Fazemos uma breve distinção entre evidência e prova na informática. De maneira geral, uma evidência é o estágio anterior duma prova e, nem sempre, a evidência se tornará uma prova. Uma evidência na área da informática é um elemento bruto, como um disco rígido, um *hardware*, uma memória USB, um telefone celular, um CD-ROM, uma página da Internet, um *software,* etc., que ainda não passou pelos processos de identificação, aquisição, preservação e análise, para o qual deve ser submetida antes de se tornar prova.[502]

Em opinião de ARMANDO DIAS RAMOS a prova digital é: "informação passível de ser extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações. (...) [a] prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta."[503]

ANABELA GONÇALVES, sobre isso, explica que a prova digital "pode ser definida como qualquer tipo de informação com valor probatório armazenada ou transmitida em sistemas informáticos sob a forma binária, e que possa ser valorada em processo judicial."[504]

Com a prova digital procura-se demonstrar a verdade, ao reunir indícios que permitam concluir pela prática (ou não) de determinados factos que preencham crimes. Dado isso, é importante investigar que tipo de crime ocorreu, quando e onde, quem e em que circunstâncias foi praticado, bem assim, os elementos que constituem a prova digital e os meios que intervieram para a sua reprodução, a fim de esclarecer qualquer dúvida que possa levar a uma falta de afirmação da origem ou destino dos indícios e dos vestígios da infração.

Desta maneira vemos que a investigação criminal no ambiente eletrónico digital impõe novas exigências, desafios e adaptações no processo penal, uma vez que se considera essencial ter em conta as características específicas das provas digitais que, em muitos casos, podem revelar a natureza particularmente complexa da mesma, para a sua obtenção e transmissão a fim poder suster as ações

---

[502] RUBIO ALAMILLO, Javier - Diferencias entre evidencia informática y prueba informática. [Em linha], Blog. 16/08/2018 [Consult. 22 Ago. 2018]. Disponível na internet: https://peritoinformaticocolegiado.es/blog/diferencias-entre-evidencia-informatica-y-prueba-informatica/

[503] Cit. por COSTA, Catarina - As proibições de prova e a prova digital – aproximação aos *lugares - comuns* de um instituto clássico em face de uma nova realidade. Braga: Escola de Direito da Universidade do Minho, 2017. Dissertação de Mestrado, p. 73

[504] GONÇALVES, Anabela - PECK NEWS: GLOBAL TRENDS. Artigos e Entrevistas 5° CONGRESSO INTERNACIONAL DIREITO NA LUSOFONIA [Em linha]. Março 2018. [Consult. 3 Set. 2018]. Disponível na internet: http://www.peckadvogados.com.br/publicacoes/artigos-e-entrevistas/peck-news-global-trends-9

criminosas na investigação, maior, enquanto a prova digital é frágil e volátil, pois, pode ser facilmente alterada, adulterada ou eliminada sem deixar vestígios.[505]

Nesse enquadramento, as principais características da prova digital como identifica ANABELA GONÇALVES[506], são:

I. **Frágil e alterável** – Ainda com o uso da criptografia e outros mecanismos que garantem a autenticidade, integridade e disponibilidade das informações, um grande desafio é verificar se a mesma foi ou não comprometida;
II. **Instável** – Por a sua mutabilidade, indica, que a mesma se modifica ou altera, de forma parcial ou total.
III. **Aparente imaterialidade** – Não é suscetível de apreensão material, por ser um impulso elétrico estruturado num código binário que forma uma sequência numérica impalpável, ou melhor, não é composto de matéria, por isto, apenas a apreensão é de dados informáticos intangíveis.
IV. **Duplicável** - Ao lidar com informações digitais, compostas de bits de informação, é possível reproduzir essas mesmas informações em vários meios diferentes sem alterar a prova original. Com isso, obtemos uma prova original intacta
V. **Efémera**, temporária ou volátil – Em alguns casos não tem a durabilidade suficiente para a sua "cristalização"; Elas podem ser perdidas rapidamente quando o equipamento eletrónico é desligado, como por exemplo, quando a evidência está numa memória RAM, e portanto devem ser recuperadas rapidamente.
VI. **Dispersa** – É difícil localizar, por se encontrar em vários locais virtuais dentro de um mesmo sistema informático (como ficheiros de imagem, áudio, vídeo, e-mail, dum computador, ou de vários utilizadores dum computador), mas também numa vasta área espacial ou geográfica ao longo de diversos sistemas informáticos (como routers ou vários fornecedores de serviços de tráfego de dados ou de armazenamento) espalhados pelo mundo.
VII. **Carácter dinâmico com os sistemas informáticos** – torna-se necessário analisar, distintos espaços de tempo, por quanto o estado da prova digital pode evoluir ou mudar através do tempo, além de que há IPs[507] dinâmicos[508] que acentuam as dificuldades na identificação.
VIII. **Indefinição da autoria** – em ocasiões nas evidências digitais os únicos dados que podemos obter para identificar aos usuários são mascarados com técnicas de anonimização ou ocultação da origem.

---

[505] MONTE, Mário [et al.]; - Direito na lusofonia. Cultura, direito humanos e globalização. 1° Congresso. Braga: Escola de Direito da Universidade do Minho, Março de 2016, p. 340

[506] GONÇALVES, Anabela - PECK NEWS: GLOBAL TRENDS. Artigos e Entrevistas 5° CONGRESSO INTERNACIONAL DIREITO NA LUSOFONIA [Em linha]. Março 2018. [Consult. 3 Set. 2018]. Disponível na internet: http://www.peckadvogados.com.br/publicacoes/artigos-e-entrevistas/peck-news-global-trends-9

[507] Endereços IP (IP é um acrônimo para Internet Protocol) são um número único e irrepetível com o qual um computador ou equipamento eletrónico conectado a uma rede que executa o protocolo IP é identificado

[508] A maioria dos dispositivos usa endereços IP dinâmicos atribuídos a eles pela rede quando se conectam. Esses endereços IP são temporários, não estão atribuídos de forma permanente a um utilizador e portanto, podem mudar com o tempo.

Com o auxílio das técnicas científicas e analíticas especializadas à infraestrutura tecnológica como a perícia forense computacional, é possível identificar, preservar, analisar e apresentar dados que sejam válidos dentro de um processo legal, obtendo o mecanismo ideal para localizar e apresentar adequadamente os factos jurídicos informáticos que sejam relevantes numa investigação civil ou criminal,[509] uma vez que, permitirá coletar as mensagens de dados existentes num equipamento informático, preservá-las e filtrá-las de tal maneira que todas essas informações digitais possam servir de prova. Ainda assim, hã que considerar que nos processos judiciais, a prova digital apresenta problemas jurídicos complexos ligados ao direito à privacidade e ao sigilo das comunicações, e os possíveis efeitos em terceiros.

A evidência digital pode ser obtida de *laptops* ou *desktops*, Tablet ou diários eletrónicos, telefones celulares, servidores de rede, registros em redes de informática, impressoras, localizador de pessoas, GPS, fax, memória flash, gravadores e, em geral, qualquer suporte material, dispositivo eletrónico ou *hardware* entre eles "a Internet das coisas"[510] que possam armazenar alguma informação ou que possa interagir com uma rede de informação eletrónica ou um sistema de informação.

O investigador precisará de uma ordem judicial para poder apreender os bens que contêm a informação digital, bem como para poder rever o seu conteúdo, uma vez que a falta da ordem de apreensão que proteja as ações da Polícia Judiciária ou do órgão de investigação pode terminar com a exclusão dos elementos probatórios pela violação das garantias constitucionais.[511]

Também é importante respeitar os procedimentos técnicos e legais preestabelecidos nas fases da investigação forense, ou seja, a coleta, a preservação, a filtragem e a apresentação das provas, uma vez que o órgão judicial não pode basear as suas decisões numa prova viciada.

