

– PARTE

**Capítulo 1 - DIREITO DA INFORMÁTICA**

- **Sociedade da informação**
  - o Sociedade da informação- expressão celebrizada por Jacques Delors, presidente da comissão da CEE, em 1993, como objetivo europeu a atingir em resposta ao programa americano semelhante
  - o Novo paradigma de sociedade: modelo de desenvolvimento social e económico onde a informação, como meio de criação de conhecimento, desempenha um papel fundamental na produção de riqueza e na contribuição para o bem-estar e qualidade de vida dos cidadãos
  - o Pressupostos:
    - A informação como fator de progresso social, económico e humano
    - Vantagens do tratamento automatizado de informação:
      - Poupança de esforço e trabalho humano
      - Redução de tempo na execução de tarefas e celeridade na comunicação
      - Encurtamento de distâncias físicas
      - Redução de custos
    - Aproveitamento das vantagens do tratamento automatizado por uso intensivo do computador e das NTIC em todos os setores da sociedade:
      - Setor primário e indústria (equipamentos e linhas de produção)
      - Comércio e serviços (novas formas de transações comerciais, por meios eletrónicos e novas utilidades, novas funcionalidades)
      - Serviços públicos e entidades estatais (Assembleia da República, Tribunais, Segurança social, Finanças, Diário da República Eletrónico)
      - Comunicação social e meios de informação
      - Lazer, entretenimento e comunicação interpessoal
    - O tratamento automatizado de informação como elemento determinante da criação de emprego e competitividade, criando mais riqueza e consequentemente qualidade de vida para os cidadãos
  - o Novas exigências sociais feitas ao Estado na sociedade da informação
    - Acesso aos canais de informação por parte de todos os cidadãos
      - Criação de infra-estruturas e redes de comunicação
      - Privatização do mercado das telecomunicações para promover a concorrência na produção e comercialização de equipamentos, na prestação de serviços, passando pelo acesso aberto as redes e serviços básicos - Lei 5/2004 de 10/02 (regime jurídico das redes e serviços de comunicações electrónicas e aos recursos e serviços conexos)

- Regulação jurídica do mercado das telecomunicações através do ICP-ANACOM (Instituto de comunicações de Portugal) - autoridade responsável pela regulação da concorrência e fiscalização das redes e serviços de comunicações electrónicas
- Formação informática (“nova alfabetização” e combate à info-exclusão) – adaptação dos programas escolares e académicos às necessidades sociais e profissionais de utilização da informática
- Informatização e modernização da Administração Pública - Decreto-lei 135/99 de 22/04 (acesso a internet em sítios públicos, sistema de informação da Administração Pública, cruzamento da dados, pedido de documentos por meios eletrónicos, endereço dos serviços públicos e correspondência com o mesmo valor, pagamentos ao Estado, etc...), Resolução do Conselho de Ministros n.º 107 a 111/2003 de 12/08 (Plano de ação para o governo eletrónico, banda larga, cidadãos com necessidades especiais, compras eletrónicas), Resolução do Conselho de Ministros 181/2004 de 22/12 (Guia para as comunicações na Administração Pública), Resolução do Conselho de Ministros 33/2016 que constitui o Conselho para as Tecnologias de Informação e Comunicação.
- Proteção dos direitos, liberdades e garantias dos cidadãos que possam ser afetados pelo uso de meios automatizados
  - Estabelecimento de garantias de não discriminação no acesso à informação- CRP
  - Proteção jurídica dos dados pessoais- art. 35º da CRP, Regulamento (EU) 2016/679, de 27 de abril, Lei n.º 58/2019, de 8 de agosto e Lei 41/2004 de 18/08
  - Tutela da propriedade intelectual - Código dos Direitos de Autor e Direito Conexos, DL 122/2000 de 4/07 (proteção jurídica das bases de dados)- alterado em último pelo DL n.º 47/2023, de 19/06 e DL 252/1994 de 20/10 (proteção jurídica dos programas de computador) - Alterado em ultimo pela Lei n.º 92/2019, de 04/09
  - Proteção dos direitos dos consumidores- DL 24/2014 de 14/02(contratos celebrados à distância), - 7ª versão - a mais recente (Lei n.º 10/2023, de 03/03) e regimes gerais- DL 446/85 de 25/10 (cláusulas contratuais gerais) - 10ª versão - a mais recente (DL n.º 123/2023, de 26/12), Lei 24/96 de 31/07 (defesa do consumidor), - 11ª versão - a mais recente (Lei n.º 28/2023, de 04/07) DL n.º 84/2021, de 18/10 venda de bens de consumo), e DL 57/2008 de 26/03 (práticas comerciais desleais)
- Favorecimento do uso de novas tecnologias como forma de impulsionar o crescimento económico e, consequentemente a qualidade de vida dos cidadãos
  - Enquadramento jurídico das novas possibilidades de uso de meios automatizados no âmbito do comércio jurídico- DL 7/2004 de 24/08 (lei do comércio eletrónico) e outros regimes especiais aplicáveis aos prestadores de serviços da sociedade da informação, como DL 134/2009 de 2/06, DL 175/99 de 21/05 e DL 177/99 de 21/05, Lei 5/2004 de 10/02, e DL 58/2000 de 18/04

- Promoção de segurança jurídica no estabelecimento de relações no campo virtual - DL 62/2003 de 3 de Abril (documentos eletrónicos e assinatura eletrónica); DL 28/2019 de 15/02 - fatura eletrónica.

- **Direito da Informática**

- o Noção

- Conjunto de normas jurídicas que regulam as situações da vida social que envolvem a utilização de meios informáticos (incluindo o comércio eletrónico)

- o Âmbito

- Não é propriamente um ramo do direito, pois não lhe é assinalada autonomia científica, mas sim um conjunto de regras jurídicas dispersas por vários ramos de direito público e privado que têm como denominador comum o facto de regularem aspectos relacionados com o uso de meios automatizados:

- Direito privado

- o Direito civil

- Direitos de personalidade – direitos à honra, reserva da intimidade da vida privada, etc.
        - Direito de propriedade sobre bens intelectuais – direitos de autor, bases de dados e software
        - Contratos celebrados por meios eletrónicos
        - Documentos em suporte eletrónico e assinatura eletrónica
        - Protecção dos consumidores nos contratos celebrados por via eletrónica
        - Aquisição do direito ao uso de um endereço IP -registo de domínios (DNS)

- o Direito do trabalho

- Teletrabalho (*networking*)- novas formas de prestação de trabalho e de controlo da atividade dos trabalhadores

- Direito público

- o Direito constitucional

- Tutela de direitos, liberdades e garantias dos cidadãos
        - Atribuições do Estado de Direito no contexto da sociedade da informação

- o Direito administrativo

- Regulação do mercado das telecomunicações
        - Fiscalização das operações de tratamento de dados pessoais
        - Controlo das entidades certificadoras de assinaturas eletrónicas

- o Direito tributário/fiscal

- Tributação de operações realizadas no ciberespaço (IVA, IRS e IRC)
        - Relacionamento com o contribuinte por via eletrónica (envio de declarações pela internet,

- consulta da situação tributária e obtenção de certidões online, notificações eletrónicas)
  - o Direito penal e contra-ordenacional
    - Contraordenações e crimes cometidos por meios informáticos
  - o Direito adjetivo ou processual
    - Valor de documentos eletrónicos como meio de prova
    - Utilização de NTIC no âmbito da justiça
- o Características:
  - Pluridisciplinaridade - engloba vários ramos do direito
  - Fragmentação e dispersão - coexistência de um regime jurídico comum com regras específicas novas, ou adaptação das antigas para abarcar as novas realidades da sociedade da informação
  - Dimensão internacional e transnacional dos casos concretos que o direito é chamado a regular
  - Carácter evolutivo - problemas recentes, em constante mutação exigem uma abertura a novas respostas e soluções
- o O direito da informática não se pode considerar um ramo do direito novo, mas um conjunto de normas jurídicas de natureza heterogénea que surgiram como reação à massificação do uso das tecnologias informáticas ou que resultaram da adaptação de regimes legais anteriores a esta nova realidade

## Capítulo II - INFORMÁTICA E DIREITOS FUNDAMENTAIS

- Direitos fundamentais - noções básicas
  - o Direitos da pessoa humana previstos e garantidos pela Constituição
  - o Direitos individuais, que qualquer pessoa tem, pelo simples facto de o ser, sendo inerentes à personalidade jurídica singular (direitos, liberdades e garantias)
  - o Exemplos: direito à vida, à integridade física e moral, ao nome, à imagem, à reserva da intimidade da vida privada
  - o Regime: as restrições aos direitos fundamentais só podem ser feitas com base numa lei (art. 18º CRP), ou no consentimento do seu titular, desde que não haja ofensa aos princípios de ordem pública (art. 81º, n.º 1, do CC)
- Os riscos de violação dos direitos fundamentais associados à utilização da informática e telecomunicações
  - o A informática proporciona a recolha, armazenamento, tratamento e pesquisa de informação organizada e facilmente acessível em bases de dados
  - o Atualmente, a informática é usada para tratar informações relativas a pessoas singulares
    - Com finalidades públicas - pela Administração Pública (registo civil, predial, e automóvel, registo criminal, Finanças, Segurança social, Serviço Nacional de Saúde, instituições de ensino, etc.)
    - Com fins privados - por entidades particulares (instituições bancárias, entidade empregadora, fornecedores de serviços públicos essenciais, empresas comerciais e de marketing, etc.)

- o Os meios eletrónicos são usados por entidades públicas e privadas para captar e registar informação pessoal:
  - Mecanismos de videovigilância (tratamento da imagem e/ou som captada por câmaras de vídeo) – permitidos por lei para garantir a segurança das pessoas e bens e o controlo do tráfego e infracções rodoviárias
  - Registos eletrónicos inerentes à utilização de certos serviços: a via verde e os dispositivos de matrícula, o cartão multibanco, o fornecimento de serviços de telefone fixo e móvel e de acesso à internet
- o A informática conjugada com as novas tecnologias da informação e comunicação (NTIC) veio facilitar o acesso, transmissão e utilização da informação, permitindo que esta chegue, de forma simples e rápida, a um universo muito amplo de destinatários (internet, email, fax...)
- o Principais perigos para as pessoas singulares:
  - Acesso e divulgação de dados pessoais de pessoas singulares, sem o seu consentimento (invasão de privacidade)
  - Formulação e divulgação de factos ou juízos ofensivos da honra e consideração de uma pessoa singular (ofensa à honra)
  - Utilização de informação confidencial para finalidades ilícitas (por exemplo, *phishing*)
  - Recepção de comunicações eletrónicas não solicitadas (spam)
- A proteção jurídica dos direitos fundamentais que apresentam maior perigo de violação na sociedade da informação
  - o **Direito à honra**
    - o Previsão – art. 25º, n.º 1<sup>1</sup>, 26º, n.º 1<sup>2</sup>, CRP e 70º, n.º 1, do CC
    - o Conteúdo
      - Direito ao respeito, ao bom nome e reputação
      - Poder de exigir a não imputação de factos ou formulação de juízos de valor, direta ou indireta, quer estes sejam verdadeiros ou não, que sejam, em abstrato, suscetíveis de afetar a sua personalidade moral ou consideração social
  - o Tutela penal – crimes contra a honra
    - Crime de injúria – art. 181º<sup>3</sup> e 182º CP (directamente)
    - Crime de difamação – art. 180º<sup>4</sup> e 182º CP (dirigindo-se a terceiros)

---

<sup>1</sup> Artigo 25 CRP - 1. A integridade moral e física das pessoas é inviolável.

