CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Relatório

CIBERSEGURANÇA EM PORTUGAL

Ética & Direito

DEZEMBRO DE 2020

Observatório de Cibersegurança

FICHA TÉCNICA

AUTORIA DO ESTUDO
Francisco Pacheco de Andrade, Isabel Fonseca, Joana Aguiar e Silva, Joana Covelo de Abreu, Patrícia Jerónimo, Pedro Dias Venâncio, Pedro Miguel Freitas

TÍTULO
Relatório Cibersegurança em Portugal: Ética & Direito

EDIÇÃO
JusGov (Universidade do Minho) e CNCS

DESIGN
Pedro Rito e CNCS

FOTOGRAFIAS
Pixy.org: fotografia de capa.

Unsplash.com *(por ordem de apresentação)*: LinkedIn Sales Navigator - p4 (esq.) | Blake Wisz - p4 (dir.) | Floriane Vita - p17 | Markus Spiske - p18 (ambas) | NASA - p21 | rupixen.com - p22 (esq.) Akira Hojo - p22 (dir.) | Arian Darvishi - p28 | Alex Vasey - p40 | Tomasz Frankowski - p46 | Mike Bryant - p54 | Macu ic - p90 | Gilles Rolland-Monnet - p104 | Brooke Cagle - p108 (esq.) | Blake Wisz - p108 (dir.) | Umberto - p110 (esq.) | Daniel McCullough - p110 (dir.) | Clint Patterson - p112 (esq.) | Campaign Creators - p112 (dir.).

IMPRESSÃO
Copissaurio Repro – Centro de Impressão

TIRAGEM
100 exemplares

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

ÍNDICE

Observatório
de **Cibersegurança**

SUMÁRIO EXECUTIVO

O objetivo deste Relatório é analisar os principais problemas éticos e jurídicos associados à (in)segurança no ciberespaço e as soluções que têm vindo a ser adotadas a nível internacional e nacional para resolver ou minorar estes problemas. A análise é dividida em três capítulos, incidindo sucessivamente sobre os desafios ético-morais, a genealogia legal e a aplicação prática do quadro normativo.

O primeiro capítulo faz o mapeamento das questões éticas suscitadas pela cibersegurança, a partir da observação da omnipresença da tecnologia na vida social e dos riscos daí decorrentes para os direitos fundamentais, a democracia e o Estado de Direito. É dedicada especial atenção ao papel eticamente ambíguo desempenhado pelos *hackers* e aos especiais deveres éticos que impendem sobre os profissionais de cibersegurança, ainda que não se descure que também os Estados, as empresas, as organizações e os cidadãos comuns têm o dever de atuar de forma responsável no ciberespaço.

O segundo capítulo – Genealogia Legal – analisa a evolução do Direito internacional, europeu e nacional da cibersegurança, começando por apresentar um panorama geral dos desenvolvimentos normativos ocorridos a partir da década de 1990, no plano interno e ao nível da União Europeia e demais organizações internacionais que Portugal integra. Segue-se a identificação das agências e organismos responsáveis por matérias de cibersegurança, na União Europeia e em Portugal, e um conjunto de análises setoriais sobre áreas relevantes para a discussão do Direito da cibersegurança – infraestruturas críticas e serviços essenciais, cibercrime e prova digital, proteção de dados pessoais, comunicações eletrónicas, comércio eletrónico, pagamentos eletrónicos e identificação eletrónica, propriedade intelectual e transição digital da Administração Pública.

O terceiro capítulo – Aplicação do Quadro Normativo – incide sobre o modo como os instrumentos legislativos de Direito da União Europeia e de Direito português têm vindo a ser aplicados pelos tribunais e pelas autoridades administrativas com poderes de fiscalização e sanção, centrando-se nas questões da cibercriminalidade, da prova digital e da proteção de dados. Analisa a jurisprudência relevante do Tribunal de Justiça da União Europeia e algumas pronúncias recentes de tribunais portugueses a respeito da conformidade da lei portuguesa com o Direito da União Europeia e da articulação da Lei do Cibercrime com o Código de Processo Penal. Analisa também as deliberações tomadas pela Comissão Nacional de Proteção de Dados desde 2018. Tendo como referência o ano de 2019, ainda que com pontuais comparações com anos anteriores, faz-se a apresentação de dados relativos ao número e tipo de cibercrimes registados pelas autoridades, ao número e tipo de incidentes de segurança registados pela Equipa de Resposta a Incidentes de Segurança Informática Nacional e pela Autoridade Nacional de Comunicações, e ao número de operadores de serviços essenciais identificados pelo Centro Nacional de Cibersegurança.

Este Relatório utiliza predominantemente fontes abertas, como bases de legislação e de jurisprudência, ainda que a sua preparação tenha envolvido a consulta de elementos facultados pelo Centro Nacional de Cibersegurança e beneficiado dos contributos dos vários parceiros ligados à Justiça e à Segurança que se prestaram a colaborar neste trabalho.

DESTAQUES ÉTICA

A insegurança no ciberespaço e os mecanismos de controlo e proteção cibernéticos podem ter efeitos devastadores para a dignidade da pessoa humana, com o potencial de afetar valores como a privacidade, a propriedade, a liberdade, a saúde ou mesmo a vida.

Os fundamentais desafios éticos com que se defronta a cibersegurança prendem-se com a necessidade de a mesma cumprir os seus propósitos no respeito pelos limites que constituem os valores subjacentes à proteção da dignidade da pessoa humana.

Os fornecedores de cibersegurança têm de lidar com os desafios éticos associados ao conhecimento dos limites da sua própria atuação: saber até onde devem ir para garantir os propósitos de segurança e integridade das redes, sem contender com os interesses e direitos fundamentais dos vários agentes envolvidos.

A heterogeneidade dos contextos em que atua a cibersegurança e a celeridade a que se verificam as transformações tecnológicas inviabilizam a implementação de diretrizes éticas estáveis e uniformes.

O legislador tem dificuldade em acompanhar, em tempo útil, as transformações tecnológicas. Em todo o caso, a ética não se esgota nas leis, nem se confunde com elas. Um comportamento lícito não é necessariamente um comportamento ético.

A definição de estratégias de cibersegurança deve atender à proteção de valores passíveis de congregação em torno dos eixos da confiabilidade, da transparência, da responsabilidade e dos direitos fundamentais.

A promoção da cultura de transparência e da ética de responsabilidade impende sobre as entidades prestadoras de serviços, públicas ou privadas, sobre os profissionais de cibersegurança e sobre os próprios cidadãos, enquanto utilizadores das plataformas e sistemas digitais.

É fundamental o papel desempenhado pelos cidadãos, informados e educados numa ética de responsabilidade, para o adequado funcionamento das estruturas e redes digitais.

DESTAQUES

GENEALOGIA LEGAL

Panorama geral

Desde a década de 1990, as iniciativas dirigidas ao reforço da cooperação entre os Estados e à definição de princípios e regras comuns em matéria de cibersegurança multiplicaram-se em vários *fora* (Organização para a Cooperação e Desenvolvimento Económico, Organização das Nações Unidas, Conselho da Europa, União Europeia, meios académicos, etc.).