Na fase de coleta, o investigador forense deve discernir qual evidência é relevante e necessária, dependendo do tipo de crime cometido, a fim de decidir quais são os objetos que têm valor para coletá-los, rotulá-los, embalá-los e inventá-los, garantindo, assim, a cadeia de custódia.

---

[509] PAEZ, Juan; ACURIO, Santiago, DERECHO Y NUEVAS TECNOLOGÍAS. 1ª. Equador, p. 285

[510] É uma rede de objetos físicos como veículos, máquinas, aparelhos, simplesmente sapatos, móveis, malas, dispositivos de medição, biossensores, ou qualquer coisa que podemos imaginar que usa usando sensores e API para conectar e trocar dados numa rede de dados eletrónica como a Internet.

[511] PAEZ, Juan; ACURIO, Santiago, Op. Cit. 1ª., p. 293

Na preservação procura-se proteger os objetos coletados que tiveram valor probatório, de maneira que estes permaneçam em forma completa e verificável, usando técnicas de encriptação como códigos de integridade ou de função *hash.*[512]

Na filtragem, o investigador com a ajuda das ferramentas e as técnicas específicas da informática, realizará uma análise das evidências recolhidas e preservadas para determinar qual delas têm valor como prova e portanto são relevantes.

Finalmente, na apresentação da prova, esta deve ser entendível, para o qual se recomenda o uso de uma terminologia compreensível para o Ministério Público e o juiz, limitando o uso de termos técnicos; De mais a mais, o investigador deve ser convincente explicando os procedimentos e técnicas utilizadas na coleta, preservação e filtragem das evidências, com a intenção de criar certeza e, consequentemente, credibilidade dentro da investigação.

Na Europa, poucos países possuem procedimentos específicos para obtenção e processamento de evidências digitais. Por exemplo, na Grã-Bretanha e na Romênia há um procedimento para obter evidências digitais formadas por regras internas da polícia.[513]

A existência de normas que regulam evidências digitais com um âmbito global, como a norma ISO/IEC 27037: 2012 T *"Information Technology – Security Techmiques – Guidelines for identification, colletion, acquisition and presercation of digital evidence"*, que faz parte da série ISO/IEC 2700, constituem um conjunto de padrões desenvolvidos pela ISO e IEC que fornecem uma estrutura de segurança da informação para todos os tipos de organizações, independentemente da sua natureza pública ou privada. Por este motivo, trata-se de um documento de referência com alcance global, que contribui à realização da perícia forense computacional, fornecendo orientações para manejar as evidências digitais, tais como: identificação, coleta, aquisição e preservação,[514] com a intenção de manter a integridade e autenticidade das provas digitais e sua conseqüente admissibilidade no tribunal. [515]

---

[512] Função de hash: Desenvolvido no Capítulo II TÉCNICAS INFORMÁTICAS QUE VISAM PROTEGER OS DADOS PESSOAIS.

[513] Cit. por SANCHIS, Carolina **dir.** – Fraude electrónico: Su gestión penal y civil. P. 222

[514] Esta norma ISO 27037 não entra na fase de Análise da evidência.

[515] SANCHIS, Carolina **dir.** – Fraude electrónico: Su gestión penal y civil. P. 224

Os princípios básicos nos quais a norma ISO 27037 baseia-se são:

I. Aplicação de Métodos: A prova digital deve ser adquirida da maneira menos intrusiva possível, tentando preservar a originalidade da prova e, na medida do possível, obter cópias de segurança.
II. Processo auditável: Os procedimentos seguidos e a documentação gerada devem ter sido validados e contrastados por boas práticas profissionais. Vestígios e evidências do que foi feito e os seus resultados devem ser fornecidos.
III. Processo reproduzível: Os métodos e procedimentos aplicados devem ser reproduzíveis, verificáveis e discutíveis no nível de compreensão dos especialistas na área, que podem dar validade e apoio às ações tomadas.
IV. Processo Defensável: As ferramentas usadas devem ser mencionadas e devem ter sido validadas e contrastadas no seu uso para o propósito em que são usadas no desempenho.

Para cada tipo de dispositivo, a norma divide como agir ou como deveram ser tratadas, em três processos diferenciados como um modelo genérico para o tratamento de evidências:

I. Identificação: consiste em localizar e identificar as possíveis informações ou elementos de evidência no seu estado físico ou lógico, como é o caso de cada evidência.
II. Coleta e/ou Aquisição: Esse processo é definido como a coleta dos dispositivos e a documentação (apreensão e sequestro dos mesmos) que podem conter as evidências a serem coletadas ou a aquisição e cópia das informações existentes nos dispositivos.
III. Conservação / Preservação: A evidência deve ser preservada para garantir a sua utilidade, ou seja a sua originalidade, para que posteriormente possa ser admissível como um elemento de prova original e completo, portanto, as ações desse processo visam preservar a Cadeia de Custódia, a integridade e a originalidade da prova.

A falta de pessoal qualificado, com preparação suficiente na área de investigação forense computacional, bem como a falta de prática para obter, coletar, documentar e depois analisar e

interpretar as evidências digitais, dificultaria a condenação de um sujeito do qual se presume a culpa ou, pelo contrário, poder-se-ia sentenciar a quem é inocente. Portanto, o fator de formação na aquisição dos conhecimentos específicos é fundamental e determinante para atingir o objetivo proposto.

Além disso, é aconselhável levar em conta que quando numa cena de crime trabalha-se em condições adversas, como inundações, incêndios, derramamentos produtos químicos ou perigosos, é essencial que o investigador tome as medidas de segurança necessárias para garantir a sua integridade física, logo devera implementar o procedimento mais apropriado para aumentar as possibilidades de recuperar as evidências da maneira mais completa.[516]

Da mesma forma, o investigador ao dar testemunho deve transmitir com absoluta certeza que as provas apresentadas não foram alteradas, modificadas ou criadas por terceiros durante a investigação que conduziu. De resto, deve explicar que o equipamento informático onde a informação foi encontrada pertence ao agente, com base na cadeia de custódia da equipe, uma vez que a sua apreensão tenha sido ordenada.

A prática desses meios de prova será caracterizada por um ato de reprodução em tribunal, onde vai ser reproduzida a gravação se houver, assim como as informações armazenadas ou contidas no suporte para torná-la acessível aos sentidos e, em última análise, ao entendimento humano do juiz, a fim de obter a sua convicção sobre a certeza dos factos discutidos. Com esta reprodução se persegue, exteriorizar a realidade que foi capturada por escrito, sinais e símbolos, como tal, em um determinado momento, já irrepetível.[517]

[516] PAEZ, Juan; ACURIO, Santiago, Op. cit. 1ª. Equador, p. 300

[517] ORDOÑO ARTÉS, C. - El Avance Tecnológico y los Nuevos Medios de Prueba en la Ley de Enjuiciamiento Civil. Régimen Jurídico de Internet. 2da Edição, Madrid: En LA LEY-ACTUALIDAD S.A. 2002, p. 504

CONCLUSÕES

A evolução da tecnologia da informação e o seu uso nos últimos anos são alguns dos fenômenos que mais afetaram a mudança social vertiginosa que estamos vivenciando e, entre elas, a maneria fácil de comercializar bens e serviços e, consequentemente, a forma de fazer o pagamento à distância, contribuindo ao desenvolvimento da chamada economia digital. Factos que causaram, por sua vez, alguns problemas jurídicos, no que respeita à privacidade e proteção de dados pessoais, incluindo aqueles relacionados aos dados pessoais de pagamento no comércio eletrónico, pelo seu mau uso, o qual pode afetar não só ao património do titular, senão também, a sua privacidade.