<sup>2</sup> Artigo 26.º CRP - 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 proteção legal contra quaisquer formas de discriminação.

<sup>3</sup> Artigo 181.º CP - 1 - Quem injuriar outra pessoa, imputando-lhe factos, mesmo sob a forma de suspeita, ou dirigindo-lhe palavras, ofensivos da sua honra ou consideração, é punido com pena de prisão até 3 meses ou com pena de multa até 120 dias.

<sup>4</sup> Artigo 80 CP - 1 - Quem, dirigindo-se a terceiro, imputar a outra pessoa, mesmo sob a forma de suspeita, um facto, ou formular sobre ela um juízo, ofensivos da sua honra ou consideração, ou reproduzir uma tal imputação ou juízo, é punido com pena de prisão até 6 meses ou com pena de multa até 240 dias.

- A pena é agravada, nos termos do art. 183º, n.º 1 e 2, do CP, se estes crimes forem praticados através de meios que facilitem a sua divulgação, ou através de meios de comunicação social
- o Tutela civil
  - Responsabilidade civil por factos ilícitos – art. 70º, n.º 2, e 483º do CC (obrigação de indemnizar os danos causados com a ofensa culposa à honra)
  - Providências adequadas a evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida- art. 70º, n.º 2, CC (exemplos: publicação de sentença condenatória, suspensão imediata de publicação periódica, retirada de obra do comércio jurídico, etc.)
- **Direito à reserva da intimidade da vida privada**
  - o Previsão - art. 26º, n.º 1 e 2, 34º<sup>5</sup>, e 35º, n.º 4<sup>6</sup>, da CRP, art. 80º<sup>7</sup> CC
  - o Conteúdo
    - Conceito de vida privada - conjunto de actividades, situações, atitudes e comportamentos individuais que não tem relação com a vida pública e dizem respeito estritamente a vida pessoal da pessoa (personalidade e modo de ser, sentimentos, vivências familiares, costumes e modos de vida, orientação sexual, política ou religiosa...), devendo subtrair-se ao conhecimento público por razões de resguardo, melindre e privacidade
    - Condutas proibidas: intromissões e ingerências na vida privada alheia, bem como a sua divulgação
    - Este direito abarca o direito à imagem e a outros dados pessoais
    - Este direito engloba ainda o *right to be let alone*- salvaguarda do isolamento, do sossego e da paz interior, liberdade de autodeterminação informacional - direito de se opor a interferências exteriores não consentidas que perturbem a pessoa (remissão para as mensagens publicitárias não solicitadas (*spam*))
  - o Âmbito de protecção
    - Art. 26º, n.º 1, CRP e 80º CC – direito à reserva da vida privada (em sentido estrito)
      - Dever de guardar reserva quanto à intimidade da vida privada de outrem (art. 80, n.º 1 e 2, CC)
        - o De acordo com a natureza do caso (finalidade da utilização da informação, objetivo visado, facto relatado, local onde o facto ocorreu)
        - o De acordo com a condição das pessoas (pessoa anónima ou notoriedade devida ao exercício de cargos públicos ou de profissões na comunicação social) -  
NOTA: a notoriedade de certas pessoas faz com que

<sup>5</sup> Artigo 34.º n.º 4 da CRP - 4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal.

<sup>6</sup> Artigo 35.º n.º 4 CRP - 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.

<sup>7</sup> Artigo 80.º CC – Todos devem guardar reserva quanto à intimidade da vida privada de outrem

não possam opor-se à divulgação de acontecimentos da sua vida pública e privada, desde que se verifique uma conexão entre o que se divulga e a atividade da pessoa que gera a sua notoriedade

- Art. 26º, n.º 1, CRP e 79º CC - direito à imagem
  - Proibição de exposição, reprodução ou lançamento no comércio do retrato (desenho, imagem fotográfica de uma pessoa em formato de papel ou eletrónico) de outrem, sem o seu consentimento (art. 79º, n.º 1, CC)
  - Exceções: razões de notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais ou quando a reprodução da imagem vier enquadrada na de lugares públicos ou de factos de interesse público que tenham decorrido publicamente- art. 79º, n.º 2, CC (exceto se daí decorrer prejuízo para honra e reputação da pessoa- n.º 3)
- Art. 34º, n.º 1 CRP – direito à inviolabilidade da correspondência, telecomunicações e meios de comunicação
  - Proibição das autoridades públicas se ingerirem na correspondência, telecomunicações e meios de comunicação, salvo exceções legais previstas em matéria de direito criminal
  - Lei 41/2004 (lei de privacidade nas comunicações eletrónicas)- estabelece obrigações e restrições às empresas que fornecem o acesso a redes e serviços de comunicações eletrónicas
- Art. 26º, n.º 2, e 35º, n.º 4, da CRP- direito à proteção dos dados pessoais
  - Proibição de acesso a dados pessoais de terceiros, salvo os casos expressamente previstos na lei
  - Regulamento (UE) 2016/679, de 27/04 - RGPD
  - Lei 58/2019 (lei de execução do RGPD)
- o Tutela penal - crimes contra a reserva da vida privada
  - Perturbação da vida privada – art. 190º, n.º 2, CP
  - Devassa da vida privada – art. 192º CP
  - Devassa por meio de informática – art. 193º CP
  - Violação de correspondência ou telecomunicações – art. 194º CP
- o Tutela civil
  - Responsabilidade civil e medidas inibitórias – art. 70º, n.º 1 e 2, do CC

## **1 - A proteção de dados como direito fundamental**

Evolução histórica

O direito no artigo 8.º na Carta dos Direitos Fundamentais

A CRP - Artigo 35.º

o O art. 35º da CRP consagra os princípios gerais que a lei tem de desenvolver em matéria de tratamento automatizado de dados pessoais:

- A lei tem que garantir os seguintes direitos ao titular de dados pessoais: direito de acesso aos dados informatizados que lhes digam

respeito, direito a exigir a sua retificação e atualização, e direito de conhecer a finalidade a que se destinam

- 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 proteção, designadamente através de entidade administrativa independente
- O tratamento informático de dados relativos a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica só pode ser feito mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis
- Proibição de acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei
- Proibição de atribuição de um número nacional único aos cidadãos (cartão do cidadão)
- Garantia de livre acesso às redes informáticas de uso público
- Extensão da proteção aos dados pessoais constantes de ficheiros manuais

## **2 - O Regime jurídico de proteção de dados pessoais: o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 – RGPD**

**Lei 58/2019 de 8 de agosto – assegura a execução na ordem jurídica do RGPD**

### **A – Dados pessoais e tratamento de dados – conceitos; âmbito de aplicação do RGPD**

O RGPD 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 - artigo 2.º RGPD.

- Dados pessoais – 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 referencia 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 – artigo 4.º n.º1
- Tratamento – uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação a conservação, a adaptação ou alteração, a



recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação o pagamento ou a destruição – artigo 4.º n.º 2

#### **B – Os sujeitos intervenientes no âmbito dos tratamentos de dados**

- ▶ Titular dos dados – pessoa singular a quem se referem as informações em causa
- ▶ Responsável pelo tratamento – a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais – artigo 4.º n.º 7 RGPD
- ▶ Subcontratante – uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes – artigo 4.º n.º 8 RGPD
- ▶ Encarregado de proteção de dados – pessoa designada pelo responsável pelo tratamento ou pelo subcontratante (elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante ou com base em contrato de prestação de serviços) que controla a conformidade com o RGPD das políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados – artigo 39.º RGPD e 9.º a 13.º da Lei n.º 58/2019
- ▶ Representante – uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27.º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do RGPD.

#### **C – Princípios gerais de tratamentos de proteção de dados: artigo 5.º do RGPD**

- Princípio da transparência - O artigo 12.º define as regras gerais aplicáveis: ao fornecimento de informações aos titulares dos dados (nos termos dos artigos 13.º a 14.º); às comunicações com os titulares dos dados a respeito do exercício dos seus direitos (nos termos dos artigos 15.º a 22.º); e às comunicações em relação a violações de dados (artigo 34.º). Mais especificamente, o artigo 12.º estipula que as informações ou a comunicação em causa devem cumprir as regras seguintes:
  - devem ser concisas, transparentes, inteligíveis e de fácil acesso
  - devem utilizar uma linguagem clara e simples (artigo 12.º, n.º 1),
  - importante quando as informações se dirigem a crianças
  - devem ser prestadas por escrito «ou por outros meios», incluindo eletrónicos
  - se o titular dos dados o solicitar, podem ser prestadas oralmente

- são em geral fornecidas a título gratuito (artigo 12.º, n.º 5).

- Princípio da licitude - Os tratamentos dos dados só são lícitos se tiverem como fundamento de legitimidade alguma das situações previstas no artigo 6.º ou 9.º do RGPD
- Princípio da lealdade
- Princípio da limitação das finalidades – artigo 5.º n.º 1 b) do RGPD – Os dados pessoais são recolhidos para finalidades determinadas, explícitas e legítimas não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades
- Princípio da minimização dos dados – Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados
- Princípio da exatidão – exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos sejam apagados ou retificados sem demora – alínea d) do n.º 1 do artigo 5.º RGPD
- Princípio da limitação da conservação – artigo 5.º n.º 1 e) do RGPD – Conservados apenas durante o período necessário para as finalidades para as quais são tratados
- Princípio da integridade e confidencialidade – tratados de uma forma que garanta a sua segurança, incluindo proteção contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas e organizativas adequadas – alínea f) do n.º 1 do artigo 5.º RGPD
- Princípio da responsabilidade - Artigo 5.º n.º 2 do RGPD – O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1e tem de poder comprová-lo

#### **D - Pressupostos legais do tratamento: condições de licitude – artigo 6.º do RGPD**

##### **1 – O consentimento: requisitos**

O titular dos dados tem de dar o consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas. «Consentimento do titular de dados», qualquer manifestação de vontade, livre, específica, informada e **explícita**, pela qual a pessoa em causa aceita, **mediante uma declaração ou um ato positivo**

**inequívoco**, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Cabe ao Responsável pelo tratamento de dados fazer prova do consentimento do titular e de que este foi obtido nos termos do RGPD.