Em 2013, um Grupo de Peritos da Organização das Nações Unidas concluiu que as normas de Direito Internacional já existentes – desde logo, a Carta das Nações Unidas – se aplicam ao ciberespaço, o que contribuiu para adiar *sine die* quaisquer planos de adoção de um tratado internacional de âmbito mundial sobre cibersegurança.

A opinião dominante entre os Estados ocidentais e as principais empresas de tecnologia tem sido a de que, atenta a velocidade dos avanços tecnológicos e a tendencial rigidez das soluções jurídicas, a regulação do ciberespaço não deve ser feita por meio de regras jurídicas vinculativas, mas sim por meio de recomendações e compromissos políticos a que as partes interessadas (Estados, empresas, organizações) adiram voluntariamente.

A popularidade dos Códigos de Conduta e demais instrumentos de *soft law não obsta a que tenham ocorrido alguns desenvolvimentos significativos no plano da adoção de instrumentos jurídicos vinculativos, sobretudo de âmbito regional, destacando-se a Convenção* de Budapeste sobre o Cibercrime, adotada em 2001, no quadro do Conselho da Europa, e os numerosos Regulamentos e Diretivas da União Europeia.

O primeiro ato legislativo da União Europeia no domínio da cibersegurança foi a Diretiva 2016/1148, relativa à segurança das redes e da informação, mas as preocupações com a cibersegurança estiveram presentes desde o início e são visíveis nos instrumentos legislativos adotados ao longo dos anos, em matérias como o tratamento de dados pessoais, a assinatura eletrónica, o comércio eletrónico, as comunicações eletrónicas e o cibercrime.

Em Portugal, as políticas públicas e os desenvolvimentos legislativos em matéria de cibersegurança têm vindo a acompanhar as diretrizes definidas pela União Europeia e os compromissos assumidos no quadro do Conselho da Europa.

Quadro institucional de referência

Na União Europeia, os atores mais relevantes no tratamento das matérias de cibersegurança são a Agência da União Europeia para a Cibersegurança (ENISA), a equipa de resposta a emergências informáticas (CERT.EU) e o Centro Europeu da Cibercriminalidade (EC3).

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

Infraestruturas críticas e serviços essenciais

O aumento das ligações (e da dependência) entre as infraestruturas críticas dos Estados e as redes e os sistemas e serviços de informação trouxe novos riscos e vulnerabilidades para a segurança dos Estados, motivando a adoção de medidas destinadas a assegurar a proteção das redes e infraestruturas.

A Diretiva 2008/114/CE, de 18 de dezembro, estabeleceu um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção.

O Decreto-Lei n.º 62/2011, de 9 de maio, que transpôs a Diretiva 2008/114/CE, estabeleceu os procedimentos de identificação e de proteção das infraestruturas essenciais nos sectores da energia e transportes.

A Diretiva 2016/1148, de 6 de julho (Diretiva SRI), veio promover uma cultura de gestão dos riscos, com partilha de responsabilidades entre entidades públicas e privadas, e consagrar um padrão mínimo comum de segurança para operadores de serviços essenciais e prestadores de serviços digitais.

Para além dos setores da energia e dos transportes, a Diretiva SRI identifica como operadores de serviços essenciais as entidades públicas ou privadas do setor bancário e infraestruturas do mercado financeiro, do setor da saúde, do setor do fornecimento e distribuição de água potável e as infraestruturas digitais.

Para a concreta identificação dos operadores de serviços essenciais, a Diretiva SRI elenca um conjunto de critérios que se prendem com a atividade social e/ou económica crucial desenvolvida, com a dependência das redes e sistemas de informação para a prestação desse serviço, e com os efeitos perturbadores na prestação desse serviço que um incidente possa causar.

Para alcançar um elevado nível comum de segurança das SRI em todo o território da União, a Diretiva cria um grupo de cooperação e uma rede de equipas de resposta a incidentes de segurança informática (Rede Europeia de CSIRT).

A Diretiva SRI foi transposta para a ordem jurídica portuguesa pela Lei n.º 46/2018, de 13 de agosto, que estabeleceu o regime jurídico da segurança do ciberespaço, fixou deveres de notificação de incidentes e estabeleceu um regime sancionatório para o incumprimento, nomeadamente, dos deveres de notificação.

A Lei n.º 46/2018, de 13 de agosto, remeteu para legislação complementar a definição dos requisitos de segurança das redes e dos sistemas de informação e a definição dos requisitos de notificação de incidentes. Esta legislação ainda não foi adotada, pelo que o regime instituído pela Lei n.º 46/2018 irá evoluir significativamente num futuro próximo.

Cibercrime e prova digital

A lei de referência em Portugal sobre o cibercrime é a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), que resulta da transposição para a ordem jurídica interna da Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e da adaptação da ordem jurídica portuguesa à Convenção do Conselho da Europa sobre o Cibercrime, de 2001, que Portugal assinou em 2001 e ratificou em 2009.

Para além de tipos legais de crime atualizados face Lei da Criminalidade Informática, de 1991, a Lei do Cibercrime introduziu, no ordenamento jurídico português, um conjunto de disposições processuais relativas à prova digital.

A interpretação e a aplicação da Lei do Cibercrime e demais normas aplicáveis em matéria de cibercrime e prova digital têm suscitado dúvidas na jurisprudência e na doutrina portuguesas, sobretudo no que respeita à articulação entre a Lei do Cibercrime e o Código de Processo Penal, mas também quanto à compatibilidade do regime jurídico relativo à conservação de dados gerados ou tratados no contexto de comunicações eletrónicas (Lei n.º 32/2008, de 17 de julho) com o Direito da União Europeia.

Aguarda-se a conclusão do procedimento formal de infração movido pela Comissão Europeia contra Portugal relativo à transposição da Diretiva 2013/40/UE, de 12 de agosto, relativa a ataques contra os sistemas de informação, que substituiu a Decisão-Quadro 2005/222/JAI.

Proteção de dados pessoais

A proteção de dados pessoais tem uma longa tradição no Direito internacional dos direitos humanos, enquanto dimensão da proteção da intimidade da vida privada e familiar. No Direito da União Europeia, a proteção de dados pessoais constitui um direito fundamental autónomo, consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.

O Regulamento Geral de Proteção de Dados, adotado em 2016, veio assegurar às pessoas singulares de todos os Estados Membros o mesmo nível de direitos suscetíveis de proteção judicial, impondo obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes e um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados Membros.

No Regulamento Geral de Proteção de Dados, a preocupação com a cibersegurança está patente na exigência de que os dados pessoais sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

A Lei n.º 58/2019, de 8 de agosto (Lei da Proteção de Dados Pessoais), que assegura a execução do Regulamento Geral de Proteção de Dados em Portugal, prevê o regime aplicável ao responsável pelo tratamento dos dados e especifica as funções do encarregado de proteção de dados. Também estabelece os regimes de proteção administrativa e judicial do titular de dados pessoais e os regimes de responsabilidade civil e sancionatória, contraordenacional e penal, para a violação das disposições do Regulamento.