Isso motivou, o estudo por um lado das técnicas informáticas que visam proteger os dados pessoais, e por outro, a proteção jurídica em pagamentos à distância com moeda eletrónica e a sua relação com o crime informático, permitindo identificar os elementos técnicos de confiança que contribuem ao desenvolvimento do comércio eletrónico e da segurança jurídica pelo uso dos meios de pagamento à distância neste mundo tecnológico, onde uma grande parte das transações do comércio ágil e competitivo de nossos dias, são realizadas por meios eletrónicos.

Assim, tentamos esclarecer neste trabalho, que com a progressiva evolução dos sistemas computacionais, o desenvolvimento das transações feitas através da Internet podem afetar os direitos fundamentais das pessoas ligadas numa rede, pelo que requerem, como é essencial, que as transações sejam asseguradas de forma preventiva contra os fraudes informáticos, ataques à privacidade e o uso não autorizado de dados pessoais, buscando, em primeiro lugar, a regulamentação normativa dos mecanismos e as soluções tecnológicas que atinjam a autenticação, a confidencialidade, a integridade, e não repúdio das transações comerciais realizadas, a fim de concluí-las de maneira satisfatória. A partir daí, fica evidente o desenvolvimento de tecnologias compatíveis com o direito.

E depois, a regulamentação normativa dos aspetos jurídicos, e a sua periódica atualização, que promovam os princípios da proteção de dados, a legitimidade, a proporcionalidade dos dados recolhidos e transparência dos mesmos, assim como, o respeito aos direitos humanos, com o objetivo de garantir o direito à Autodeterminação Informacional, cara às tecnologias de ambientes inteligentes e a

disponibilização e troca de dados entre vários sistemas, aparelhos e bases de dados, que têm permitido a vigilância e monitorização contínua das pessoas interferindo na privacidade de elas.

Disso resulta, que a obrigação geral de retenção de dados pessoais e a sua conservação deve ser proporcional de acordo com as finalidades da recolha e do tratamento, de modo a evitar uma apropriação perpétua dos dados numa sociedade democrática, o que permite limitar ao mínimo a interferência necessária dos direitos fundamentais das pessoas titulares dos dados. Contudo, estamos cientes que o objetivo de combater a criminalidade grave implica sérios riscos decorrentes desta obrigação, mas, não podemos esquecer os direitos legalmente consagrados do titular dos dados, como o direito ao esquecimento e o direito a ser deixado só. Ele permitirá a supressão sem demora injustificada no caso em que os dados não são necessários, retire-se o consentimento, oponha-se ao tratamento, ou que seus dados tenham sido tratados de forma ilegal, entre outros.

Nesse cenário, a notícia do novo Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho relativa à proteção das pessoas no que respeita ao tratamento de dados pessoais e à livre circulação desses dados (RGPD), vem completar as diretrizes anteriores para criar procedimentos mais seguros. Por isso, notamos que a normativa da União Europeia de Proteção de Dados Pessoais buscam evitar os riscos associados ao uso do elemento tecnológico, os quais provocam danos físicos, materiais ou imateriais às pessoas singulares, assim como a perda de controlo sobre os seus dados pessoais, e a limitação dos seus direitos, ao ser objeto de discriminação, roubo ou usurpação da identidade, ademais das perdas financeiras, os danos à reputação, e a perda de confidencialidade dos dados pessoais protegidos pelo sigilo profissional.

De todo modo, as reflexões jurídicas devem considerar ainda mais, o plano físico e o virtual na sua interface, rumo a uma perceção jurídica mais sofisticada. O pensamento jurídico conservador deve ir além do materialismo e dogmatismo que o caracteriza, a fim de contribuir à ampliação do horizonte mental dos juristas, permitindo-lhes uma compreensão mais coerente com a realidade social atual, que requer uma mistura das ciências para o desenvolvimento do homem.

Vale destacar, mais uma vez, que se estabelece a necessidade duma harmonização ou uniformização das leis internacionais relacionadas à tecnologia da informação, a transferência de dados eletrónicos transfronteiriços e ao cibercrime, assim, como a eficácia dos mecanismos legais que regulam

e aplicam de maneira concreta e concisa ou que foi acordado em leis internacionais, especialmente, em relação à cooperação internacional contra os crimes informáticos.

Estas leis internacionais devem assegurar às pessoas singulares o mesmo nível de direitos suscetíveis de proteção judicial em todos os Estados - membros, e impor obrigações equivalentes aos responsáveis pelo tratamento (incluindo as micro, pequenas e medianas empresas), e aos seus subcontratantes, que assegurem um controlo coerente do tratamento dos dados pessoais, com sanções iguais, bem como uma cooperação efetiva entre as autoridades de controlo. A referida proteção de dados deve-se aplicar a qualquer informação relativa a uma pessoa singular identificada ou identificável, incluindo os dados pseudonimizados que possam ser atribuídos a uma pessoa singular identificável, considerando os meios suscetíveis de ser razoavelmente utilizados para identificar direta ou indiretamente a essa pessoa.

Essa segurança técnica e legal que buscamos, não deve nascer apenas como uma obrigação daqueles que tratam os dados como forma de garantir os direitos dos usuários, senão, que os usuários também devem implementar os seus próprios mecanismos de defesa da privacidade e controle da sua informação. Lembremos que o autocuidado dos usuários, sempre ajudaram a garantir a intimidade dos dados.[518]

Muitas das empresas atuais foram criadas, baseadas na dependência de sistemas informáticos e dos meios modernos de pagamento, que se tornaram particularmente vulneráveis, devido em grande parte às características do tratamento telemático. No entanto, apesar do fato de que os atuais meios de proteção são insuficientes, ao menos nos Estados-Membros da EU, e portanto em Portugal, note-se que a defesa na proteção de dados pessoais de pagamento favorece ao titular, contra o uso indevido dos mesmos e contra as cláusulas escuras em contratos de pagamento à distância. Sem embargo, será necessário utilizar todos os métodos que a tecnologia disponibiliza para reduzir a burla e o uso indevido de dados nesses tipos de pagamentos, garantindo a identificação das partes, do ponto de vista físico e lógico nas transações.

---

[518] "Como bem refere Antoni Roig, os investigadores da área tecnológica tenderão a deslocar a protecção da privacidade para as mãos dos indivíduos fornecendo-lhes mecanismos e ferramentas tecnológicas de protecção de direitos. (...) [onde] a eficácia dos direitos dependerá cada vez mais das escolhas e comportamentos dos individuos." (Cit. por MONTE, Mario; BRANDÃO, Paulo; **Coord.(s)** - DIREITOS HUMANOS E SUA EFETIVAÇÃO NA ERA DA TRANSNACIONALIDADE. Debate Luso-Brasileiro. Comunicações Eletrónicas e Diretos Humanos: O Perigo do "Homo Conectus" Curitiba: Juruá Editora, 2012, P.224)

No âmbito internacional, a lei criminal sobre crimes informáticos, é caracterizada por diferentes formas de ser regulada, para combater este flagelo que se torna cada vez maior, assim, alguns países adotaram pela sanção em leis especiais, onde há casos que incorporam os seus próprios conceitos, os princípios, a parte criminal material, a parte processual criminal, e até os órgãos ou as instituições dedicadas à sua investigação e perseguição. Outros países (a maioria) optaram por modificações parciais nos seus Códigos Penais atuais, adaptando as figuras criminais clássicas para possibilitar a sua aplicação no Cibercrime.