2 - Execução do contrato em que o titular de dados seja parte ou diligências prévias à formação do contrato ou declaração de vontade negocial efetuadas a seu pedido

3 - Cumprimento de obrigação jurídica a que o responsável pelo tratamento esteja sujeito

4 - Proteção de interesses vitais do titular dos dados ou de outra pessoa singular

5 - Se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício de autoridade pública em que esteja investido o responsável pelo tratamento

6 - Prossecução de interesses legítimos do responsável ou de um terceiro, prevalecentes sobre os interesses ou direitos e liberdades fundamentais do titular dos dados que exijam a proteção de dados pessoais, em especial se o titular for uma criança.

### **O regime do tratamento de categorias especiais de dados pessoais – artigo 9.º RGPD**

Proibição de tratamento de categorias especiais de dados pessoais – dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Exceções:

- Consentimento explícito do titular dos dados
- Cumprimento de obrigações e exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, segurança social e de proteção social
- Se o tratamento for necessário para proteger interesses vitais do titular dos dados ou de outra pessoa singular, no caso do titular dos dados estar física ou legalmente incapacitado de dar o consentimento
- Se o tratamento for efetuado por uma fundação ou associação sem fins lucrativos
- Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelos seus titulares
- Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional
- Se o tratamento for necessário por motivos de Interesse público importante
- Para efeitos de medicina preventiva ou de trabalho, para avaliação da capacidade de trabalho do empregado, diagnóstico médico, prestação de

cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas ou serviços de saúde ou de ação social

- Motivos de interesse público no domínio da saúde pública
- Se o tratamento for necessário para fins de arquivo de interesse público, Investigação científica ou histórica ou para fins estatísticos

#### **E - Direitos dos titulares dos dados**

- Direito de informação – artigo 12.º a 14.º do RGPD
- Direito de acesso – artigo 15.º do RGPD
- Direito de retificação – artigo 16.º do RGPD
- Direito ao esquecimento – artigo 17.º do RGPD
- Direito à limitação do tratamento – artigo 18.º do RGPD
- Direito de portabilidade dos dados – artigo 20.º do RGPD
- Direito de oposição (definição de perfis) – artigo 21.º e 22.º do RGPD
- Direito a resposta no prazo – artigo 12.º n.º 3 do RGPD

#### **F- Obrigações dos responsáveis e dos subcontratantes**

- ▶ Manter registos sobre tratamentos de dados que efetuem – artigo 30.º do RGPD
- ▶ Adotar os princípios de proteção de dados desde a conceção e por defeito – artigo 25.º do RGPD
- ▶ Nomear um DPO – artigo 37.º do RGPD:

Quando o tratamento for efetuado por uma autoridade ou um organismo público

As atividades principais consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala

As atividades principais consistam em operações de tratamento em grande escala de categorias especiais de dados e de danos relacionados com condenações penais e infrações

Aptidões de um DPO:

Conhecimentos especializados no domínio do direito nacional e europeu de proteção de dados e das práticas de proteção de dados

Profundo conhecimento do RGPD

Conhecimento do setor e da organização

Conhecimento dos sistemas de informação e das necessidades de segurança dos dados

Capacidades para desempenhar as suas funções: qualidades pessoais e posição dentro da organização

Interno ou em prestação de serviços

- ▶ Obrigação de comunicar quebras de segurança – artigo 33.º do RGPD
- ▶ Necessidade de realizar estudos de impacto sobre tratamentos de dados – artigo 35.º do RGPD
- ▶ Utilizar tecnologias tais como pseudonimização e cifragem de dados – artigo 32.º do RGPD
- ▶ Aplicabilidade do Regulamento a subcontratantes – artigo 28.º do RGPD

## **G - O papel da Autoridade Nacional de Proteção de Dados e do Comité Europeu de proteção de Dados**

G.1 - Natureza, atribuições e competências

**Regulamento (Art.º 51.º) e Lei n.º 43/2004, de 18 de agosto republicada pela Lei 58/2019 de 8 de agosto – artigo 3.º a 8.º**

- ▶ Cada Estado-membro deve nomear uma ou mais Autoridade de Controlo, independente, com a responsabilidade pela fiscalização da aplicação do RGPD, a fim de:
- ▶ Defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento
- ▶ Facilitar a livre circulação dos dados na União

Estatuto independente:

- ▶ Independência na ação- art.º 52.º
- ▶ nomeação dos seus membros, prazo e termo dos mandatos - art.º 53.º
- ▶ Regras aplicáveis à constituição da Autoridade de Controlo - art.º 54.º

Novo paradigma:

- ▶ Fim do controlo prévio dos tratamentos de dados pessoais;
- ▶ Reforço do papel do encarregado de proteção de dados (art.º 37.º e 39.º b) – controla a conformidade com o RGPD);
- ▶ Aposta na ação fiscalizadora e à posteriori, das autoridades de controlo.

### ☐ Competências, atribuições e poderes

Competência - Artigo 55.º

- ▶ «1. As autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro.
- ▶ 2. Quando o tratamento for efetuado por autoridades públicas ou por organismos privados que atuem ao abrigo do artigo 6.º, n.º 1, alínea c) (cumprimento de uma obrigação jurídica) ou e) (necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública), é competente a autoridade de controlo do Estado-Membro em causa. Nesses casos, não é aplicável o artigo 56.º.
- ▶ 3. As autoridades de controlo não têm competência para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional.»

#### ☐ Poderes da Autoridade de Controlo

- ▶ Poderes de investigação – Artigo 58.º n.º 1
- ▶ Poderes de correção – Artigo 58.º n.º 2
- ▶ Poderes consultivos e de investigação - Artigo 58.º n.º 3

### **H – Mecanismos de cooperação e controlo de coerência**

#### ☐ Mecanismos de cooperação

RGPD (Art.º 60.º a 62.º)

A Autoridade de Controlo principal coopera com as outras autoridades de controlo interessadas, trocando informações, prestando assistência mútua e realizando operações conjuntas;

Autoridade de Controlo Principal – autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável ou subcontratante

Autoridade de Controlo Interessada – uma autoridade de controlo afetada pelo tratamento de dados pessoais por o responsável ou subcontratante estar estabelecido no seu território os titulares dos dados aí residirem ou ter sido apresentada reclamação junto dessa autoridade

#### ☐ O procedimento do controlo da coerência

RGPD (Art.º 60.º a 67.º)

- ▶ A autoridade de controlo principal coopera com as outras autoridades de controlo interessadas para procurar alcançar um consenso.
- ▶ Quando tal consenso não se efetive, entra em ação o Comité Europeu para a Proteção de Dados, emitindo pareceres ou adotando decisão vinculativa.

### **I – Vias de recurso, responsabilidade civil e sanções**

#### ☐ Mecanismos de tutela

- direito a apresentar uma reclamação a uma autoridade de controlo – artigo 77.º do RGPD e 32.º da LERGPD
- ação judicial contra uma autoridade de controlo – artigo 78.º e 34.º da LERGPD
- ação judicial contra um responsável pelo tratamento ou subcontratante – artigo 79.º do RGPD e 34.º n.º 4 da LERGPD

#### ☐ Responsabilidade civil – artigo 82.º do RGPD e 33.º da LERGPD

- Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do Regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o regulamento. O subcontratante é responsável apenas se não tiver cumprido as obrigações decorrentes do regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.

#### ☐ Coimas

RGPD (Art.º 83.º e 84.º) e 37.º e 38.º da LERGPD

Coimas até €20.000.000 ou 4% do volume de negócios anual a nível mundial, em caso de violação de:

- o Princípios básicos do tratamento, incluindo as condições do consentimento
- o Os direitos dos titulares dos dados
- o Transferências internacionais de dados
- o As obrigações ao abrigo do capítulo IX (situações específicas de tratamento)
- o Incumprimento de uma ordem de limitação ou suspensão de fluxos ou violação do direito de acesso

As regras relativas às (outras) sanções (art.º 84.º) aplicáveis perante a violação das disposições do RGPD que não são sujeitas a coimas, são determinadas pelos Estados-Membros.

#### **COMUNICAÇÕES ELETRÓNICAS**

A União Europeia começou a dar maior atenção à regulação jurídica das comunicações eletrónicas a partir de 2002, altura em que foi adotado um pacote legislativo composto pelos seguintes atos:

- Diretiva 2002/19/CE, relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos
- Diretiva 2002/20/CE, relativa à autorização de redes e serviços de comunicações eletrónicas
- Diretiva 2002/22/CE, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas.

A preocupação era assegurar que todos os Estados Membros se dotassem de redes e serviços de comunicações eletrónicas e que as suas operações pudessem ser efetivamente reguladas observando regras mínimas quanto às relações entre autoridades reguladoras nacionais e os prestadores desses serviços e às relações estabelecidas entre estes últimos e os consumidores.

A regulação das comunicações eletrónicas é pautada por preocupações de regulação social, com vista a mitigar as assimetrias entre as populações com base num conceito de “serviço universal”

O Estado português em cumprimento deste pacote legislativo, adotou a Lei n.º 5/2004, de 10 de fevereiro designada por Lei das Comunicações Eletrónicas.

A transformação digital determinou a transição da telefonia vocal para o acesso a internet, o que motivou a adoção da Diretiva (EU) 2018/1972, de 11 de dezembro, que estabelece o Código Europeu das Comunicações Eletrónicas. O Código visa assegurar a liberdade de oferta de serviços e redes de comunicações eletrónicas, mas os serviços devem ser prestados com um nível particularmente elevado de segurança. Os fornecedores de redes públicas de comunicações eletrónicas ou de serviços de comunicações eletrónicas acessíveis ao público, ou de ambos os serviços, estão obrigados a tomar medidas para salvaguardar a segurança das suas redes e serviços e impedir ou minimizar o impacto dos incidentes de segurança.

Para defesa dos direitos dos consumidores, o Código impõe ao fornecedor dos serviços que especifique no contrato celebrado com o utilizador, as medidas que adotará em caso de incidentes de segurança, de ameaças e de vulnerabilidades, e também que esclareça o regime indemnizatório e de reembolso aplicável no caso de dar uma resposta inadequada a um incidente de segurança.