Comunicações eletrónicas

Na União Europeia, tem havido a preocupação em assegurar que todos os Estados Membros se dotem de redes e serviços de comunicações eletrónicas de boa qualidade, sendo as operações daí decorrentes sujeitas a competente regulação pelas autoridades reguladoras nacionais (no caso português, a Autoridade Nacional de Comunicações).

A regulação das comunicações eletrónicas é pautada por preocupações de regulação social, com vista a mitigar as assimetrias entre as populações, atendendo a um conceito de "serviço universal" suficientemente dinâmico para se adequar aos desenvolvimentos no âmbito tecnológico e digital.

A transformação digital determinou a transição da telefonia vocal para o acesso à Internet, o que motivou a adoção da Diretiva (UE) 2018/1972 que estabelece o Código Europeu das Comunicações Eletrónicas.

O Código Europeu das Comunicações Eletrónicas visa assegurar a liberdade de oferta de serviços e redes de comunicações eletrónicas que observem um nível particularmente elevado de segurança.

Os padrões de segurança a assegurar exigem segurança física e ambiental, de fornecimento, de controlo de acesso às redes e de integridade dessas redes; a adoção de procedimentos de gestão que permitam detetar e minimizar incidentes de segurança; uma capacidade de continuidade operacional e a implementação de políticas de monitorização, de auditoria e de condução de testes.

A Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas tem como prazo de transpoição pelo Estado português o dia 21 de dezembro de 2020.

Comércio eletrónico, pagamentos eletrónicos e identificação eletrónica

Em matéria de identificação eletrónica, assinaturas eletrónicas e certificação eletrónica, os momentos decisivos na evolução do regime jurídico foram a adoção da Diretiva 1999/93/CE, que estabeleceu o princípio da neutralidade tecnológica e definiu as regras essenciais do sistema de certificação eletrónica nos Estados Membros, e a adoção do Regulamento (UE) 910/2014 (eIDAS), que colocou a tónica na questão da identificação eletrónica (autenticação e assinatura) e introduziu um conjunto de novos serviços da sociedade da informação tendentes a garantir um nível mais elevado de segurança na prestação de serviços e nas transações eletrónicas e a interoperabilidade na prestação de serviços.

Em matéria de comércio eletrónico, o diploma de referência continua a ser a Diretiva 2000/31/CE, que estabelece regras de transparência e deveres de informação a cargo dos prestadores de serviços da sociedade da informação. O desenvolvimento tecnológico dos últimos anos virá certamente impor uma nova abordagem e uma profunda revisão do quadro atual. A regulação e funcionamento das plataformas e mercados *online* já foram anunciados como temas sobre os quais versarão, em breve, novas iniciativas legislativas.

Em matéria de pagamentos eletrónicos, os marcos na evolução do regime jurídico são a Diretiva 2007/64/CE, que estabeleceu regras em matéria de transparência das condições e requisitos de informação aplicáveis aos serviços de pagamento, e a Diretiva 2015/2366/EU, que reforçou a segurança dos pagamentos eletrónicos, com a introdução de conceitos novos como as credenciais de segurança personalizada e de autenticação forte e com a

responsabilização dos prestadores de serviços de pagamento pelo estabelecimento de medidas para mitigar os riscos e manutenção de procedimentos eficazes de gestão de incidentes.

Propriedade intelectual

A matéria da propriedade intelectual encontra-se harmonizada internacionalmente através de um conjunto nuclear de tratados cuja preocupação central, a par da harmonização internacional da propriedade intelectual, tem sido a promoção da sua efetividade, essencialmente, pela criação de medidas cautelares, de investigação e de prova contra potenciais violações, associados a mecanismos de cooperação internacional.

A ubiquidade inerente à qualidade "imaterial" da criação tutelada pela propriedade intelectual torna o seu objeto particularmente vulnerável à violação do respetivo exclusivo patrimonial em ambientes digitais transnacionais.

Na área do Direito de Autor, tem sido aprovada legislação sobre medidas tecnológicas de proteção e gestão, com o fim de assegurar a cibersegurança do exclusivo de exploração digital das obras, prestações e produções protegidas por direito de autor e direitos conexos.

Na área da propriedade industrial e concorrência desleal, é na tutela da confidencialidade de informações comerciais e industriais (*know-how*), enquanto elemento essencial da competitividade das empresas e da lealdade da concorrência, que a preocupação com a cibersegurança dos sistemas informáticos empresariais se torna mais relevante.

Há ainda um caminho a fazer na tutela da propriedade intelectual no âmbito da cibercriminalidade, já que estes bens jurídicos ainda não se encontram devidamente valorizados como elementos agravantes dos crimes informáticos.

Transição digital da Administração Pública

A necessidade de criar uma Administração Pública em linha, assente no princípio da interoperabilidade, foi assumida pela Comissão Europeia, em 2015, como um vetor essencial ao estabelecimento do Mercado Único Digital.

O *Princípio da credibilidade e da segurança* é um dos princípios estruturantes do Plano de Ação para a Administração Pública em linha 2016-2020, exigindo que os esforços de modernização digital da Administração Pública se norteiem pela observância do quadro jurídico em sede de proteção de dados e de privacidade, assegurando a segurança informática desde a fase de conceção dos serviços.

O objetivo da Comissão Europeia de dotar a União Europeia de uma Plataforma Digital Única foi prosseguido com o Regulamento (UE) 2018/1724, de 2 de outubro, relativo à criação de uma plataforma digital única para a prestação de acesso a informações, a procedimentos e a serviços de assistência e de resolução de problemas.

Em 2020, foram aprovados o Plano de Ação para a Transição Digital e a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, ambos com objetivos e medidas em matéria de cibersegurança. Está ainda em curso o desenvolvimento da Estratégia para a Transformação Digital da Administração Pública 2021-2023, que, com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, completará este conjunto de políticas públicas na área do digital para o Estado.

DESTAQUES

APLICAÇÃO DO QUADRO LEGAL

A aplicação do quadro legal de Direito da União Europeia e de Direito português tem suscitado dúvidas por parte dos tribunais e das entidades administrativas com poderes de fiscalização e sanção.

A declaração de invalidade da Diretiva 2006/24/CE, pelo Tribunal de Justiça da União Europeia, no acórdão *Digital Rights Ireland*, de 2014, suscitou, em Portugal, a questão de saber qual a validade jurídica da Lei n.º 32/2008, sobre conservação de dados, que transpôs a Diretiva para a ordem jurídica portuguesa. A Comissão Nacional de Proteção de Dados considera-a inválida e, em deliberação de 2017, decidiu deixar de a aplicar, ao passo que o Ministério da Justiça e o Gabinete Cibercrime da Procuradoria-Geral da República entendem que a Lei permanece válida.