Considerando a transnacionalidade do crime informático, no que diz respeito à lei aplicável para julgar a responsabilidade civil pela violação dos direitos de personalidade em Portugal, esta é determinada pela lei do país onde decorreu a principal atividade causadora do prejuizo,[519] pelo qual, o legislador portugues adotou a tese da *Lex Loci Delicti Commissi.* No entanto, a ocorrência dessas situações, na sua maioria, envolvem delitos transnacionais por meio da Internet, o que limita a possibilidade da acusação criminal, sendo quase impossível determinar qual é o local onde o agente conetou o facto criminal, de modo que a tese não é a mais adequada, Em oposição, temos a tese do lugar de residência habitual da parte lesada que oferece maiores possibilidades para o julgamento do crime, desde que seja permitida uma flexibilidade para aplicar uma outra lei.

No concernente às provas digitais, estes são um aspeto fundamental na luta contra a criminalidade informática, por isso é importante fazer maiores esforços para estabelecer procedimentos adequados, como a adoção da norma ISO 27037: 2012, a fim de contribuir para a padronização global das normas eletrónicas que regulam os meios de obtenção das provas digitais, e convencionar sobre esta matéria, papéis, metodologia e uma linguagem comum, como resultado da evolução jurídica testada.

Por fim importa referir, que com a ajuda de modernos e atualizados laboratórios de investigação por parte dos órgãos auxiliares da justiça e através de uma capacitação eficiente para aqueles que devem investigar essas condutas, bem como o pessoal encarregado de administrar a justiça, muito progresso seria feito no caminho da proteção dos dados pessoais de pagamento utilizados no comércio eletrónico.

[519] Art.° 45 n.° 1 do Código Civil português

BIBLIOGRAFIA[520]

DOUTRINA, LIVROS, PUBLICAÇÕES PERIÓDICAS, TESES EM GERAL

1. ANDRADE, Francisco António Carneiro Pacheco de – **DA CONTRATAÇÃO ELECTRÓNICA – EM PARTICULAR DA CONTRATAÇÃO ELECTRÓNICA INTER-SISTÉMICA INTELIGENTE**. Braga: Universidade do Minho, 2008. Tese de Doutoramento 2008.

2. AZEVEDO, Ana – **Burlas Informáticas: Modos de Manifestação**. Braga: Universidade de Minho, 2016. Dissertação de Mestrado.

3. BARBIERI, Diovanna – **A PROTEÇÃO DO CONSUMIDOR NO COMÉRCIO ELETRÓNICO**. Lisboa: Juruá, 2013. ISBN: 978-989-712-206-4

4. BARRETO, Ricardo – **DIREITO & REDES SOCIAIS NA INTERNET**: A proteção do consumidor no comércio eletrónico. 2ª. Curitibia: Juruá, 2014. ISBN: 978-85-362-4889-9

5. BERNABÉ, Franco – **LIBERDADE VIGIADA:** Privacidade, segurança e mercado na rede. Rio de Janeiro: Sinergia, 2013. ISBN: 978-85-7947-211-4

6. BOTANA GARCIA, Gerna Alejandra. Coord. – **COMERCIO ELECTRONICO Y PROTECCION DE LOS CONSUMIDORES.** Madrid: La Ley, 2001. ISBN: 84-9725-158-X

7. CASTRO, Catarina Sarmento - **O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro**. Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa. [Em linha]. Coimbra: 2005. [Consult. 21 janeiro 2018] Disponível na internet: http://www.egov.ufsc.br/portal/sites/default/files/anexos/5544-5536-1-PB.pdf

8. CORREIA, Eduardo – **A Teoría do Concurso em Direito Criminal**. 2ª, Coimbra: Almedina, 1996.

9. CORREIA, Victor – **SOBRE A PRIVACIDADE.** Óbidos: Sinapis, 2016. ISBN: 978-989-691-563-6

10. COSTA, Catarina - **As proibições de prova e a prova digital** – aproximação aos *lugares - comuns* de um instituto clássico em face de uma nova realidade. Braga: Escola de Direito da Universidade do Minho, 2017. Dissertação de Mestrado

11. DA MATTA, Caeiro – **Direito Criminal Português.** II, Coimbra: F., França Amdado. 1911. Pressupostos 11ª. Navarra: Aranzadi. 2015. ISBN 978-84-9098-750-6

12. DAVARA RODRÍGUEZ., Miguel Á. – **Manual de Derecho informático**. 11ª, Madrid: Aranzadi. 2015. 978-84-9098-750-6

[520] De acordo com a Norma Portuguesa de descrição bibliográfica (Np 405).

13. DE LA CUESTA ARZAMENDI, José L. **(Dir.) [et al.]** – **Derecho Penal Informático**. Navarra: Aranzadi, 2010. ISBN 978-84-470-3429-1

14. DEL PESO NAVARRO, EMILIO.- **Servicios de la Sociedad de la información (comercio electrónico y protección de datos). Madrid:** Díaz de Santos, S.A. 2013. ISBN 9788479785604

15. DEL PINO, Santiago - **Delitos Informáticos: Generalidades.** [Em linha]. Ecuador [Consult. 21 maio 2017] Disponível na internet: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

16. ESTRADA, Manuel. **O comércio de dados pessoais dos trabalhadores pelas empresas de tecnologia e pelos governos através da invasão da privacidade e da intimidade**. Revista de Direito do Trabalho. vol. 172. ano 42. p. 35-54. São Paulo: Ed. RT, nov.-dez. 2016.

17. GUIMARÃES, Maria - **As transferências eletrónicas de fundos e os cartões de débito: alguns problemas jurídicos relacionados com as operações de levantamento.** Coimbra: Almedina, 1999.

18. GUIMARÃES, Maria – **Separata Infrações Económicas e Financeiras. Estudos de Criminologia e Direito.** A fraude no comércio electrónico: O problema da repartição do risco por pagamentos fraudulentos. Coimbra, 2015

19. KUROSE, James e ROSS Keith; **REDES DE COMPUTADORES E A INTERNET: Uma abordagem Top-down**. 5ta. Brasil: Pearson, 2010. ISBN: 978-85-88639-97-3

20. LÓSCIO, Bernadette. HARA, Carmem. Martins Vidal. (**Orgs**.) **[et al.]**; - **Tópicos em Gerenciamento de Dados e Informações 2014**. 1a, Curitiba: Sociedade Brasileira de Computação – SBC. 2014. ISBN 978-85-7669-290-4

21. MACEIRA, Irma – **A PROTEÇÃO DO DIREITO À PRIVACIDADE FAMILIAR NA INTERNET**. Rio de Janeiro: Lumen Jurís, 2015. ISBN: 978-85-8440-179-6

22. MONTE, Mário **Coord.** [et al.]; - **Direito na lusofonia. Cultura, direito humanos e globalização.** 1º Congresso. Braga: Escola de Direito da Universidade do Minho, Março de 2016. ISBN 978-989-97970-7-9

23. MONTE, Mario; BRANDÃO, Paulo; **Coord.(s)** - **DIREITOS HUMANOS E SUA EFETIVAÇÃO NA ERA DA TRANSNACIONALIDADE. Debate Luso-Brasileiro**. Coumicações Eletrónicas e Diretos Humanos: O Perigo do "Homo Conectus" Curitiba: Juruá Editora, 2012. ISBN 978-85-362-3948-4.