Lei n.º 16/2022, de 16 de agosto  
Aprova a Lei das Comunicações Eletrónicas, transpondo as Diretivas 98/84/CE, 2002/77/CE e (UE) 2018/1972, alterando as Leis n.os 41/2004, de 18 de agosto, e 99/2009, de 4 de setembro, e os Decretos-Leis n.os 151-A/2000, de 20 de julho, e 24/2014, de 14 de fevereiro, e revogando a Lei n.º 5/2004, de 10 de fevereiro, e a Portaria n.º 791/98, de 22 de setembro



- **Regime especial de protecção de dados pessoais no setor das comunicações eletrónicas**
  
- **A Lei n.º 41/2004 de 18/08**
  - o Antecedentes- transposição das Diretivas 2002/58/CE e 2009/136/CE
  - o Complemento à Lei 58/2019- legislação especial que visa garantir a segurança e confidencialidade de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas (art. 1º, n.º 2)
  - o Âmbito objetivo:
    - Comunicações eletrónicas- noção
      - Qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público- art. 2º, n.º 1, al. a)
      - São serviços de comunicações eletrónicas os previstos no art. 3º, al. x) da Lei 5/2004 de 10/02: sistemas e equipamentos de comunicação por cabo (telefone, televisão e internet por cabo), por meios radioelétricos (radiodifusão sonora e televisiva), por meios óticos (fibra ótica), ou outros meios eletromagnéticos como redes de satélites e redes de telefone e internet móveis
      - Restrição do conceito de comunicação electrónica para efeitos da Lei 41/2004- exclusão de informações enviadas no âmbito de um serviço de difusão ao público em geral que não possam ser relacionadas com o assinante de um serviço de comunicações eletrónicas ou com qualquer utilizador identificável, como é o caso da radiodifusão sonora e televisiva, e TDT- art. 2º, n.º 2
  - o Âmbito subjetivo:
    - Pessoas singulares (e excecionalmente, pessoas coletivas - art. 1º, n.º 3)
    - Utilizador- pessoa singular que utiliza um serviço de comunicações eletrónicas acessível ao público para fins privados ou comerciais, não sendo necessariamente o assinante - art. 2, n.º 1, c)
      - Assinante é a pessoa que é parte num contrato de fornecimento de redes ou serviços com uma empresa
    - Empresas que prestam serviços de comunicações eletrónicas acessíveis ao público e fornecedores de redes públicas de comunicações
  - o Obrigações das empresas que prestam serviços de comunicações eletrónicas:
    - Dever de adotar medidas de segurança técnicas e organizacionais eficazes para garantir a segurança dos seus serviços e a segurança da rede, adequadas à prevenção dos riscos existentes, pelo menos, o controlo do acesso a dados pessoais - art. 3º, n.º 1, 3, 9 - controlo das medidas através de auditorias realizadas pelo ICP- ANACOM

- Dever de notificar a CNPD e o assinante ou utilizador da ocorrência de violação de dados pessoais tratados no contexto da prestação do serviço de comunicações eletrónicas, isto é, falha de segurança que provoque, de modo acidental ou ilícito, a destruição, perda, alteração, divulgação, acesso não autorizado a dados pessoais dos utilizadores – art. 3º-A e art. 2º, n.º 1, al. g)
- Dever de garantir a inviolabilidade do conteúdo das comunicações eletrónicas e respetivos dados de tráfego realizadas através de redes e serviços de comunicações eletrónicas acessíveis ao público- art. 4º, n.º 1 – proibição de escutas ou armazenamento de dados das comunicações, com exceção das gravações legalmente autorizadas de comunicações e dados de tráfego realizadas, no âmbito de práticas comerciais lícitas, para prova de uma transação ou no âmbito de uma relação contratual, se o titular tiver sido informado e tiver dado o seu consentimento prévio e expresso – art. 4º, n.º 2 e 3 – cfr. DL 134/2009 (regime dos call centres)
- Dever de não armazenar e aceder à informação armazenada no equipamento terminal de um assinante ou utilizador (exceto aquele armazenamento que for tecnicamente necessário para transmitir as comunicações eletrónicas pela rede ou para prestar um serviço expressamente solicitado pelo assinante ou utilizador, e desde que este tenha dado o seu consentimento prévio, livre e esclarecido sobre as finalidades do processamento) – art. 5º
- Dever de eliminar os dados de tráfego dos assinantes e utilizadores depois de deixarem de ser necessários para a transmissão da comunicação, (ou torná-los anónimos)- art. 6º, n.º 1 - dados de tráfego são quaisquer dados tratados para efeitos de envio de uma comunicação através da rede de comunicações eletrónicas ou para efeitos de faturação da mesma- art- 2º, n.º 1, al. d); com exceção dos tratamentos de dados de tráfego permitidos:
  - Para efeitos de faturação dos assinantes e pagamentos de interligações, podem ser tratados os seguintes dados de tráfego: identificação, endereço e tipo de posto do assinante; número total de unidades a cobrar, tipo, hora de início e duração e volume de dados transmitidos; data do serviço e número chamado; pagamentos e avisos- art. 6º, n.º 2 – estes dados só podem ser tratados enquanto forem necessários para os fins a que se destinam, ou seja, enquanto a fatura puder ser contestada ou o pagamento reclamado – art. 6º, n.º 3 – e, antes do tratamento, as empresas devem informar os assinantes e utilizadores acerca dos dados a tratar, finalidades e duração do tratamento, e eventual comunicação a terceiros – art. 6º, n.º 4
  - Para comercialização e fornecimento de serviços de comunicações eletrónicas ou para prestação de serviços de valor acrescentado, desde que o assinante ou utilizador tenha dado o seu prévio e expresso consentimento, com respeito pelos princípios da proporcionalidade e adequação do tratamento às finalidades visadas (o

- consentimento do utilizador ou assinante para este efeito é livremente revogável, em qualquer altura) - art. 6º, n.º 4
- Para efeitos judiciais – art. 6º, n.º 7- para prevenção, investigação, detecção e repressão de infracções penais graves como terrorismo e criminalidade organizada (aplica-se aos dados de tráfego, dados de localização, dados de identificação do assinante e utilizador registado, mas já não ao conteúdo das comunicações)
- Dever de não proceder ao tratamento de dados de localização que identifiquem o utilizador - art. 7º, n.º 1 - dados de localização são quaisquer dados que indicam a posição geográfica do equipamento terminal do utilizador do serviço de comunicações eletrónicas – art. 2º, n.º 1, al. e) – o tratamento destes dados só é permitido nos seguintes casos:
- Chamadas de emergência médica (112) – art. 7º, n.º 2. Esta disposição foi alterada pela Lei 16/2022 passando a ter a seguinte redação «2 - É permitido o registo, o tratamento e a disponibilização de dados de localização, nomeadamente da informação sobre a localização do chamador, às organizações com competência legal para receber ou tratar comunicações de emergência, para efeitos de resposta a essas comunicações.
  - Para prestação de serviços de valor acrescentado, desde que o assinante ou utilizador tenha dado o seu consentimento prévio e expresso – art. 7º, n.º 3 – o consentimento deve ser precedido da informação sobre os dados a tratar, fins e duração do tratamento, e eventuais transmissões – art. 7º, n.º 4 – o consentimento é livremente revogável e o utilizador deve ter ao seu alcance um meio simples de recusar o tratamento dos dados de localização em cada comunicação eletrónica que efetua – art. 7º, n.º 5
- Dever de emitir faturas não detalhadas, exceto se o assinante o solicitar; porém, devem ter em consideração o direito à privacidade dos utilizadores, que deve ser devidamente conciliado com o direito do assinante a receber uma fatura detalhada- art. 8º, n.º 1 e 2
- Dever de disponibilizar aos utilizadores e assinantes um meio simples e gratuito que garanta a confidencialidade do número da linha chamadora, linha a linha e chamada a chamada (a pedido do chamador ou do chamado), e rejeitar chamadas de entrada não identificadas - art. 9º, n.º 1, 2 e 3 – exceto nos casos do art. 10º:
- A pedido escrito, devidamente fundamentado, de um assinante que pretenda determinar a origem de chamadas perturbadoras da paz familiar ou intimidade da vida privada – art. 10º, n.º 1
  - Chamadas de emergência médica – art. 10º, n.º 2. Os n.ºs 3 e n.º 4 deste artigo foi alterado pela Lei 16/2022 «3 - As empresas referidas no n.º 1 devem igualmente anular, numa base linha a linha, a eliminação da apresentação da linha chamadora, bem como registar e tratar os dados de localização de um assinante ou utilizador, nomeadamente

a informação sobre a localização do chamador, no caso previsto no n.º 2 do artigo 7.º, por forma a disponibilizar esses dados às organizações com competência legal para receber ou tratar comunicações de emergência, para efeitos de resposta a essas comunicações. «4 - Nos casos dos números anteriores deve ser obrigatoriamente transmitida informação prévia ao titular dos referidos dados sobre a transmissão dos mesmos, ao assinante que os requereu nos termos do n.º 1 ou às organizações com competência legal para receber ou tratar comunicações de emergência, nos termos do n.º 3.

- Dever de disponibilizar um meio simples e gratuito que permita aos assinantes impedir o reencaminhamento de chamadas efetuado para o seu equipamento terminal – art. 11º
- Dever de não incluir os dados pessoais dos assinantes em listas (eletrónicas ou impressas) – a não ser que os assinantes deem previamente o seu consentimento, depois de informados dos fins a que se destinam e das possibilidades de utilização das listas, decidindo sobre os dados a incluir – art. 13º, n.º 1 e 2 – além de garantir que os assinantes podem exercer os seus direitos de acesso, retificação, atualização e eliminação a todo o tempo – art. 13º, n.º 3

o Comunicações eletrónicas não solicitadas

- O direito à reserva da intimidade da vida privada engloba uma dimensão de direito ao sossego, recolhimento e a não ser perturbado por comunicações indesejadas
  - O vulgarmente designado “spam” consiste no envio de comunicações eletrónicas em massa, com finalidades comerciais ou não (ajuda, informações, divulgação de eventos, etc.), sem prévia solicitação do destinatário – os principais incómodos para o recetor deste tipo de mensagens são a perda de tempo e a diminuição da capacidade de armazenamento dos sistemas eletrónicos, além de implicar um acréscimo indireto do custo de acesso às redes de comunicações eletrónicas tendo em conta o impacto no volume global de tráfego de dados- aos meios técnicos disponíveis (programas informáticos que filtram e bloqueiam mensagens não solicitadas) juntam-se os meios estritamente jurídicos (lei)
- O endereço de correio eletrónico é um dado pessoal, nos termos do art. 3º, al. a) da LPD, pelo que só pode ser tratado com consentimento prévio, expresso e esclarecido, do seu titular (art. 6º da LPD), que pode ser sempre revogado se o tratamento for feito para fins de marketing direto (art. 12º, al. b) LPD)
- A lei 41/2004 foi alterada pela Lei 46/2012, que lhe aditou os art. 13ºA e 13ºB, destinados a regular a questão das comunicações eletrónicas não solicitadas, questão essa até então tratada pelo art. 22º do DL 7/2004 (Lei do Comércio Eletrónico), agora revogado
- Regime legal das comunicações eletrónicas não solicitadas para fins de marketing direto- art. 13º-A e 13ºB:

- Noção: comunicações não solicitadas para fins de marketing direto
  - o Comunicações eletrónicas por telefone fixo ou móvel (chamadas automáticas e mensagens sms, ems e mms), por correio eletrónico (email), ou por telecópia (fax)
  - o Mensagens enviadas sem haver um pedido prévio e expresso formulado pelo destinatário para receber uma mensagem concreta
  - o Com objetivo de promover a comercialização de bens e serviços através do estabelecimento de uma relação personalizada com os clientes que permita conhecer adequar os bens e serviços às suas necessidades
- Adoção de um sistema de *opting in*, ou listas brancas, para os destinatários que sejam peessoas singulares
  - o A lei exige, como condição de legitimidade para o envio de mensagens eletrónicas não solicitadas, o consentimento prévio do destinatário- art. 13º-A, n.º 1
  - o Excecionalmente, o art. 13ºA, n.º 3, admite a um fornecedor de produtos ou serviços o envio de comunicações eletrónicas não solicitadas a clientes, nas seguintes condições:
    - tenha obtido lícitamente os dados pessoais dos clientes no momento da transação comercial, e lhes tenha dado, de forma clara e explícita, a possibilidade de recusarem a utilização dos seus dados de contacto eletrónicos, sem que estes tenham recusado
    - cada uma das mensagens não solicitadas se destine a promover a comercialização de bens e serviços análogos aos que o cliente adquiriu em virtude da transação anterior, e contenha um meio fácil e gratuito de recusar futuras mensagens do mesmo género
  - o O incumprimento das normas constantes do art. 13º, n.º 1 e 3, constitui contraordenação punível com coima, nos termos do art. 14º, n.º 1, al. f) e g)
- Adoção do sistema de *opting out*, ou listas negras, para os destinatários que sejam peessoas coletivas (associações, fundações, sociedades comerciais, etc.)
  - o O art. 13ºA, n.º 2, permite o envio de mensagens de marketing direto não solicitadas a pessoas coletivas, sem consentimento prévio
  - o Contudo, as pessoas coletivas, através dos representantes legais, têm o direito de se opor ao envio deste tipo de comunicações para futuro,

inscrevendo-se na lista da Direção Geral do Consumo- art. 13º A, n.º 2

- o O incumprimento do disposto no art. 13º, n.º 2, constitui contraordenação punível com coima, nos termos do art. 14º, n.º 1, al. f)
- É proibido, e portanto ilícito, o envio de mensagens de correio eletrónico para fins de marketing direto nas condições do art. 13º-A, n.º 4:
  - Ocultando ou dissimulando a identidade da pessoa em nome de quem é enviada a comunicação
  - Que não ostentem claramente quem é a entidade que promove a iniciativa (o anunciante), a natureza publicitária da comunicação, e as condições concretas das ofertas, concursos ou jogos promocionais (descontos, prémios, brindes, concursos...) – art. 21º, al. a), b) e c) DL 7/2004
  - Que não indique, em cada mensagem, um meio de contacto válido (endereço de email) para o qual o destinatário recusar o envio, para futuro, dessas comunicações
  - Que incentive os destinatários a visitar sítios na internet que não cumpram as condições acima referidas no art. 21º do DL 7/2004 – identificação inequívoca da entidade responsável pela informação prestada, do carácter publicitário da mensagem e descrição pormenorizada das condições promocionais
- o O desrespeito pelo art. 13ºA, n.º 4, em qualquer das suas modalidades, implica a prática de uma contraordenação punível nos termos do art. 14º, n.º 1, al. h)
- Em qualquer dos casos de envio legítimo de comunicações de marketing direto (para pessoas singulares ou coletivas), o destinatário pode recusar, a qualquer momento, sem custos e encargos, e sem ter de indicar motivo, o envio dessas comunicações para o futuro
- A entidade que promove o envio de comunicações eletrónicas para fins de marketing direto está ainda obrigada a manter uma lista atualizada de todos os destinatários pessoas singulares a quem podem licitamente enviar estas comunicações (lista branca), porque as deram o seu consentimento expresso ou que não recusaram esse envio no momento em que realizaram certa transação comercial – art. 13ºB, n.º 1 e art. 13º-A, n.º 1 e 3
  - o A falta da lista em questão constitui contraordenação punível nos termos do art. 14º,

n.º 1, al. i) (e a exigência de qualquer quantia aos destinatários como contrapartida da inclusão na lista é punida pela alínea j) do mesmo artigo)

- A entidade que promove estas comunicações está também obrigada a consultar uma lista de pessoas coletivas que se opõem à receção de comunicações não solicitadas para fins de marketing direto (lista negra), disponibilizada a seu pedido pela Direção-Geral do Consumidor – art. 13ºB, n.º 2 a 5 (esta lista de âmbito nacional é atualizada mensalmente, sendo integrados os endereços eletrónicos das pessoas coletivas cujos representantes preenchem um formulário eletrónico no portal do consumidor)

o Tutela administrativa e jurisdicional

- O incumprimento da presente Lei 41/2004 é controlado e fiscalizado por duas entidades administrativas, com competências repartidas em função da matéria: art. 15º
  - ICP-ANACOM- entidade reguladora em matéria de telecomunicações e comunicações eletrónicas – fiscaliza e pune o incumprimento das regras relativas à prestação de serviços de comunicações eletrónicas (art. 3º, n.º 1, 2, 3 e 10, art. 4º, n.º 1 e 2, art. 9º, art. 11º, art. 13ºE e art. 14º, n.º 1, al. m))
  - CNPD- entidade com competência exclusiva em matéria de tratamento de dados pessoais – fiscaliza e pune o incumprimento das regras relativas à proteção de dados pessoais de pessoas singulares (art. 3º, n.º 9, 3ºA, art. 4º, n.º 3, art. 5º, art. 6º, art. 7º, art. 8º, n.º 1, 2 e 4, art. art. 10º, art. 13º, art. 13ºA, n.º 1 a 4, art. 13ºB, n.º 1 e 3, art. 14º, n.º 1, al. l))
- A título preventivo, a CNPD e o ICP\_ANACOM podem elaborar regulamentos, publicitar informações e códigos de conduta e prestar informações a pedido dos interessados – art. 13º-D e 13º-E
- Detetada alguma infração à presente legislação, a entidade competente – CNPD ou ICP-ANACOM – notifica o infrator desse facto e dá-lhe a possibilidade de se defender, no prazo de 10 dias, findo o qual toma uma deliberação com força obrigatória geral, exigindo ao infrator que cesse o incumprimento – art. 13ºF
- Além de exigir a cessação da conduta ilícita, a entidade administrativa competente instaura um processo de contraordenação e pune o infrator com a aplicação de uma coima (art. 14º), além de outras sanções acessórias (art. 15ºA) e de eventual sanção pecuniária compulsória destinada a fazer cumprir a decisão tomada (art. 15ºC) – art. 14º, n.º 3 e 4
  - Constituem contraordenação punível com coima de valor mínimo 1500€ ou 5000€ e máximo 25000€ ou 5000000€, consoante o agente seja pessoa singular ou coletiva, a violação das normas constantes dos artigos 3º, n.º 1, 3 e 10, 3ºA, n.º 1 a 6, 9 e 10, 4º, n.º 1, 2 e 3, 5º, 13ºA, n.º 1, 2, 3 e 4, 13ºB, n.º 3, 13ºE e 13ºD
  - Constituem contraordenação punível com coima de valor mínimo 500€ ou 2500€ e máximo 20000€ ou 2500000€,

consoante o agente seja pessoa singular ou coletiva, a violação das normas constantes dos artigos 3ºA, n.º 7, 8, 9 e 10, 6º, 7º, 8º, n.º 1, 2 e 4, 9º, 10º, 11º, e 13º

- A negligência e tentativa são puníveis, sendo as coimas reduzidas a metade nos respetivos valores mínimos e máximos – art. 14º, n.º 5

## **DIREITOS DE AUTOR E DIREITOS CONEXOS**

### **Capítulo IV - A PROTEÇÃO JURÍDICA DA PROPRIEDADE INTELECTUAL E FIGURAS AFINS**

A propriedade intelectual – conceito e princípios básicos vigentes

- O direito de propriedade é um direito pleno que incide sobre uma coisa, permitindo ao seu titular usá-la (utilização direta), fruí-la (receber os seus frutos e rendimentos) e dispor dela (transmiti-la e onerá-la), com exclusividade (isto é, com exclusão de qualquer outra pessoa) (art. 1305º do CC)
- Noção de coisa prevista no art. 202º do Código Civil: “tudo aquilo que pode ser objecto de relações jurídicas”- esta noção engloba coisas corpóreas (coisas com existência material, que lhes permite serem apreendidas pelos sentidos) e coisas incorpóreas (coisas sem suporte material, insusceptíveis de apreensão sensorial, com existência no mundo jurídico)
- O direito de propriedade pode incidir sobre coisas corpóreas ou incorpóreas:
  - o Se incide sobre coisas corpóreas, é regulado pelo CC (art. 1302º do CC)
  - o Se incide sobre coisas incorpóreas, é regulado por legislação especial (art. 1303º do CC), sendo a mais importante:
    - Código dos Direitos de Autor e Direitos Conexos- propriedade sobre bens intelectuais (obras literárias, científicas e artísticas, e prestações de intérpretes, artistas, executantes e produtores)
    - Código da Propriedade Industrial – propriedade sobre bens industriais (processos técnicos de produção e desenvolvimento de atividades económicas- marcas, patentes, modelos de utilidade, nomes e insígnias de estabelecimento, logótipos, denominações de origem, etc.)
    -

As violações dos direitos de propriedade intelectual perpetradas por meios informáticos:



- A proteção jurídica dos direitos de autor e conexos pré-existe ao advento da sociedade da informação, mas, como o uso massificado das novas tecnologias da informação, ganhou novos contornos
- Hoje, os mecanismos eletrónicos que permitem reproduzir, registar, gravar, e copiar obras protegidas estão disponíveis para qualquer cidadão, a preços acessíveis (fotocopiadoras, scanners, computadores, gravadores de CD e DVD, etc.)
- A acessibilidade e facilidade de circulação de informação nas redes abertas de comunicação, designadamente na internet, veio alargar exponencialmente o círculo de destinatários, potenciais e efetivos, de conteúdos protegidos por direitos de autor e conexos
- A ideia de que a reprodução de uma obra protegida implicava necessariamente a multiplicação de exemplares em suporte físico foi posta de parte, face à possibilidade de reprodução, transferência e acesso em rede meramente eletrónicos, sem necessidade de usar diretamente um suporte material
- A esta banalização dos meios eletrónicos de reprodução e comunicação pública de conteúdos protegidos, acresce ainda o desconhecimento e falta de consciencialização dos cidadãos em geral sobre a ilicitude dos seus atos em matéria de propriedade intelectual, além de uma certa sensação de impunidade
- Face à falibilidade e ineficácia das medidas de carácter tecnológico utilizadas para proteger obras, prestações e produções, o direito foi chamado a tutelar os direitos respetivos através da incriminação de condutas lesivas
- Noutro sentido, a informática veio criar novos valores intelectuais que mereciam protecção jurídica mas dificilmente tinham acolhimento no conceito de obra protegida, motivando a criação de legislação especial – referimo-nos, em particular, à proteção jurídica de bases de dados eletrónicas e programas de computador

## O regime jurídico de protecção dos direitos de propriedade intelectual previsto pelo **Código dos Direitos de Autor e Direitos Conexos**