Num acórdão de 2019, o Tribunal reconheceu que, apesar de a declaração da invalidade da Diretiva 2006/24/CE não pôr imediatamente em causa a Lei n.º 32/2008, isso não obsta a que se considere imperativo avaliar a conformidade desta com o Direito da União Europeia, em especial com a Carta dos Direitos Fundamentais da União Europeia. Encontra-se pendente no Tribunal Constitucional um processo de fiscalização abstrata da constitucionalidade da Lei n.º 32/2008, requerido pela Provedora de Justiça, em 2019.

Os tribunais portugueses também se têm debatido com dúvidas quanto à articulação entre a Lei do Cibercrime e o Código de Processo Penal, em virtude da área de sobreposição existente entre o artigo 189.º do Código e os artigos 17.º (apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 19.º (interceção de comunicações) da Lei do Cibercrime. A orientação dos tribunais tem sido no sentido de sustentar uma revogação implícita ou tácita, pelo menos parcial, do artigo 189.º do Código de Processo Penal.

Dados da Direção-Geral de Política da Justiça indicam que os cibercrimes registados sofreram um crescimento acentuado desde a entrada em vigor da Lei do Cibercrime, na ordem dos 600%, sendo que o número total de cibercrimes registados pelas autoridades policiais em 2019 (18.158) corresponde a 5.41% do total de crimes registados no território nacional nesse ano.

Ainda não existem registos de processos contraordenacionais instruídos ao abrigo da Lei n.º 46/2018, por não ter sido adotada a legislação que irá definir os requisitos de segurança e os requisitos de notificação de incidentes cujo incumprimento importará responsabilidade contraordenacional.

A Comissão Nacional de Proteção de Dados já exerce as suas competências de fiscalização e sanção ao abrigo do Regulamento Geral de Proteção de Dados desde 2018, tendo produzido, até ao momento, cinco deliberações condenatórias (uma em 2018 e quatro em 2019). Os valores globais das coimas aplicadas oscilam entre dois mil euros e quatrocentos mil euros.

Em cumprimento do disposto no artigo 29.º, n.º 1, da Lei n.º 46/2018, o Centro Nacional de Cibersegurança procedeu à identificação dos operadores de serviços essenciais. Os dados disponíveis indicam que foram

identificados 26 serviços essenciais e 1250 operadores de serviços essenciais. Segundo relatório da Comissão Europeia, Portugal está abaixo da média da União no que respeita à identificação de serviços essenciais (35 serviços) e acima da média da União no que respeita à identificação de operadores de serviços essenciais (633 operadores).

INTRODUÇÃO

O *Relatório Cibersegurança em Portugal – Linha de Observação Ética & Direito* é o quarto Relatório lançado pelo Observatório de Cibersegurança do Centro Nacional de Cibersegurança, depois de publicados os Relatórios da Linha de Observação Sociedade (2019 e 2020) e da Linha de Observação Riscos & Conflitos (2020). De acordo com a missão e os objetivos do Observatório, este relatório sistematiza informação sobre os problemas éticos e jurídicos associados à cibersegurança e as soluções adotadas a nível internacional e nacional para os debelar, com o propósito de contribuir para o desenvolvimento e a difusão de conhecimento multidisciplinar sobre cibersegurança em Portugal e para a criação de uma sociedade mais segura e consciente dos riscos e das responsabilidades inerentes ao ciberespaço.

Na ausência de uma definição universalmente aceite do que seja cibersegurança (ENISA, 2016: 10-11), este relatório usa como conceito operativo a definição que é dada, em Portugal, pela Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (aprovada pela Resolução do Conselho de Ministros n.º 92/2019), nos termos da qual cibersegurança consiste no "conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço e das pessoas que nele interagem".

A análise dos problemas éticos e jurídicos associados à cibersegurança é organizada em três capítulos nucleares:

Problemas Ético-Morais, referente às dimensões éticas da cibersegurança, aos desafios éticos enfrentados por governos, empresas e profissionais de cibersegurança e aos esforços no sentido de definir códigos de conduta para todos os participantes no ciberespaço, assentes em valores como a confiabilidade, a transparência, a responsabilidade e o respeito pelos direitos fundamentais.

Genealogia Legal, referente à evolução do quadro normativo de Direito internacional, da União Europeia e português, combinando uma visão global dos principais marcos legislativos ao longo das últimas três décadas com análises setoriais de medidas legislativas relativas a infraestruturas críticas e serviços essenciais, cibercrime e prova digital, proteção de dados pessoais, comunicações eletrónicas, comércio eletrónico, pagamentos eletrónicos e identificação eletrónica, propriedade intelectual e transição digital da Administração Pública.

Aplicação Prática do Quadro Normativo, referente aos processos judiciais e contraordenacionais decididos pelas autoridades portuguesas nos últimos dois anos, bem como ao processo de caracterização dos operadores de serviços essenciais por parte do Centro Nacional de Cibersegurança, e ainda à jurisprudência relevante do Tribunal de Justiça da União Europeia.

O presente relatório foi elaborado por uma equipa de investigadores do Centro de Investigação em Justiça e Governação (JusGov) da Universidade do Minho. Tal como os relatórios do Observatório de Cibersegurança que o antecederam, este trabalha com indicadores propostos pelo Centro Nacional de Cibersegurança e acordados com a equipa do JusGov. A exposição é, no entanto, substancialmente mais narrativa do que a dos relatórios anteriores, o que se deve às características de alguns dos indicadores utilizados (genealogia do processo legislativo da União Europeia, desafios éticos) e ao tipo de fontes consultadas (documentos de política, legislação e jurisprudência).

O relatório foi realizado com base em informações colhidas em diversas fontes públicas, como as Bases Jurídico-Documentais do Instituto de Gestão Financeira e Equipamentos da Justiça, a Procuradoria-Geral da República de Lisboa, a Direção-Geral de Políticas de Justiça e o portal EUR-Lex. O Relatório privilegiou os dados mais recentes, relativos a 2018 e a 2019, comparáveis internacionalmente e observáveis ao longo do tempo, ainda que tenha, pontualmente, feito uso de dados respeitantes a anos anteriores, quando considerados pertinentes. Procurou-se, sempre que possível, estabelecer a linha temporal e a respetiva tendência.

O relatório foi desenvolvido em estreita colaboração com a equipa do Centro Nacional de Cibersegurança e beneficiou da orientação e dos contributos prestados pelo Conselho Consultivo do Observatório de Cibersegurança. Foram também consultadas várias instituições nacionais e internacionais a operar na área da cibersegurança, como o Gabinete Cibercrime da Procuradoria-Geral da República, a Polícia Judiciária, o Gabinete Português de Acreditação (IPAC), a Autoridade Nacional de Comunicações (ANACOM) e a Agência da União Europeia para a Cibersegurança (ENISA), que disponibilizaram informações e prestaram esclarecimentos da maior importância para a concretização do projeto.


Canada

TERMOS E ABREVIATURAS

Assinatura digital: a modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.

(Decreto-Lei n.º 290-D/99, de 2 de agosto, na versão dada pelo Decreto-Lei n.º 88/2009, de 9 de abril)

Assinatura eletrónica: "os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar".