24. ORDOÑO ARTÉS, C. - **El Avance Tecnológico y los Nuevos Medios de Prueba en la Ley de Enjuiciamiento Civil**. Régimen Jurídico de Internet. 2da Edição, Madrid: En LA LEY-ACTUALIDAD, 2002.

25. PAEZ, Juan; ACURIO, Santiago, **DERECHO Y NUEVAS TECNOLOGÍAS.** 1ª. Ecuador: Corporación de Estudios y Publicaciones, 2010. ISBN: 978-9978-86-920-8

26. PALAZZI, Pablo - **DELITOS INFORMATICOS**. 1ra. Buenos Aires. 2000.

27. PINHEIRO, Alexandre – ***Privacy*** **e Protecção de dados pessoais; a contrução dogmatica do direito à identidade informacional**. Lisboa: Alameda da Universidade, 2015.

28. PLAZA PENADÉS, Javier **(Dir.) [et al.]** – **DERECHO Y NUEVAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN**. 1ª. Navarra: Aranzadi, 2013. ISBN: 978-84-9014-399-5

29. ROBERTO, Wilson – **DANO TRANSNACIONAL E INTERNET.** Direito Aplicável e Competência Internacional: alguns aspectos. Lisboa: Jurua, 2010. ISBN 978-989-8312-68-6

30. RODRIGUEZ, ALONSO e LASCURAÍN - **DERECHO PENAL E INTERNET**. Régimen Jurídico de Internet. 2da. Madrid: En LA LEY-ACTUALIDAD S.A., 2002

31. RUIZ Miguel, C., **[et al.];- Temas de Direito da Informatica e da Internet.** 1ª ed. Coimbra: Editor Coimbra. 2004.

32. SANCHIS, Carolina **dir.** – **Fraude electrónico: Su gestión penal y civil**. Valencia: Tirant Lo Blanch, 2015. ISBN 978-84-9086-556-9

33. SANTOS, Manuel e LEAL-HENRIQUES, Manuel **– Noções Elementares de Direito Penal**. 2.ª Lisboa: Rei dos Livros, 2003, ISBN: 972-51-1046-3

34. SANTOS, Rita, **O Tratamento Jurídico-Penal da Transferência de Fundos Monetários Através da Manipulação Ilícita dos Sistemas Informáticos**. Studia Jurídica, n.º 82. s.l.: Coimbra Editora, 2005.

35. SILVEIRA, Alessandra; MARQUES, João. **DO DIREITO A ESTAR SÓ AO DIREITO AO ESQUECIMENTO. CONSIDERAÇÕES SOBRE A PROTEÇÃO DE DADOS PESSOAIS INFORMATIZADOS NO DIREITO DA UNIÃO EUROPEIA: SENTIDO, EVOLUÇÃO E REFORMA LEGISLATIVA**. Revista da Faculdade de Direito – UFPR, vol. 61, n. 3, Curitiba: set./dez. 2016, p. 91 – 118

36. SIMAS, Diana – **O CIBERCRIME.** Lisboa: Universidade Lusófona de Humanidades e Tecnologias, 2014, Dissertação de Mestrado.

37. TEIXEIRA, Angelina – A Chave para a Regulamentação da Protecção de Dados – **DATAVENIA,** Revista Jurídica Digital. Ano 4 No.6. s.l:s.n., 2016. pag. 5-32

38. TÉLLEZ Valdés, Julio - **Derecho Informático**. 4ta. México: McGRAW-HILL/INTERAMERICANA. 2008 ISBN-13: 978-970-10-6964-6

39. TORRES CHAVES, Efraín - **Breves Comentarios a la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.** Quito: Corporación de Estudios y Publicaciones. 2002

40. VENÁNCIO, Pedro – **Lei Do Cibercrime. Anotada e Comentada**. Coimbra: Coimbra Editora. 2011 ISBN: 978-972-32-1906-7

41. VERDELHO, Pedro; BRAVO, Rogeiro; e LOPES ROCHA, Manuel – **LEIS DO CIBERCRIME**. Vol. I. Famalicão: Centro Atlântico. 2003 ISBN: 972-8426-69-0

42. VILARIÑO PINTOS, Eduardo - **El delito informático**. Derecho comparado y aspectos jurídicos internacionales Hacia un nuevo orden internacional y europeo: homenaje al Profesor M. Díez de Velasco, Madrid, ES: Tecnos, 1993. pp. 807-826 ISBN: 84-309-2333-0

43. ZÚQUETE, André - **Segurança em redes informáticas.** 3ra. Lisboa: FCA - Editora de Informática, 2010. ISBN: 9789727226467

LEIS, DECISÕES, CONVENÇÕES

1. ACÓRDÃO DO TRIBUNAL DA RELAÇÃO DE COIMBRA de 15-10-2008**, processo nº 368/07.8TAFIG.C1,** relatora Alice Santos [Em linha] Coimbra [Consult. 19 Agosto 2018] Disponível na internet: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/ae4145b5e5a62059802574f70058c7fe?OpenDocument

2. ACÓRDÃO DO TRIBUNAL DA RELAÇÃO DE ÉVORA de 26-06-2012, **processo n.º 264/06.6GBPSR.E1** relator MARTINHO CARDOSO [Em linha] Évora [Consult. 31 Agosto 2018] Disponível na internet: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9e4d23e33c93144580257de10056f883?OpenDocument

3. ASSEMBLEA COSTITUENTE – **COSTITUZIONE DELLA REPUBBLICA ITALIANA**. [Em linha]. In Gazzetta Ufficiale, n° 298, Roma, dicembre 1947, [Consult. 15 ene 2018] Disponível na internet: https://www.senato.it/documenti/repository/istituzione/costituzione.pdf

4. ASSEMBLEIA CONSTITUINTE - **CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA**. VII Revisão Constitucional [2005] entra em vigor no dia 25 de Abril de 1976 Diário da República, n.° 155 – I Série - A, de 12 de agosto de 2005.

5. ASSEMBLÉIA DA REPÚBLICA - Lei n.° 109/2009 **Lei do Cibercrime**. [Em linha]. D.R. I Série. 179 (2009-09-15) 6319 – 6325. [Consult. 10 ene 2018] http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1137A0004&nid=1137&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=

6. ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE COSTA RICA – **Ley N.º 9048,** Reforma de la Sección VIII, Delitos Informáticos y Conexos, do Título VII del Código Penal, de 10 de julio de 2012. [Em linha]. San Jose [Consult. 24 julho 2018] Disponível na internet: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

7. ASAMBLEA NACIONAL CONSTITUYENTE - **CONSTITUCIÓN DE 1967**. **ECUADOR**. [Em linha]. Quito [Consult. 25 nov 2017] Disponível na internet: http://www.cancilleria.gob.ec/wp-content/uploads/2013/06/constitucion_1967.pdf

8. ASAMBLEA NACIONAL CONSTITUYENTE - **CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR 2008**, [Em linha]. Registro Oficial No. 449, del 20 de octubre del 2008. Ecuador. 2008. Consult. 26 nov 2017] Disponível na internet: https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

9. ASAMBLEA NACIONAL CONSTITUYENTE - **CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DEL ECUADOR**. [Em linha]. Decreto Legislativo No. 000. RO/ 1 de 11 de Agosto de 1998. Riobamba [Consult. 25 nov 2017] Disponível na internet: http://www.cancilleria.gob.ec/wp-content/uploads/2013/06/constitucion_1998.pdf

10. ASAMBLEA NACIONAL DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA - **Ley Especial Contra los Delitos Informáticos**, [Em linha]. Gaceta Oficial N° 37.313 del 30 de octubre de 2001. [Consult. 24 julho 2018] Disponível na internet: http://www.wipo.int/edocs/lexdocs/laws/es/ve/ve041es.pdf

11. ASAMBLEA NACIONAL DE LA REPÚBLICA DEL ECUADOR - **CODIGO ORGANICO INTEGRAL PENAL, COIP,** Registro Oficial Suplemento 180 de 10-feb-2014.

12. ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS - **PACTO INTERNACIONAL DOS DIREITOS CIVIS E POLÍTICOS.** (1966-12-16).

13. ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS (ONU) - Resolução No. 217 A (III). **DECLARAÇÃO UNIVERSAL DOS DIREITOS DO HUMANOS.** (1948-12-10).

14. ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS (ONU) - Resolução No. 2450 (XXIII) **DIREITOS HUMANOS E PROGRESSO CIENTÍFICO E TECNOLÓGICO .** 1968.

15. CÂMARA DE REPRESENTANTES NA HOLANDA - **Lei de 13 de Abril de 1995 que contém disposições relativas à luta contra o tráfico de seres humanos e a pornografia infantil**. [Em linha]. Dado em Châteauneuf-de-Grasse, 13 de abril de 1995. [Consult. 01 de agosto de 2018] Disponível na internet: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1995041332&table_name=wet

16. **CODE CIVIL DES FRANÇAIS** - Dernière modification le 03 janvier 2018. [Em linha]. Paris. [Consult. 29 nov 2017] Disponível na internet: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721

17. CONGRESO DE COLOMBIA – **LEY 1273 DE 2009,** por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [Em linha]. DIARIO OFICIAL Lunes 5 de enero de 2009, Edición 47.223, [Consult. 25 julho de 2018] Disponível na internet: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

18. CONGRESO NACIONAL DE ECUADOR - **Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Ley No. 67,** Registro Oficial Suplemento No. 557 del 17 de abril del 2002. Equador. 2002

19. CONGRESSO NACIONAL DE BRASIL- **CÓDIGO CIVIL**. [Em linha]. LEI Nº 10.406, DE 10 DE JANEIRO DE 2002. [Consult. 28 nov 2017] Disponível na internet: http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm

20. CONGRESSO NACIONAL DE BRASIL - **LEI Nº 11.829, DE 25 DE NOVEMBRO DE 2008**, Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. Brasilia: Diário Oficial da União - Seção 1 - 26/11/2008

21. CONGRESSO NACIONAL DE BRASIL - **LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012 (Lei Azeredo)**, Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto- Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrónico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasilia: Diário Oficial da União - Seção 1 - 3/12/2012, Página 1.

22. CONGRESSO NACIONAL DE BRASIL - **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012, (Lei Carolina Dieckmann; Lei de Crimes Cibernéticos),** dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasilia: Diário Oficial da União - Seção 1 - 3/12/2012, Página 1

23. CONGRESSO NACIONAL DE BRASIL- **MARCO CIVIL DA INTERNET.** [Em linha]. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. [Consult. 28 nov 2017] Disponível na internet: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

24. CONSELHO NACIONAL DA ÁUSTRIA - **Penal Code (Strafgesetzbuch - StGB)** [Em linha]. [Austria], 1 January 1975, [Consult. 30 Julho 2018] Disponível na internet: http:// www.refworld.org/docid/3ae6b5bf0.html

25. COMISSÃO DAS COMUNIDADES ECONÓMICAS EUROPEIAS - **Recomendação No. 81/679/CEE, relativa a uma convenção do Conselho da Europa para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**, de 29 de Julho de 1981. BRUXELAS: Jornal Oficial das Comunidades Europeias. 29.8.81. L 246/31

26. COMISSÃO DAS COMUNIDADES EUROPEIAS - COM(2005) 184 final, **Comunicação da Comissão ao Conselho e ao Parlamento Europeu, de 10 de Maio de 2005: "Programa de Haia: dez prioridades para os próximos cinco anos. Parceria para a renovação europeia no domínio da liberdade, da segurança e da justiça,** de 10 de maio de 2005. BRUXELAS: Jornal Oficial C 236 de 24.9.2005.

27. COMISSÃO DAS COMUNIDADES EUROPEIAS - COM(2005) 232 final, **Comunicação da Comissão ao Conselho e ao Parlamento Europeu - "Elaboração de um conceito estratégico para combater a criminalidade organizada" {SEC (2005) 724},** de 02 de Junho de 2005. BRUXELAS.

28. COMISSÃO EUROPEIA **- Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.** Bruxelas, 2016: Jornal Oficial da União Europeia 1.8.2018 L 207/1.

29. COMISSÃO EUROPEIA **- Regulamento Delegado (UE) 2018/389 da Comissão de 27 de novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.** [Em linha]. Bruxelas, 2017. [Consult. 17 jun 2018]. Disponível na internet: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R0389

30. CONSELHO DA EUROPA - **Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais** (Convenção Europeia dos Direitos Humanos CEDH) Roma, (1950-11-04).

31. CONSELHO DA EUROPA **- Convenção 108 para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal.** Estrasburgo (1981-01-28).

32. CONSELHO DA EUROPA. Recomendação n.º R (87) 15 do Comité de Ministros - **A UTILIZAÇÃO DE DADOS DE CARÁCTER PESSOAL NO SECTOR DA POLÍCIA**.- [Em linha].S.l.: Conselho da Europa, 1987. [Consult. 13 jan 2018]. Disponível na internet http://www.dgsi.pt/bpjl.nsf/83cbe9acef94db5a8025730800549412/3194f5e16ec96622802567b5003ce40b?OpenDocument

33. CONSELHO DA EUROPA **- Convenção sobre o Cibercrime**, Budapeste (2001-01-23).

34. CONSELHO DA UNIÃO EUROPEIA **-** DECISÃO-QUADRO 2008/913/JAI **relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia,** de 28 de Novembro de 2008. Jornal Oficial da União Europeia 6.12.2008. L 328/55

35. CONSELHO DA UNIÃO EUROPEIA - DECISÃO-QUADRO 2008/977/JAI **relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal**, de 27 de Novembro de 2008. Jornal Oficial da União Europeia 30.12.2008. L 350/60

36. CONSELHO EUROPEU (2010 /C 115/01), - **Programa de Estocolmo "Uma Europa aberta e segura que sirva e proteja os cidadãos "**. Jornal Oficial da União Europeia 4.5.2010 C 115/1

37. DECRETO-LEI nº 47/344, **Código Civil Português.** (Actualizado até à Lei 59/99, de 30/06) Diário do Governo nº 274 Série I Parte A (1966-10-25) 1884-2086.

38. DECRETO-LEI nº 400/82 **Codigo Penal Portugues.** D.R. I Série - 1º Suplemento 221, (1982-09-23) 3006-(2) a 3006-(64).

39. DECRETO-LEI nº 7/2004 **Comercio Eletrónico** D.R. I Série - A. 5 (2004-01-07) 71-78.

40. DECRETO-LEI nº 317-2009. Anexo I **Regimen Juridico de Pagamentos da Moeda Eletrónica**, de 30 de ouctubro D.R. I Série - 211, (2009-10-30) 8271 – 8301.

41. DECRETO-LEI nº 24/2014 **Regime aplicável aos contratos celebrados à distância e aos contratos celebrados fora do estabelecimento comercial, bem como a outras modalidades contratuais de fornecimento de bens ou serviços, incorporando a Diretiva n.º 2011/83/UE, do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, relativa aos direitos dos consumidores,** D.R. 1.ª Série — 32 (2014-02-14) 1393-1403

42. Lei n.º 67/98 **Lei de Protecção de Dados Pessoais.** D.R. I Série-A. 247 (1998-10-26) 5536 – 5546.

43. Lei n.º 5/2004 **das Comunicações Eletrónicas** D.R. I Série - A. 34 (2004-02-10) 788 – 821.

44. Lei n.º 41/2004 (**relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas**) D.R. I Série - A. 194 (2004-08-18) 5241 – 5245.