- **Os direitos de autor**
  - Direito de propriedade sobre uma obra
    - Conceito de obra: criação intelectual original do domínio literário, científico ou artístico, exteriorizada por qualquer modo (art. 1º, n.º 1, e art. 2º, n.º 1 CDA), por exemplo:
      - Livros, folhetos, revistas, jornais
      - Conferências, lições
      - Obras dramáticas e a sua encenação
      - Obras cinematográficas, televisivas, fonográficas, videográficas e radiofónicas
      - Desenho, pintura, escultura, arquitectura
      - Fotografia, desde que seja uma criação intelectual pela escolha do objecto ou condições de execução
    - Equiparação às originais de certas obras: traduções, arranjos, dramatizações, transformações da obra, sumários e compilações de obras protegidas e compilações de textos legais e outros (art. 3º CDA)
    - Notas:
      - o direito sobre a obra ou prestação é independente do direito de propriedade sobre as coisas materiais que sirvam de suporte à sua fixação ou comunicação- art. 10º, n.º 1 CDA

- o direito de autor protege uma determinada forma de expressão ou exteriorização de ideias, princípios e conceitos, e não as ideias e princípios em si, as quais não são suscetíveis de apropriação exclusiva (por exemplo, uma mesma história pode ser contada e escrita de modos completamente distintos, dependendo da sensibilidade escrita e literária do autor)
- a criação intelectual tem de ser original, isto é, tem que ter mérito literário, artístico ou científico, reflectindo a personalidade do seu autor, independentemente da avaliação positiva ou negativa que dela se faça
- o Conteúdo do direito de autor- art. 9ª CDA- engloba dois tipos de sub-direitos:
  - Direitos de natureza patrimonial
    - Compreende:
      - o Direito ao uso, fruição e disposição da sua obra em exclusivo, no todo ou em parte- art. 67º CDA
      - o Direito a autorizar o uso e fruição da obra por terceiro, total ou parcialmente
    - Direitos disponíveis- art. 40º CDA:
      - o O autor pode autorizar a utilização da obra por terceiro- art. 41º CDA
      - o O autor pode transmitir ou onerar, no todo ou em parte, o conteúdo patrimonial de seu direito sobre a obra- art. 42º, 43º, 44ª CDA
    - Direitos com duração limitada: 70 anos após a morte do autor- art. 31º CDA- findo esse prazo, a obra cai no domínio público- 38º CDA
    - Exercício: a gestão dos direitos de autor e conexos pode ser feita directamente pelo titular dos direitos ou por intermédio de entidades de gestão colectiva de direitos de autor (art. 72º CDA):
      - o Entidades de gestão colectiva: associações e organismos nacionais ou estrangeiros que fazem a gestão dos direitos patrimoniais de autor e conexos e agem em defesa dos direitos morais- Lei 83/2001 de 30/08 (são consideradas pessoas colectivas de utilidade pública e estão sujeitas a inscrição do IGAC)
  - Direitos de natureza moral ou pessoal
    - Compreendem:
      - o Direito à paternidade da obra- art. 9º, n.º 3, 27º, 56º CDA
      - o Direito à integridade e genuinidade da obra- art. 9º, n.º 3, e 56º, n.º 1, 59º CDA
      - o Direito de retirada de circulação- art. 62º CDA
    - Direitos inalienáveis e irrenunciáveis- 56º CDA
    - Direitos imprescritíveis, perpetuando-se após morte do autor- 56º, n.º 2 CDA
    - Exercício por si mesmo, pelos herdeiros, ou pelo Estado (art. 57º CDA)
- o Aquisição do direito de autor
  - No momento em que a obra é feita

- Independente de registo, depósito ou outras formalidades (art. 213º CDA) - salvo títulos de obras não publicadas ou títulos de jornais e revistas (214º CDA)
- o Titularidade
  - Os direitos morais pertencem sempre ao criador intelectual da obra (autoria), e em princípio, os direitos patrimoniais também (art. 11º, n.º 1 CDA), mas pode haver distinção entre autoria e titularidade quanto a estes em duas situações:
    - Obra feita por encomenda ou por conta de outrem (no âmbito de contrato de trabalho ou de contrato de prestação de serviços) - em princípio, os direitos patrimoniais cabem ao criador intelectual, mas as partes podem convencionar que estes ficam a pertencer originalmente ao destinatário da obra (art. 14º, n.º 1, CDA), sem prejuízo de ter de dar uma remuneração especial ao criador intelectual em certos casos (art. 14º, n.º 4 CDA)
    - Obras coletivas - os direitos patrimoniais de autor sobre as obras realizadas por vários autores sob organização de uma entidade e divulgadas e publicadas em seu nome pertencem a essa entidade (art. 16º e 19º CDA)
    - Nas obras em colaboração (obras criadas por vários autores que é divulgada e publicada em nome de todos ou algum dos colaboradores), os direitos patrimoniais cabem a todos eles, em compropriedade (art. 16º e 17º CDA)
- o Proibição de usar e fruir uma obra protegida, sem autorização expressa e escrita do autor (art. 9º, n.º 2, e 67º CDA)
  - Proíbe-se a utilização da obra, por qualquer modo, segundo a sua espécie e natureza, que podemos sucintamente resumir em 3 modalidades fundamentais (68º CDA):
    - Reprodução
      - o Conceito amplo de reprodução: produção de originais ou cópias da obra, totais ou parciais, por via direta ou indireta, por qualquer meio e independentemente do respectivo suporte ou forma (art. 68º, n.º 2, al. i) CDA)
      - o Exclusão dos actos de reprodução temporária transitórios que constituam parte integrante e essencial de um processo tecnológico com o único objetivo de permitir uma transmissão na rede ou uma utilização legítima da obra (art. 75º, n.º 1)
    - Comunicação pública
      - o Comunicação a terceiros do conteúdo da obra (art. 68º, n.º 2, al. e) CDA)
      - o Divulgação da obra através da sua representação, recitação, exibição, execução, transmissão, exposição ao público, etc. (art. 6º, n.º 3, e 68º, n.º 2, al. b) CDA)
      - o Colocação à disposição do público em rede (art. 68º, n.º 2, al. j) CDA)
    - Distribuição de originais ou cópias (art. 68º, n.º 2, al. f) CDA)
      - o Publicação - fabrico de exemplares à disposição do público (art. 6º, n.º 2, e 68º, n.º 2, a), CDA)

- A regra da proibição de utilizar a obra protegida tem as exceções previstas no art. 75º, n.º 2 CDA, que constituem utilizações lícitas da obra, sem o consentimento do autor, tendo em conta os fins visados:
  - Fins privados
    - Reprodução para fins exclusivamente privados, em papel ou suporte similar feita por tipo de técnica fotográfica (fotocópias e fotografias)
    - Reprodução, por qualquer meio, feita por pessoa singular para uso privado sem fins comerciais diretos ou indiretos (utilizações e cópias feitas por qualquer técnica, em qualquer tipo de suporte material, incluindo suporte eletrónico)
  - Fins informativos
    - Reprodução e colocação à disposição do público pelos meios de comunicação social de discursos e conferências ou de fragmentos de obras literárias ou artísticas integrada em relatos de acontecimentos atuais com fins informativos justificados
  - Fins científicos e educativos
    - Reprodução de obras por bibliotecas, museus, arquivos de centros de documentação e investigação públicos sem vantagens comerciais directas ou indirectas e comunicação à disposição do público das obras que possuem
    - Reprodução, distribuição e disponibilização públicas de partes de uma obra publicada para fins de ensino e educação e inclusão de obras e partes de obras em obras destinadas ao ensino
  - Fins de crítica e fundamentação
    - Citações ou resumos de obras alheias em obra própria para se apoiar nela ou para a criticar
  - Fins publicitários
    - Utilização da obra para efeitos de publicidade relacionada com a exibição pública ou venda de obras artísticas, na medida em que seja necessário para promover o evento e não vise qualquer outra finalidade comercial
- Mas, para serem lícitas, as utilizações para os fins previstos no art. 75º, n.º 2 do CDA, tem que cumprir as condições do art. 76º CDA:
  - Indicar o autor e editor, título da obra e circunstâncias identificativas (por ex. edição e ano)
  - A integração total ou parcial de uma obra alheia não deve confundir-se com a obra própria (citação entre aspas, com indicação da obra e autor), e a reprodução e citação não podem ser tão extensas que prejudiquem o interesse pela obra original (critério substancialista)
  - Atribuição de uma remuneração económica equitativa ao autor e editor, em certos casos
- A lei permite ainda a reprodução de uma cópia de obra protegida pelo seu utilizador legítimo no art. 82º CDA:

- Reprodução de um exemplar único para fins de interesse exclusivamente científico ou humanitário de obras não disponíveis no comércio ou de obtenção impossível
- Reprodução para uso exclusivamente privado, desde que não atinja a exploração normal da obra e não cause prejuízo injustificado aos interesses legítimos do autor, não podendo ser utilizada para quaisquer fins de comunicação pública ou comercialização

#### O Proteção jurídica

- Fundamento (art. 67º, n.º 2 CDA): garantia das vantagens patrimoniais da exploração da obra, como forma de estimular a criação de obras intelectuais e remunerar a criatividade do autor
- A proteção dos direitos do autor sobre a obra é independente de registo, depósito ou outra formalidade- art. 12º e 213º CDA
- Âmbito de protecção:
  - Abrange integralmente a obra e o título da obra, desde que seja original e não possa confundir-se com outro título de obra do mesmo género anteriormente divulgada ou publicada- art. 4º
    - o Mas nota: o título pode ser livremente citado e utilizado, desde que não sirva para identificar uma outra obra do mesmo género!
  - Exclusão de proteção a certas obras: notícias do dia e relatos de acontecimentos diversos com carácter de simples informação, requerimentos e textos apresentados por escrito perante autoridades ou serviços públicos, textos proferidos em debates públicos e discursos políticos (art. 7ª CDA)

#### • Os direitos conexos

- o Direitos que não incidem sobre uma obra propriamente dita, mas uma utilização que dela é feita ( art. 176º, n.º 1, CDA)- podem ser de 3 tipos:
  - Direitos sobre prestações de artistas, intérpretes ou executantes (actores, cantores, músicos, bailarinos, intérpretes ou executantes, por qualquer forma, de obras literárias e artísticas) - art. 176º, n.º 1 e 2 CDA
  - Direitos dos produtos de fonogramas e videogramas (pessoas que procedem ao registo de obras ou prestações constituídas por som e imagem, pela primeira vez, através fixação em suporte material) - art. 176º, n.º 1, 3, 4 e 5 CDA
  - Direitos dos organismos de radiodifusão (entidade que efectua emissões de radiodifusão sonora ou visual, por fios ou sem fios) - art. 176º, n.º 1 e 9 CDA
- o Nota: A concessão destes direitos não afecta a proteção jurídica dos direitos do autor da obra utilizada- art. 177º CDA (protecção cumulativa)
- o Conteúdo dos direitos conexos:
  - Direitos patrimoniais
    - O artista, intérprete ou executante tem o direito exclusivo de fazer ou autorizar a radiodifusão e comunicação ao público, a fixação da sua prestação, a reprodução, por qualquer meio, da

fixação das suas prestações, e a colocação à disposição do público (art. 178º, n.º 1, CDA)