[Regulamento (UE) 910/2014, de 23 de julho]

Autenticação eletrónica: "processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar".

[Regulamento (UE) 910/2014, de 23 de julho]

Cibercrimes: "factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa".

(Estratégia Nacional de Segurança do Ciberespaço 2019-2023)

Ciberespaço: "consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

(Estratégia Nacional de Segurança do Ciberespaço 2019-2023)

Cibersegurança: "consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem".

(Estratégia Nacional de Segurança do Ciberespaço 2019-2023)

Confidencialidade dos dados: "a proteção das comunicações ou dos dados armazenados contra a interceção e a leitura por pessoas não autorizadas".

[Regulamento (CE) 460/2004, de 10 de março]

Desinformação: "informação comprovadamente falsa ou enganadora que, cumulativamente, (a) é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e (b) é suscetível de causar um prejuízo público, entendido como ameaças aos processos políticos democráticos e aos processos de elaboração de políticas, bem como a bens públicos, tais como a proteção da saúde dos cidadãos da UE, o ambiente ou a segurança".

(Código de Conduta da UE sobre Desinformação)

Equipa de resposta a incidentes de segurança informática: "a equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação".

(Lei n.º 46/2018, de 13 de agosto)

Hacktivistas: agentes "orientados a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais".

(ENISA, Threat Landscape Report 2018)

Identificação eletrónica: "o processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa coletiva".

[Regulamento (UE) 910/2014, de 23 de julho]

Incidentes: "eventos com um efeito adverso real na segurança das redes e dos sistemas de informação".

(Lei n.º 46/2018, de 13 de agosto)

Infraestrutura crítica: "componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções".

(Lei n.º 46/2018, de 13 de agosto)

Infraestrutura crítica europeia: infraestrutura crítica situada nos Estados Membros cuja perturbação ou destruição teria um impacto significativo em pelo menos dois Estados Membros.

(Diretiva 2008/114/CE, de 8 de dezembro)

Interoperabilidade: "capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo, implicando a partilha de informações e conhecimentos entre si, no âmbito dos processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC".

[Decisão (UE) 2015/2240, de 25 de novembro]

Malware [*Software* Malicioso]: "programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima".

(NIST, IR 7298 Revision 2, Glossary of Key Information Security Terms)

***Opt-in*:** "regime de consentimento prévio pelo qual alguém consente em receber determinado tipo de mensagens".

[Comunicação da Comissão Europeia COM (2004) 28]

Opt-out: "ação pela qual alguém manifesta a vontade de não receber determinado tipo de mensagens".

[Comunicação da Comissão Europeia COM (2004) 28]

Phishing: "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de *emails* ou mensagens para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas, façam transferências de dinheiro, etc.".

(ENISA, *Threat Landscape Report* 2018)

Plataforma eletrónica: "a infraestrutura tecnológica constituída por um conjunto de aplicações, meios e serviços informáticos necessários ao funcionamento dos procedimentos eletrónicos de contratação".

(Lei n.º 96/2015, de 17 de agosto)

Rede e sistema de informação: "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção".

(Lei n.º 46/2018, de 13 de agosto)

Segurança das redes e da informação: "a capacidade de uma rede ou sistema informático para resistir, com um dado nível de confiança, a eventos acidentais ou a ações dolosas ou ilícitas que comprometem a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema".

[Regulamento (CE) 460/2004, de 10 de março]

Serviço da sociedade da informação: "qualquer serviço prestado a distância por via eletrónica, mediante remuneração ou, pelo menos, no âmbito de uma atividade económica, na sequência de pedido individual do destinatário".

(Lei n.º 7/2004, de 7 de janeiro)

Serviço essencial: "um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço".

(Lei n.º 46/2018, de 13 de agosto)

Sistema de informação: "um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção".

(Diretiva 2013/40/UE, de 12 de agosto)

Sistema informático: "os computadores e as redes de comunicações eletrónicas, bem como os dados por eles armazenados, processados, extraídos ou transmitidos para efeitos de exploração, utilização, proteção e manutenção".

[Regulamento (CE) 460/2004, de 10 de março]

Violação de dados pessoais: "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

(Regulamento Geral de Proteção de Dados)

ANACOM: Autoridade Nacional de Comunicações

CDADC: Código de Direito de Autor e Direitos Conexos

CDFUE: Carta dos Direitos Fundamentais da União Europeia

CEDH: Convenção Europeia dos Direitos Humanos

CERT.EU: Computer Emergency Response Team for the EU Institutions

CERT.PT: Equipa de Resposta a Incidentes de Segurança Informática Nacional

CNCS: Centro Nacional de Cibersegurança

CNPD: Comissão Nacional de Proteção de Dados

COTEC: Associação Empresarial para a Inovação

CPA: Código do Procedimento Administrativo

CPI: Código da Propriedade Industrial

CRP: Constituição da República Portuguesa

DGPJ: Direção-Geral de Políticas de Justiça

DPO: Data Protection Officer

EBA: Autoridade Bancária Europeia [European Bank Authority]

EDI: Transferência/Intercâmbio Eletrónica(o) de Dados [Electronic Data Interchange]