45. ORGANIZACION DE LOS ESTADOS AMERICANOS - **CONVENCION AMERICANA SOBRE DERECHOS HUMANOS. San José Costa Rica: (1969-11-22)**

46. PARLAMENTO EUROPEO - **Declaración de derechos y libertades fundamentales** de 12 de abril de 1989. publicada mediante resolución en D.O.C.E. C 120/51, de 16 de mayo de 1989.

47. PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 95/46/CE **Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulaçâo**

desses dados. Luxemburgo: Jornal Oficial das Comunidades Europeias (1995-10-24). L281/31 – L281/50

48. PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2000/31/CE **relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre comércio eletrónico»).** Luxemburgo: Jornal Oficial das Comunidades Europeias (2000-07-17) L 178/1 – L 178/16

49. PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/22/CE **Relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas** (directiva serviço universal)**.** Bruxelas**:** Jornal Oficial das Comunidades Europeias (2002-03-07) L 108/51 - L 108/68

50. PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2002/58/CE Relativa **ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas** (Directiva relativa à privacidade e às comunicações electrónicas). Bruxelas: Jornal Oficial das Comunidades Europeias (2002-07-12) L 201/37 - L 201/47

51. PARLAMENTO EUROPEU E DO CONSELHO - Directiva 2009/136/CE de 25 de Novembro de 2009 que altera a Directiva 2002/22/CE **relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor**. Estrasburgo: Jornal Oficial das Comunidades Europeias (2009-12-18) L 337/11 - L 337/36

52. PARLAMENTO EUROPEU E DO CONSELHO - Directiva 2011/92/UE, **relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho,** de 13 de Dezembro de 2011. Jornal Oficial da União Europeia 17.12.2011, L 335/1

53. PARLAMENTO EUROPEU E DO CONSELHO - Diretiva 2013/40/EU - **Relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.** Bruxelas: Jornal Oficial das Comunidades Europeias, (2013-08-12), L 218/8 - L 218/14

54. PARLAMENTO EUROPEU E DO CONSELHO – Diretiva 2015/2366/UE **Relativa aos serviços de pagamento no mercado interno.** Estrasburgo: Jornal Oficial das Comunidades Europeias (2015-11-25) L 337/35 - L 337/115

55. PARLAMENTO EUROPEU E DO CONSELHO – Diretiva (EU) 2016/680 **relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação**

desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de abril de 2016. Bruxelas: Jornal Oficial da União Europeia. (2016-05-04) L 119/89 - L 119/131

56. PARLAMENTO EUROPEU E DO CONSELHO - Directiva (UE) 2016/681 **relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave**, de 27 de abril de 2016. Bruxelas: Jornal Oficial da União Europeia (4.5.2016) L 119/132 - L 119/149

57. PARLAMENTO EUROPEU E DO CONSELHO - Regulamento (CE) n.º 45/2001 **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.** Bruxelas: Jornal Oficial das Comunidades Europeias (2001-01-12) L 8 /1- L 8/22

58. PARLAMENTO EUROPEU E DO CONSELHO - Regulamento (UE) 910/2014 de 23 de julho de 2014 relativo **à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.** Bruxelas: Jornal Oficial das Comunidades Europeias (2014-07-23) L 257/73 - L 257/114

59. PARLAMENTO EUROPEU E DO CONSELHO – Regulamento (UE) 2016/679 - **Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Bruxelas: Jornal Oficial das Comunidades Europeias (2016-04-27). L 119/1 - L 119/88

60. REGIO DECRETO 16 marzo 1942, n. 262 - **Codice civile** Pubblicato nella edizione straordinaria della Gazzetta Ufficiale, Italia n. 79 del 4 aprile 1942.

61. SENADO FEDERAL - **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL**. [Em linha]. Secretaria de Editoração e Publicações Coordenação de Edições Técnicas Brasília, 5 de outubro de 1988. [Consult. 03 Dic 2017] ISBN: 978-85-7018-698-0 Disponível na internet: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf

62. **TRATADO DA UNIÃO EUROPEIA (TUE)** VERSÃO CONSOLIDADA Maastricht: Jornal Oficial da União Europeia (7.6.2016) C 202/13 - C 202/45

63. **TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA** (TFUE) VERSÃO CONSOLIDADA Roma: Jornal Oficial da União Europeia (1957-03-05) C 83/47 - C 83/199

64. UNION EUROPEIA (2000/C 364/01) **CARTA DOS DIREITOS FUNDAMENTAIS.** Niza, el 7 de Dez. 2000. O Parlamento Europeio, el Conselho da União Europeia e a Comissão Europeia.

ARTIGOS ELECTRÓNICOS:

1. ABOGADOS PORTALEY - **La incorporación de los delitos informáticos al Código Penal argentino**. [Em linha]. 2008 [Consult. 25 julho 2018] Disponível na internet:

HTTPS://DELITOSINFORMATICOS.COM/06/2008/NOTICIAS/LA-INCORPORACION-DE-LOS-DELITOS-INFORMATICOS-AL-CODIGO-PENAL-ARGENTINO

2. ALVES, Laurinda - **Facebook e Google vítimas de esquema de 'phishing' de mais de 100 milhões**. [Em linha]. Portugal: 2017 [Consult. 21 Maio 2017]. Disponível na internet: http://observador.pt/2017/04/28/facebook-e-google-vitimas-de-esquema-de-phishing-de-mais-de-100-milhoes/

3. BASTO, Inés – **A nova Diretiva de Serviços de Pagamento.** Revista "Actualidad Jurídica Uría Menéndez" [Em linha]. Lisboa, Nº. 46-2017, Páginas 118-123 [Consult. 14 maio 2018]. Disponível na internet http://www.uria.com/documentos/publicaciones/5458/documento/foro_port01.pdf?id=7137 ISSN: 2174-0828

4. COMISSÃO EUROPEIA - COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na EU. COM(2013) 847 final. [Em linha]: Bruxelas, 27.11.2013 [Consult. 14 janeiro 2018]. Disponível na internet http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_pt.pdf

5. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS – **Comunicado da CNPD Aplicação do novo quadro legal de proteção de dados.** [Em linha]: Lisboa, 25 de maio de 2018, [Consult. 18 agosto 2018]. Disponível na internet https://dre.pt/documents/10184/826042/Comunicacao+CNPD_25_5_2018.pdf/87e28703-4e8c-4439-9ba9-f0f7b75ceab1

6. COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS - **O que é a CNPD.** [En linha] Lisboa. [Consult. 10 março 2018]. Disponível na internet: https://www.cnpd.pt/bin/cnpd/acnpd.htm

7. CORREIA, Pedro; DE JESUS, Inês - **Combate às transferências bancárias ilegítimas pela Internet no direito português:entre as experiências domésticas e políticas globais concertadas.** Scientific Electronic Library Online – SCIELO. [Em linha]. Rev. direito GV vol.12 no.2 São Paulo May/Aug. 2016 [Consult. 17 Ago. 2018]. Disponível na internet: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322016000200542

8. DINERO.COM - **El cibercrimen es un delito más rentable que el narcotráfico.** 28/09/2015 [Consult. 01 jul 2018]. Disponível na internet: https://www.dinero.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988