- O produtor de fonogramas e videogramas tem o direito exclusivo de proceder à reprodução por qualquer meio, a distribuição ao público de cópias e a importação ou exportação, a difusão por qualquer meio e a colocação à disposição do público (art. 184º, n.º 1 e 2, CDA)
- Os organismos de radiodifusão têm o direito exclusivo de autorizar ou não a retransmissão das emissões, a sua fixação em suporte material, a colocação à disposição do público em rede ou com entradas pagas (art. 187º CDA)
- Direitos disponíveis e com duração limitada – 50 anos após a prestação, fixação ou emissão (art. 183º CDA)

▪ **Direitos morais**

- Direito a ser identificado como artista, intérprete ou executante da obra, em toda a divulgação da sua prestação (art. 179º CDA); direito a ser identificado como produtor (art. 185º, n.º 2 CDA)
- Direitos irrenunciáveis, inalienáveis e perpétuos

o **Proteção jurídica:**

- Proibição de usar e fruir da prestação, fonograma ou videograma, ou da emissão de radiodifusão
- Utilizações livres (art. 189º CDA), entre outras:
  - Reprodução para uso privado
  - Reprodução de excertos para fins informativos ou críticos
  - Utilização para fins exclusivamente científicos ou pedagógicos
  - Nos casos em que é permitida a utilização sem consentimento do autor (art. 75º, n.º 2, e 81º CDA)

• **Consequências da violação dos direitos de autor e direitos conexos**

o **Consequências criminais**

- Crime de usurpação (art. 195º e 197º CDA)
  - Utilização de obra alheia sem autorização
  - Divulgação ou publicação abusiva e compilação de obras inéditas
  - Excesso dos limites de autorização (incluindo o próprio autor)
- Crime de contrafação (art. 196º e 197º CDA)
  - Utilização não consentida de uma obra, como sendo criação sua (basta não indicar o autor) - violação de direitos patrimoniais e morais
- Aproveitamento de obra contrafeita ou usurpada (art. 199º CDA)
  - Venda, exposição, importação e exportação, e distribuição ao público de obras contrafeitas e usurpadas e de cópias não autorizadas de fonogramas e videogramas
- Violação de direito moral (art. 198º CDA)
  - Reivindicação da paternidade de obra que não lhe pertence
  - Atentados contra a genuinidade e integridade da obra, que a desvirtuem e possam afectar a honra e reputação do autor ou artista

- Apreensão e perda de coisas relacionadas com a prática do crime como consequência da condenação por algum dos referidos crimes (art. 201º CDA)
- o Consequências civis
  - Responsabilidade civil nos termos gerais (art. 211º CDA e 483º do CC)
    - Obrigação de indemnizar os danos patrimoniais e não patrimoniais causados por ato culposo (com dolo ou negligência) que viole os direitos de autor ou direitos conexos
    - No cálculo do valor indemnizatório, o tribunal deve ter em conta, além dos danos causados, o lucro obtido pelo infractor, as despesas suportadas para proteção dos direitos de autor, a gravidade da lesão e o grau de difusão ilícita da obra ou prestação
  - Medidas cautelares administrativas e judiciais destinadas a evitar a consumação de uma ameaça de violação iminente ou a impedir a continuação de uma violação efetiva de direitos de autor ou conexos (art. 209º e 210ºG CDA)
  - Medidas inibitórias cumulativas com a condenação, como a proibição de exercício de certas atividades ou profissões e encerramento temporário ou definitivo do estabelecimento 8art. 210º J CDA)
- Na última alteração ao CDA, foram aditadas normas punitivas (art. 217º e ss. CDA) que visam prevenir e desencorajar a eliminação das protecções electrónicas que visam impedir a reprodução ilícita de obras protegidas ou provar a autenticidade dos exemplares lícitamente distribuídas (*labels*)
  - Crime de neutralização de medidas eficazes de carácter tecnológico que se destinem a impedir ou restringir atos relativos a obras, prestações e produções protegidas não autorizados pelo seu titular - art. 217º e 218º CDA
  - Crime de detenção ou utilização de dispositivos, produtos ou componentes, ou de prestação de serviços concebidos, utilizados ou promovidos para neutralizar medidas eficazes de carácter tecnológico-art. 219º CDA
  - Crime de supressão, alteração das informações de gestão eletrónica dos direitos de autor e conexos ou de distribuição de prestações ou produções com alteração dessa informação (art. 223º e 224º CDA)

## Capítulo V – A CRIMINALIDADE INFORMÁTICA

- Criminalidade informática
  - o Em sentido amplo – abrange todos os crimes praticados através de meios de processamento eletrónico de dados (informática)

- o Em sentido estrito – crimes praticados através de meios automatizados que têm como objeto a própria informática, isto é, que lesam bens jurídicos que se prendem com a segurança, integridade, funcionalidade dos meios de tratamento automatizado de informação
- Direito penal- conceitos e princípios básicos
  - o Crime é uma conduta humana socialmente intolerável que é sancionada com uma pena criminal, desde que estejam reunidos todos os pressupostos legais:
    - Tipicidade – prevista numa norma legal de direito penal
    - Ilícitude – violadora de normas jurídicas que protegem bens jurídicos fundamentais da sociedade (a vida, a integridade física e moral, o património, etc.)
    - Culpa – praticada com dolo (consciência e intenção de agir e produzir o resultado danoso proibido por lei) ou negligência (desrespeito por um dever objectivo de cuidado que o direito lhe impõe naquelas circunstâncias)
    - Punibilidade – punida por lei com uma sanção criminal (prisão ou multa)
  - o O princípio da legalidade- art. 1º, n.º 1, CP
    - Só pode ser punido como crime o facto humano voluntário que se encontre descrito e seja punível com pena de prisão ou multa por lei anterior ao momento da sua prática
  - o As regras gerais que fixam o lugar da prática do facto e aplicação da lei penal portuguesa
    - O facto considera-se praticado no lugar em que o agente actuou ou devia ter actuado, mas também no lugar onde se produziu o resultado do facto se produziu- art. 7º, n.º 1, CP
    - Princípio geral de aplicação da lei portuguesa a factos praticados em território português, independentemente da nacionalidade do agente -art. 4º, al. a) do CP
  - o Valores para efeitos de aplicação da lei penal (art. 202º CP):
    - Valor elevado- 50 Ucs = 5100€
    - Valor consideravelmente elevado – 200 Ucs = 20400€
- O fenómeno da criminalidade informática
  - o As novas funcionalidades das tecnologias informáticas podem ser usadas em benefício das pessoas, mas também em seu prejuízo...
  - o As tecnologias informáticas, em particular os computadores e a internet, são frequentemente usados como meios para atingir objetivos criminosos - muitos crimes comuns podem ser praticados através de meios informáticos:
    - Crimes contra a honra - difamação e injúria (art. 180º, 181º, 182º, e 183º CP)
    - Crimes contra a reserva da vida privada – devassa da vida privada (art. 192º e 193º CP), violação de correspondência e telecomunicações (art. 194º CP)
      - crime de perturbação da vida privada– art. 190º, n.º 2, do CP: telefonar para habitação ou telemóvel com intenção de perturbar a vida privada, da paz e sossego
      - crime de devassa da vida privada - art. 192º CP: interceptação, gravação, transmissão ou divulgação de conversas, comunicações telefónicas, mensagens de correio eletrónico ou faturação detalhada, sem consentimento e com intenção de devassar a vida privada; captação, fotografia, filme ou



divulgação de imagem de pessoas, objectos ou espaços íntimos; observar ou escutar pessoas em locais privados; divulgar factos relativos à vida privada ou doença grave de outra pessoa (conceito mais íntimo e restrito de vida privada familiar e sexual)

- crime de devassa por meio da informática – art. 193º do CP: criação, manutenção ou utilização de ficheiro automatizado de dados pessoais referentes a convicções políticas, religiosas ou filosóficas, filiação partidária ou sindical, vida privada, origem étnica
- crime de violação de correspondência ou telecomunicações – art. 194º CP: abrir carta, encomenda ou qualquer escrito fechado dirigido a outra pessoa, sem o seu consentimento, ou tomar conhecimento do seu conteúdo por processos técnicos, ou impedir que o mesmo seja recebido pelo seu destinatário, intrometer-se no conteúdo de telecomunicações ou tomar conhecimento sem consentimento, e ainda divulgar o seu conteúdo
- crime de gravações e fotografias ilícitas - art. 199º do CP: gravações de imagem e som não autorizadas e sua utilização
- Crimes contra o património – burla informática (art. 221º CP) e abuso de cartão de garantia ou de crédito (art. 225º CP)
  - Burla informática e nas telecomunicações – art. 221º CP:
    - Interferência no tratamento de dados informáticos, e utilização incorreta ou não autorizada de dados, feitas com intenção de causar prejuízo ou obter benefício ilegítimo
    - Uso de programas ou dispositivos que alterem ou impeçam o normal funcionamento ou exploração dos serviços de telecomunicações com intenção de causar prejuízo ou obter benefício ilegítimo (baixadas ilegais e meios de evitar a facturação)
    - Bens jurídicos protegidos: património, fiabilidade dos dados informáticos, e segurança dos meios de pagamento eletrónico
  - Abuso de cartão de garantia ou de crédito – art. 225º CP
    - Utilização indevida de cartão de crédito ou garantia (obtido por furto ou abuso de confiança), levando o emitente bancário a fazer um pagamento, em prejuízo do emitente ou de terceiro
- Crimes contra a autodeterminação sexual – pornografia infantil (art. 176º CP)
- Crimes de usurpação, contrafação, e aproveitamento de obra contrafeita ou usurpada (art. 195º, 196º, 197º e 199º CDADC) e utilização para fins comerciais de bases de dados (art. 11º DL 122/2000) e programas de computador (art. 10º DL 252/94)
- Crimes de acesso indevido (art. 47º LERGD) e viciação e destruição de dados pessoais (art. 49º LERGD)
- O próprio uso de mecanismos, redes e sistemas informáticos, em si mesmo, comporta riscos para a segurança e confidencialidade da informação, mas também para a sua própria integridade e bom funcionamento - surgiram então

novos tipos de crimes, que tutelam bens jurídicos informáticos, punindo comportamentos que visam atingir os sistemas, redes, programas e dados informáticos (a informática é, no fundo, o próprio objeto ou alvo do crime):