ENISA: Agência da União Europeia para a Cibersegurança

GNS: Gabinete Nacional de Segurança

IA: Inteligência Artificial

ICE: Infraestruturas Críticas Europeias

INE: Instituto Nacional de Estatística

MP: Ministério Público

OCDE: Organização para a Cooperação e Desenvolvimento Económico

ONU: Organização das Nações Unidas

PATD: Plano de Ação para a Transição Digital para Portugal

RGPD: Regulamento Geral sobre a Proteção de Dados

RNCSIRT: Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática

SRI: Segurança das Redes e da Informação

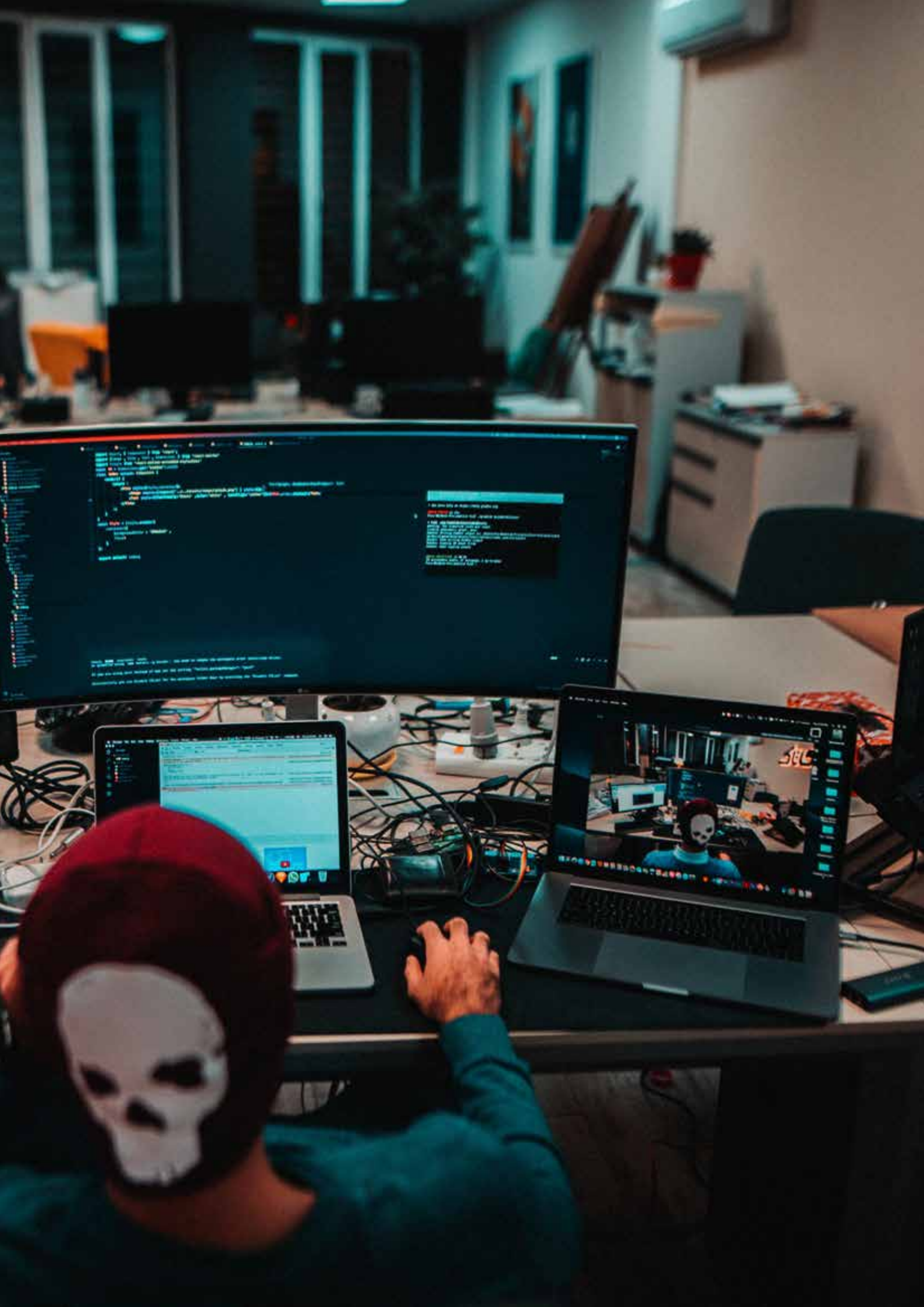
TEDH: Tribunal Europeu dos Direitos Humanos

TEDIS: Trade Electronic Data Interchange Systems

TIC: Tecnologias de Informação e Comunicação

TJUE: Tribunal de Justiça da União Europeia

UE: União Europeia



1. PROBLEMAS ÉTICO-MORAIS

1.1. Sociedade, tecnologia e dimensões éticas da cibersegurança

Vivemos numa sociedade cada vez mais dependente das tecnologias digitais. O uso crescente de tecnologias de informação e comunicação (TIC) em praticamente todas as esferas da vida contemporânea, se traz inequívocos benefícios à generalidade da população, comporta igualmente inúmeros riscos e vulnerabilidades de que muitos indivíduos não têm consciência. Outros, tendo consciência desses riscos, desvalorizam-nos face ao grau de sedução exercido pelo *marketing* associado a determinados produtos e serviços. Não é possível garantir a absoluta segurança das redes e sistemas digitais, pelo que estes podem converter-se num espaço propício a ameaças e violações de valores e interesses fundamentais para a vida em democracia, como a privacidade, a propriedade, a liberdade e a própria vida. Aquela dependência, aliada a este potencial de insegurança, determina a atual expansão de estratégias e mecanismos de cibersegurança, com os quais se visa "aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas" (Estratégia Nacional de Segurança do Ciberespaço).

O domínio da cibersegurança mostra-se, atualmente, um espaço fundamental para preservar a confiança dos cidadãos nas infraestruturas digitais, nas instituições e na própria autoridade estatal. Um espaço que é essencial para garantir valores fundamentais, como os da segurança e integridade das redes digitais, protegendo a sua utilização por parte de entidades públicas e privadas, e assim protegendo essas mesmas entidades nos seus direitos e interesses fundamentais. Ainda assim, os mecanismos e práticas que mobiliza podem igualmente mostrar-se perigosamente intrusivos, coartando os mesmos direitos e liberdades que visa proteger. Nessa medida, **os últimos anos têm vindo a acentuar a natureza intrinsecamente ética da própria cibersegurança, reconhecendo a necessidade de a mesma, e daqueles que a providenciam, atentarem nas implicações não apenas técnicas, mas, sobretudo, éticas e sociais da sua atuação.** Pronunciando-se em 2003 sobre a criação de uma cultura global de cibersegurança (Resolução 57/239), a Assembleia Geral das Nações Unidas incluiu a ética entre os elementos estruturantes dessa cultura global, explicando que, dada a omnipresença de sistemas e redes de informação nas sociedades modernas, todos os participantes (Governos, empresas, organizações e utilizadores individuais) devem respeitar os interesses legítimos dos outros e ter consciência de que os seus atos e omissões podem prejudicar esses outros.

As realizações práticas resultantes da implementação da tecnologia nem sempre serão eticamente neutras. A partir do momento em que reconhecemos o seu potencial de transformação social, económica e cultural, apreendemos também o seu papel enquanto promotoras da qualidade de vida. A ideia segundo a qual a tecnologia permite uma generalizada melhoria das condições de vida não é consensual, havendo quem a responsabilize por muitos dos problemas que afligem o cidadão moderno. A tecnologia será potencialmente

responsável pela aceleração dos ritmos da vida contemporânea, pelo consumismo desenfreado, pela delapidação dos recursos e ecossistemas naturais, ou pela degradação das próprias relações humanas. Ainda assim, pode afirmar-se que **o desenvolvimento da tecnologia tanto revela como molda aquilo que os seres humanos valorizam, indo ao encontro daquilo que lhes permite alcançar determinados níveis de bem-estar**.

Ao mesmo tempo, os extraordinários desenvolvimentos tecnológicos a que assiste o século XXI vêm a constituir uma reconfiguração da global distribuição de poder, de justiça e de responsabilidade, pelo que se assumem, cada vez mais, como um instrumento eminentemente político (Vallor, 2018: 3). **Na atual sociedade em rede, de sistemas de informação e comunicação digital, a posse de dados sensíveis sobre qualquer cidadão é cada vez mais uma fonte de poder.** O armazenamento em larga escala de informação pessoal, de dados sensíveis sobre a vida particular de cada um, sobre os seus hábitos e comportamentos, nas mãos de um número restrito de entidades, pode ser problemático, como problemática pode ser a implícita capacidade, sem precedentes, de autoridades estatais e de entidades várias, públicas e privadas, para controlar e monitorizar dados, comunicações e movimentos de qualquer pessoa ou organização. O receio aumenta quando o cidadão recorre à assinatura eletrónica para certificar os seus documentos, ou quando leva a cabo transações financeiras com recurso ao *e-banking*, ou quando troca informações confidenciais através de meios eletrónicos. Numa outra perspetiva, também ela eticamente relevante, levanta-se a questão de saber até que ponto o acesso aos benefícios potenciados pela tecnologia, bem como a exposição aos seus riscos, se encontram devidamente distribuídos.