9. EERSTE KAMER - Goedkeuring Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerke. [Em linha]. [Consult. 28 feb 2018]. Disponível na internet: https://www.eerstekamer.nl/wetsvoorstel/30036_goedkeuring_verdrag_inzake

10. EUR-LEX **- Comércio eletrónico — Normas comuns da EU**. SÍNTESE DE: Diretiva 2000/31/CE — Comércio eletrónico na UE. Última atualização 13.10.2015. [Consult. 21 maio

2017]. Disponível na internet: http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:l24204&from=ES

11. EUR-LEX **- Proteger la privacidad de los ciudadanos de la UE en las transferencias de datos a los Estados Unidos.** [Em linha]. [Consult. 03 sep. 2018]. Disponível na internet: https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX%3A32016D1250

12. EUR-LEX - **Regras revistas relativas aos serviços de pagamento na União Europeia**. [Em linha]. [Consult. 03 may. 2018]. Disponível na internet: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3A2404020302_1

13. EXPRESIONBINARIA - **Espionaje e Interceptación de las comunicaciones** [En linha]. PUBLICADO EN CIENCIA Y TECNOLOGÍA, NOTICIAS, 10 NOVIEMBRE, 2011. [Consult. 25 Ago 2018]. Disponível na internet https://www.expresionbinaria.com/espionaje-e-interceptacion-de-las-comunicaciones/

14. F. AUGUST - **CABLEADO VETICAL O BACKBONE.** [Em linha].2013. [Consult. 21 feb 2018]. Disponível na internet: https://prezi.com/wyk3supokugw/cableado-vetical-o-backbone/

15. FLORENTINO, Bruno - **Tipo e tipicidade, tipo objetivo e tipo subjetivo. Dolo e culpa.** [Em linha]. [Consult. 21 junho 2018]. Disponível na internet: https://brunoflorentinosilva.jusbrasil.com.br/artigos/183249818/tipo-e-tipicidade-tipo-objetivo-e-tipo-subjetivo-dolo-e-culpa

16. GALEON.COM HISPAVISTA - **Delitos informáticos en el derecho comparado.** [Em linha]. [Consult. 25 de julho de 2018]. Disponível na internet: http://derela.galeon.com/enlaces2303544.html

17. GONÇALVES, Anabela - **PECK NEWS: GLOBAL TRENDS.** Artigos e Entrevistas 5º CONGRESSO INTERNACIONAL DIREITO NA LUSOFONIA [[Em linha]. Março 2018. [Consult. 3 Set. 2018]. Disponível na internet: http://www.peckadvogados.com.br/publicacoes/artigos-e-entrevistas/peck-news-global-trends-9

18. GONÇALVES, Ramiro Manuel [et al.]. - **Modelo das iniciativas de comércio electrónico em organizações portuguesas.** Scientific Electronic Library Online – SCIELO. [Em linha]. Vol.33, No.2, Caracas: 2008, p. 15. [Consult. 17 Fev. 2017]. Disponível na internet: http://search.scielo.org/?q=Modelo+das+iniciativas+de+com%EF%BF%BDrcio+electr%EF%BF%BDnico+em+organiza%EF%BF%BDes+portuguesas&lang=pt&count=15&from=0&output=site&sort=&format=summary&fb=&page=1&q=Modelo+das+iniciativas+de+com%C3%A9rcio+electr%C3%B3nico&lang=pt&page=1. ISSN 03781844.

19. MEDINA, Manel; MOLIST, Mercè - **INFORME VIU: Ciberseguridad: Tendencias** 2017. [Em linha]. Valencia: 2017. [Consult. 16 maio 2017]. Disponível na internet: http://www.viu.es/wp-content/uploads/2017/03/Informe-Ciberseguridad.pdf

20. OLIVEIRA, Mariana **- Dezenas de clientes de bancos portugueses burlados por rede brasileira.** [Em linha]. Portugal: 5 de Dezembro de 2016. [Consult. 16 maio 2017]. Disponível

na internet https://www.publico.pt/2016/12/05/sociedade/noticia/mp-acusa-24-arguidos-que-desviaram-mais-de-260-mil-euros-de-contas-bancarias-de-terceiros-1753749

21. ORIGEM DA PALAVRA **- Consultas e artigos com a palavra "privacidade"** 01/11/2011 [Consult. 25 dezembro 2017]. http://origemdapalavra.com.br/site/?s=privacidade

22. RUBIO ALAMILLO, Javier - Diferencias entre evidencia informática y prueba informática. [Em linha], Blog. 16/08/2018 [Consult. 22 Ago. 2018]. Disponível na internet: https://peritoinformaticocolegiado.es/blog/diferencias-entre-evidencia-informatica-y-prueba-informatica/

23. SANTOS, Barbara - **SPAM: o que é e como evitar essa prática.** [Em linha]. Portugal: 2016 [Consult. 28 decembro 2017]. Disponível na internet: https://blog.hotmart.com/produtores/spam-o-que-e-e-como-evitar/

24. SEGU.INFO - **Legislación y Delitos Informáticos – Holanda.** [Em linha]. Argentina [Consult. 16 junho 2018]. Disponível na internet: https://www.segu-info.com.ar/delitos/holanda.htm.

25. SIMÕES, Ana; FERREIRA, Mariana - **PROTECÇÃO DE DADOS PESSOAIS**. REGULAMENTO (UE) 2016/679. [Em linha]. Lisboa: 2016. [Consult. 05 sep. 2017]. Disponível na internet: http://www.slcm.pt/xms/files/FYI_PI_Maio16.pdf

FONTES METODOLÓGICAS:

1. ARIAS, Fidias G. - **EL PROYECTO DE INVESTIGACION: Guía para su elaboración.** [Em linha]. 3ra. Ed. Caracas: Episteme, 1999. [Consult. 4 junho 2017]. Disponível na internet: http://www.smo.edu.mx/colegiados/apoyos/proyecto-investigacion.pdf

2. NP 405-1. 1994. Informação e Documentação - **Referências bibliográficas: documentos impressos.** Caparica. Instituto Português da Qualidade.

3. NP 405-4. 2002. Informação e Documentação – **Referências bibliográficas: parte 4: documentos electrónicos.** Caparica: Instituto Português da Qualidade.

4. POPPER, Karl R. – **La Lógica de la Investigación Científica**. [Em linha]. 5ª ed. Madrid: TECNOS, 1980. [Consult. 4 junho 2017]. Disponível na internet: http://www.raularagon.com.ar/biblioteca/libros/Popper%20Karl%20-%20La%20Logica%20de%20la%20Investigacion%20Cientifica.pdf ISBN: 80-309-0711- 4

5. PONCE DE LEON ARMENTA., Luis – **La Metodología en la Investigación Científica del Derecho.** [Em linha]. Mexico: 2017 [Consult. 4 junho 2017]. Disponível na internet: https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-facultad-derecho-mx/article/view/28239/25507

6. POSGRADUANDO - **As diferenças entre pesquisa descritiva, exploratória e explicativa**. [Em linha]. Portugal: 2017 [Consult. 4 junho 2017]. Disponível na internet: http://posgraduando.com/diferencas-pesquisa-descritiva-exploratoria-explicativa/

7. TAMAYO Y TAMAYO, Mario. **- El Proceso de la Investigación Científica.** [Em linha]. **4ª Ed., México, Limusa, 2003,** [Consult. 6 junho 2017]. Disponível na internet: https://clea.edu.mx/biblioteca/Tamayo%20Mario%20-%20El%20Proceso%20De%20La%20Investigacion%20Cientifica.pdf