- Falsidade informática – manipulação de dados informáticos e introdução de dados falsos para obter vantagens (*data didding*, *superzapping*, *salame*)
- Dano e sabotagem informática – disseminação de vírus (conjunto de instruções informáticas que se instalam no equipamento e sistema informáticos, destinadas a causar a alteração ou eliminação de dados e ficheiros, ou a tornar inutilizáveis programas ou o próprio sistema informático), e *trojan horse* (introdução de dados clandestinos num programa informático que se destinam a fazer e permitir instruções abusivas, comprometendo a segurança do sistema informático)
- Acesso e intercetação ilegítimos – acesso e captação de dados informáticos e do conteúdo de comunicações eletrónicas designadamente através de sistemas de *spyware*
- o Assim, a criminalidade informática encontra-se prevista e punida em legislação vária: CP, CDADC, LERGPD...
- A Lei do Cibercrime- Lei 109/2009 de 15/09
  - o Antecedentes
    - A lei 109/91 de 17/08 (lei da criminalidade informática)
    - A LC resulta da transposição para a ordem jurídica interna da Decisão-Quadro n.º 2005/222/JAI de 24/02 do Conselho da Europa, relativa a ataques contra sistemas de informação e da adaptação da ordem jurídica portuguesa à Convenção sobre Cibercrime do Conselho da Europa, de 2001, que Portugal assinou em 2001 e ratificou em 2009.
  - o Âmbito de aplicação
    - Definições:
      - Sistema informático – dispositivos que procedem ao tratamento automatizado de dados informáticos (computadores), outros dispositivos associados (impressoras, scanners), a rede que suporta a ligação entre eles (cabos) e o conjunto de dados informáticos tratados para o seu funcionamento, utilização, protecção e manutenção (programas de computador e outros dados electrónicos) - art. 2º, al. a) LC
      - Dados informáticos – qualquer representação de factos, informações ou conceitos suscetíveis de processamento num sistema informático (incluindo programas) – art. 2º, al. b) LC
      - Dados de tráfego – dados informáticos relacionados com uma comunicação eletrónica gerados pelo sistema (origem, destino, trajeto, data e hora, duração ou tipo de serviço) - art. 2º, al. d) LC
    - Podem ser condenadas na prática de crimes informáticos:
      - Pessoas singulares
      - Pessoas coletivas (associações, sociedades civis e comerciais, etc.) – Responsabilização criminal das pessoas coletivas pelos crimes praticados em seu nome e no interesse coletivo - mas não exclui a responsabilidade pessoal dos agentes que os praticaram (cumulativa)
    - Crimes dolosos (e não negligentes)

- Aplicação no espaço da LC: art. 27º
  - Factos praticados por portugueses (ou em benefício de pessoas colectivas sediadas em Portugal)
  - Factos praticados em território português, ainda que visem sistemas informáticos estrangeiros
  - Factos que visem sistemas informáticos situados em Portugal, independentemente do lugar da prática do facto
- Direito penal material – normas que prevêm e punem crimes informáticos:
  - Falsidade informática (art. 3º LC)
    - Espécie de falsificação de dados e documentos eletrónicos, por introdução de dados falseados ou programas de computador que visam criar dados falsos, desde que tais dados sejam suscetíveis de servir como meio de prova ou para outras finalidades juridicamente relevantes – exemplos: transações bancárias, operações de contabilidade e pagamentos, dados académicos, deferimento de prestações sociais ou concessão de benefícios
    - Bens jurídicos protegidos: segurança, fiabilidade e força probatória de dados e documentos eletrónicos
    - Pressupostos (n.º 1):
      - Introdução, modificação, apagamento ou supressão de dados informáticos ou interferência com tratamento automatizado de dados de modo a produzir dados ou documentos não genuínos
      - Com a intenção de provocar engano nas relações jurídicas, fazendo com que os dados ou documentos não genuínos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem verdadeiros
    - Agravação das penas em caso de falsificação de dados incorporados em cartão bancário ou registados em dispositivos que permitam o acesso a meios eletrónicos de pagamento, sistema de comunicações ou serviços de acesso condicionado (n.º 2)
    - Agravação da pena se o crime for praticado por funcionário no exercício das suas funções (n.º 5)
    - Punição idêntica do uso de documentos ou dispositivos produzidos com dados informáticos falsos, desde que feito com intenção de causar prejuízo a outrem ou obter um benefício ilegítimo para si ou para terceiro (n.º 3) – quando não se consegue provar quem alterou os dados
  - Dano relativo a programas ou dados informáticos (art. 4º LC)
    - Afectação do uso de dados ou programas informáticos alheios, por infeção de vírus que destroem ou alteram dados e programas ou por eliminação ou alteração de dados informáticos sem intenção de os usar para fins juridicamente relevantes
    - Bens jurídicos protegidos: integridade dos dados e programas informáticos
    - Pressupostos (n.º 1):

- o Apagamento, alteração, destruição total ou parcial, danificação, supressão, tornar não inutilizáveis ou inacessíveis, ou afectar a capacidade de uso de programas ou dados informáticos alheios
  - o Sem autorização legal ou do titular dos dados ou programas
- Agravação das penas se o dano causado for de valor elevado (5010€) ou consideravelmente elevado (2040€) (n.º 4 e 5)
- Sabotagem informática (art. 5º LC)
  - Perturbação grave do funcionamento de um sistema informático (só no software e não no equipamento ou hardware) - infestação por vírus e bombas lógicas
  - Bem jurídico protegido: bom funcionamento dos sistemas informáticos
  - Pressupostos (n.º 1):
    - o Entravamento, impedimento, interrupção, ou perturbação grave do funcionamento de sistema informático por introdução, alteração ou eliminação de programas ou dados informáticos
    - o Sem autorização legal ou do titular do sistema informático
  - Agravação em caso de danos de valor elevado ou consideravelmente elevado e perturbação de sistema informático de apoio ao fornecimento de serviços públicos essenciais (água, luz, saúde, segurança, etc.) (n.º 4 e 5)
- Acesso ilegítimo (art. 6º LC)
  - Acesso ilícito a sistemas informáticos, directo ou indirecto (por apropriação ilícita de passwords de acesso, *trojan horse*, etc.) - não releva a intenção (pode ser com objetivo de retirar algum proveito económico, ou simplesmente pelo jogo e desafio)
  - Bem jurídico protegido: segurança dos sistemas informáticos
  - Pressupostos (n.º 1):
    - o Acesso, de qualquer modo, a sistema informático
    - o Sem autorização legal ou do titular do sistema
  - Agravação da pena em função:
    - o Do meio usado - violação de regras técnicas de segurança (n.º 3)
    - o Do resultado - conhecimento de segredo comercial ou industrial ou dados confidenciais protegidos por lei (segredo de Estado, sigilo profissional, etc.); e benefício ou vantagem patrimonial de valor consideravelmente elevados (n.º 4)
- Intercepção ilegítima (art. 7º LC)
  - Captação por meios técnicos dos dados de tráfego e conteúdo de comunicações eletrónicas (espionagem informática)
  - Bem jurídico protegido: segurança das comunicações eletrónicas de dados
  - Pressupostos (n.º 1):
    - o Intercepção de transmissões de dados informáticos por meios técnicos, através de dispositivos

- eletromagnéticos, acústicos, mecânicos ou outros- art. 2º, al. e) LC
  - o Sem autorização legal ou do titular do sistema
- Reprodução ilegítima de programa protegido (art. 8º LC)
  - Bem jurídico protegido: direito de autor de programa de computador (tutela do investimento e criatividade)
    - o Reprodução (gravação e obtenção de cópias, totais ou parciais – a mera utilização de programa não é considerada reprodução), divulgação pública (colocação de exemplares à disposição do público através de venda, aluguer, empréstimo ou cedência), ou comunicação pública (realização de atividades que permitam o acesso público sem distribuição de exemplares)
    - o Programa informático protegido pelo DL 252/94 (só os programas criativos!)
    - o Sem a devida autorização
  - Proteção dos direitos de propriedade industrial sobre topografias de semicondutores (circuitos eletrónicos-hardware)- n.º 2
- Produção, distribuição, e introdução em sistemas informáticos de dispositivos, programas ou dados informáticos destinados a cometer os crimes informáticos previstos nos art. 3º a 7º LC
- o Direito processual penal – normas relativas ao processo de obtenção de prova em processo crime que complementam as do Código de Processo Penal.

A Lei do Cibercrime introduziu um conjunto de disposições processuais relativas à prova digital. Portugal passou a contar com mecanismos processuais como a preservação expedita de dados

- Meios de obtenção de dados informáticos destinados a provar a prática de crimes informáticos ou outros crimes: art. 11º e ss. LC
  - Preservação, acesso e pesquisa de dados informáticos – art. 12.º
  - Revelação de dados de tráfego pelos fornecedores de serviço – art. 13.º
  - Injunção para apresentação ou concessão do acesso a dados – art. 14.º
  - Pesquisa de dados informático – art. 15.º
  - Apreensão de dados informáticos – art. 16.º
  - Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – art. 17.º
  - Interceção de comunicações – art. 18.º
  - Ações encobertas – art. 19.º

Com exceção dos artigos 18.º e 19.º todos estes mecanismos processuais podem ser usados, não apenas na investigação da prática dos crimes previstos na LC mas também nos processos criminais em que se investiguem crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, por força do artigo 11.º n.º 1 da LC.

Ainda no domínio da produção de prova digital em processo penal, importa referir a Diretiva n.º 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, que foi transposta para a ordem jurídica portuguesa pela Lei n.º 32/2008, de 17 de julho. O objetivo destes diplomas legais foi o de estabelecer as condições nas quais poderia ocorrer a conservação e a transmissão dos dados de tráfego, de localização e dados conexos necessários para identificar o assinante ou o utilizador, para fins de investigação, deteção e repressão de crimes graves. A Lei n.º 32/2008 identifica como crimes graves os crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima [artigo 2.º, n.º 1, alínea g)].

Os fornecedores de serviços de comunicações eletrónicas estão obrigados a conservar, por um período de um ano, dados que indiquem, inter alia, a origem da comunicação, o destino, a hora, a data, a duração ou o tipo de comunicação. De fora ficam os dados de conteúdo, ou seja, os dados relativos ao conteúdo das comunicações. Esta conservação ocorre de modo automático, não carecendo de qualquer intervenção judicial e independentemente do conhecimento e consentimento do titular dos dados. Independentemente também de qualquer suspeita criminal. A transmissão dos dados conservados é requerida pelo Ministério Público ou autoridade de polícia criminal, sob autorização do juiz de instrução. Pelo facto de estarem em causa direitos fundamentais, só o juiz de instrução pode autorizar a transmissão dos dados e essa autorização só será concedida se estiver em causa a investigação, deteção e repressão de crimes graves e se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter. Para além disso, só podem ser transmitidos os dados relativos a certas pessoas:

- O suspeito ou arguido
- a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido;
- ou a vítima de crime, mediante o respetivo consentimento, efetivo ou presumido.

O incumprimento da obrigação de conservação, do prazo de conservação ou da transmissão dos dados é punido com coimas que ascendem aos cinquenta mil euros, se o agente for uma pessoa singular, ou 10 milhões de euros, perante pessoas coletivas. A aplicação destas coimas, bem como a instrução do processo contraordenacional, é da competência da Comissão Nacional de Proteção de Dados.

- Conjugação da LC com o Código Penal e a LERGPD
  - A LC é uma lei especial face ao CP, o que significa que se aplica prioritariamente face a este - art. 28º LC
    - A LERGPD é específica para as situações de tratamento de dados pessoais, aplicando-se, em detrimento da LC - art. 30º LC:
      - Se o acesso a sistema informático visar ou permitir o acesso a dados pessoais, está em causa o crime de acesso indevido do art. 47º LERGPD, e não do art. 6º LC

- A viciação ou destruição de dados pessoais está prevista no art. 49º LERGD, não se enquadrando no art. 4º LC