Transversal a toda esta realidade é o **esforço de sensibilização da sociedade, não apenas para as ameaças a que está sujeita, como para a responsabilidade que tem ao nível de um funcionamento adequado das estruturas digitais**. O cidadão não tem, muito frequentemente, consciência do quão vulnerável é a sua situação face à dependência de toda a tecnologia que o rodeia, e não tem consciência dos potenciais riscos que esse ambiente comporta para a sua privacidade, a sua propriedade ou a sua liberdade, face a estratégias inadequadas de cibersegurança. Trata-se, por um lado, de fomentar a chamada literacia digital da população[1], para que a mesma possa adotar comportamentos eticamente responsáveis face aos constantes desafios impostos pelo espaço digital envolvente. Comportamentos que dizem respeito às práticas que adota ao nível das redes sociais, aos cuidados que tem no âmbito das comunicações e transações financeiras que leva a cabo no mundo digital, aos sistemas de proteção que adquire para os seus próprios suportes informáticos, ou às cautelas de que se rodeia aquando do fornecimento dos seus dados pessoais.

Trata-se, por outro lado, de perceber que essa mesma literacia digital não substitui, antes complementa, a educação para a cidadania que às sociedades democráticas compete desenvolver. Se é certo que vivemos na era da informação, não o é menos que a informação de pouco vale se não houver educação. Nessa medida, uma competência que hoje se revela essencial é a da capacidade para devidamente filtrar, de entre a avassaladora quantidade de informação disponível, aquela que se mostra relevante, pertinente e fidedigna. Se não houver um pano de fundo cultural que permita processar, selecionar e organizar essa mesma informação, dificilmente se conseguirá lidar com aqueles desafios. Haverá sociedades que privilegiam valores como os da privacidade ou da liberdade, subalternizando outros como os da segurança e da estabilidade. De qualquer forma, e ainda

1 De acordo com o Relatório da Comissão Europeia sobre o Índice de Digitalidade da Economia e da Sociedade (IDES) de 2020, o nível de literacia digital da população portuguesa é reduzido por comparação à média da UE, ainda que Portugal tenha registado progressos na dimensão do capital humano, graças a uma melhoria no nível básico de competência digitais e uma maior percentagem de licenciados em TIC. Informação disponível em https://ec.europa.eu/digital-single-market/en/scoreboard/portugal [21.12.2020].

que dependendo dessas perspetivas socioculturais, **a imputação ao cidadão desta ética de responsabilidade mostra-se uma plataforma fundamental ao equilíbrio das relações que o mesmo estabelece com a realidade tecnológica e digital em que se encontra inserido**.

Todo este quadro permite realçar não só o **carácter essencial da cibersegurança, enquanto linha crítica de proteção do cidadão face a ameaças a direitos e valores fundamentais à vida em democracia, como a sua natureza intrinsecamente ética, na medida em que pode a mesma, se mal pensada ou aplicada, contender com esses mesmos direitos e valores.** Uma maior proteção traduz-se frequentemente num maior controlo sobre as redes e sistemas monitorizados, bem como numa mais intensiva recolha e armazenamento de dados. Constatando-se o potencial da cibersegurança enquanto eventual meio, mais ou menos sub-reptício, para monitorizar ou controlar os comportamentos dos seus beneficiários, sejam eles particulares, organizações ou o próprio Estado, a solução não passa por simplesmente prescindir dela. Pior do que ter estratégias pobres (ou abusivas) de cibersegurança – que podem configurar práticas antiéticas, ou práticas moralmente ambíguas – é não as ter de todo, uma vez que os riscos, como as vulnerabilidades, são potencialmente muito mais graves. Igualmente perigosa se mostrará uma cibersegurança excessivamente agressiva, que, procurando extremar os seus objetivos de garantir a integridade e a segurança, não apenas se mostre invasiva de espaços eminentemente privados, como torne inutilizáveis/inacessíveis as redes e sistemas que visa proteger.

O desafio ético fundamental que assim se coloca aos profissionais de cibersegurança é o de saber quão intrusivos devem ser os instrumentos aplicados e os recursos mobilizados, de modo a garantir a segurança, integridade e fiabilidade das redes e sistemas digitais, sem com isso pôr em causa as respetivas acessibilidade e funcionalidade, por um lado, e, por outro, a privacidade, propriedade e liberdade dos destinatários/utilizadores que com a sua intervenção se pretende resguardar. Muitas das recomendações feitas por organizações internacionais nos últimos anos têm incidido precisamente sobre a necessidade de assegurar uma adequada formação ética dos profissionais da cibersegurança, de modo a que estes tenham consciência do impacto significativo que as suas escolhas vão ter na qualidade de vida dos seus destinatários e adotem uma ética de responsabilidade que lhes permita, em cada cenário particular, proceder a uma cuidadosa reflexão, em função dos valores e interesses em presença, analisando riscos e benefícios, estando assim habilitados a fazer escolhas e a tomar decisões que não descurem a preservação e promoção daqueles valores e direitos fundamentais.

1.2. Ética do *hackerismo*

Uma das questões que mais debate tem suscitado no âmbito da cibersegurança prende-se com a eventual consagração de padrões éticos no seio da chamada comunidade *hacker*. Uma grande parte das estratégias de cibersegurança é dirigida à proteção de dados e recursos digitais contra ataques/acessos intencionais e não autorizados. O uso de elevadas competências informáticas para conseguir aceder indevidamente a recursos digitais é habitualmente designado pelo termo *hacking*, sendo que os respetivos agentes têm por hábito formar comunidades, ou redes, entre as quais partilham informação e conhecimento. **A origem, em certa medida comum, do *hacking* e das práticas de cibersegurança no seio de coletividades amadoras e informais, torna necessário desenvolver padrões éticos claros dentro da classe emergente dos profissionais de cibersegurança.** Dados os diferentes papéis que as suas competências específicas os podem levar a desempenhar, e dada a multiplicidade de interesses em jogo, pode haver uma tensão acentuada entre a lealdade devida por estes

prestadores de segurança aos interesses do público e a que é devida aos interesses dos seus empregadores, ou aos interesses de agências governamentais, ou ainda aos interesses de particulares grupos ou subculturas no seio da comunidade da cibersegurança. Isto para além da lealdade devida aos interesses próprios de cada um destes agentes (Vallor, 2018: 11).

A expressão *hacker* é frequentemente empregada com uma conotação negativa, em direta relação com práticas de cibercrime. No entanto, o *hacking*, em si mesmo, não é ilegal, a não ser quando comprometa a segurança de um computador ou de uma rede informática sem o prévio consentimento do seu proprietário. Hoje em dia, muitas empresas e mesmo agências governamentais têm *hackers* ao seu serviço, com a responsabilidade de garantir a segurança dos respetivos sistemas digitais. Esta mesma duplicidade tem levado alguns autodenominados *hackers* a traçar uma distinção entre invasões não maliciosas de computadores ou redes informáticas, que descrevem como *hacking*, e maliciosas, que designam de *cracking*. Uma designação mais comum é a que distingue entre *hackers* de chapéu branco, preto ou cinzento, uma nomenclatura inspirada nos antigos filmes do Oeste, onde os "maus" usavam um chapéu de *cowboy* preto, enquanto os "bons" se distinguiam por usar um chapéu branco (Gerard, 2019: 189). Determinantes para a integração em cada uma destas categorias são as respetivas motivações e a ilegalidade das práticas, uma vez que os recursos e métodos empregados são fundamentalmente os mesmos. Os *hackers* de chapéu branco, também conhecidos como *ethical hackers*, dedicam-se a descobrir vulnerabilidades em sistemas ou redes digitais, com o conhecimento e consentimento dos respetivos proprietários. O objetivo é o de reforçar a segurança das mesmas redes, prevenindo eventuais ataques pela prévia resolução daquelas falhas. Podem trabalhar para empresas, agências governamentais, ou outras entidades, públicas e privadas, como especialistas de segurança aos quais compete detetar vulnerabilidades ao nível do *software* ou do *hardware* digital, de preferência antes que os *hackers* de chapéu preto o façam. Por contraposição, estes são aqueles *hackers* que, dotados dos mesmos extensos conhecimentos sobre como entrar nas redes digitais e contornar protocolos de segurança, o fazem sem autorização dos proprietários e com intuitos perniciosos. São movidos pelo ganho pessoal, que pode ou não ser financeiro, ou podem também estar envolvidos em ciberespionagem ou em ações de protesto, por entenderem, desde logo, que o acesso à informação deve ser livre (são os chamados *hacktivistas*). Podem-se dedicar ao roubo de dados, especialmente de natureza financeira, mas também de ordem pessoal, ou de credenciais de *login*; para além do roubo, podem pretender a modificação ou destruição desses mesmos dados.

Há ainda a referência aos *hackers* de chapéu cinzento que, não tendo propósitos maliciosos, procuram falhas e vulnerabilidades em determinados computadores ou redes informáticas sem a autorização dos respetivos proprietários, para com isso obter algum ganho, ainda que sem intenção de explorar as falhas detetadas. O seu propósito é o de, uma vez detetada alguma brecha de segurança, reportar a mesma ao proprietário a troco de alguma compensação financeira. Não conseguindo acordo da parte deste, propõem-se divulgar publicamente aquela mesma vulnerabilidade. A metáfora do chapéu cinzento vai precisamente ao encontro de uma zona ambígua de moralidade, que é aquela em que se movem estes agentes.

O que sucede muito frequentemente é que qualquer *hacker* se vê com acesso a informação sensível, quer de natureza pessoal, quer empresarial, detendo um enorme poder sobre redes, aplicações e sistemas digitais. O modo como irá gerir esse conhecimento, esse poder e essa autoridade, resume-se muitas vezes aos seus próprios padrões ético-morais (Persing, 2018). Isto justifica o cuidado que devem ter as empresas fornecedoras de serviços na contratação dos seus profissionais de cibersegurança: estes devem dar mostras de elevada competência técnica, naturalmente, mas devem igualmente ser selecionados em função dos padrões éticos que imprimem nas suas escolhas e decisões.

A este propósito, é também de referir o conceito muito debatido de divulgação responsável, ou divulgação ética (*responsible or ethical disclosure*). **A partir do momento em que um hacker deteta uma vulnerabilidade numa rede ou num sistema operativo, qual o caminho que deve trilhar?** Uma divulgação pública imediata, sem que exista uma solução que permita colmatar aquela "abertura" do sistema, poderá prejudicar o fornecedor, deixando também expostos os próprios consumidores. Mas até que ponto é ético não proceder a essa divulgação, deixando os utilizadores à mercê de eventuais ataques e ameaças? Uma divulgação responsável, também dita híbrida (CANVAS, 2017b: 9), é aquela que reporta a fragilidade ao fornecedor do serviço em causa, dando-lhe um prazo razoável para encontrar uma solução, antes de proceder a uma divulgação total. A necessidade, hoje, é a de conciliar esta divulgação responsável com o chamado "mercado de vulnerabilidades", em que peritos em segurança se dedicam a descobrir falhas nas redes digitais com o objetivo de as vender aos respetivos fornecedores.

As questões éticas levantadas pela cibersegurança são tão variadas como os próprios contextos em que a mesma se vai tornando uma exigência, apresentando particularidades próprias consoante se esteja a lidar com armazenamento de dados, questões de criptografia, contratação eletrónica, assinaturas digitais, cibercrime ou segurança nacional. Esta heterogeneidade contextual e a permanente evolução do universo digital tornam difícil a implementação uniforme de diretrizes éticas pelas quais se possa pautar esse domínio. **Não existe um código único, pormenorizado e estável, que permita aos fornecedores de tecnologias de cibersegurança saber, em cada situação particular, qual a melhor estratégia a adotar**.

1.3. Cibersegurança, Ética e Direito

Há muito que os juristas romanos ensinaram que nem tudo o que é permitido por lei é honesto, ou seja, moral ou eticamente aceitável. O Direito e a Ética não se confundem, nem se podem substituir. O risco de que isso aconteça é, desde logo, o de que os agentes a quem compete implementar recursos de cibersegurança se conformem com a conceção e aplicação de mecanismos técnicos que se limitem a cumprir os parâmetros morais mínimos que a lei incorpora, desprezando a verdadeira dimensão ética inerente à sua atuação. Não basta o respeito pela legislação aplicável, sendo igualmente necessária a observância de princípios e valores éticos. Isso mesmo é assumido, por exemplo, nas *Orientações Éticas para uma Inteligência Artificial (IA) de Confiança*, de 2019[2], onde a Ética é identificada como uma das três componentes essenciais de uma IA de confiança, lado a lado com a legalidade e a solidez técnica e social. Segundo este documento, cada uma das componentes é necessária, mas não suficiente, para alcançar uma IA de confiança, pelo que o ideal é que as três funcionem em harmonia, sobrepondo-se na sua ação.

A esfera jurídica pode, e deve, fornecer o enquadramento da atuação dos agentes a quem compete implementar recursos de cibersegurança. Tem procurado fazê-lo, a nível nacional, supranacional e internacional. Mas compete aos seus agentes ir mais além do Direito. Até porque o discurso da lei, onde ela existe, se vê naturalmente permeado por esse potencial de indeterminação de sentidos que torna a sua aplicação largamente dependente da sensibilidade de quem tem que a interpretar.

2 As Orientações foram preparadas por um grupo independente de peritos de alto nível sobre a IA, criado pela Comissão Europeia em 2018, e estão disponíveis em https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [21.12.2020].

As inovações tecnológicas sucedem-se a um ritmo vertiginoso, avassalador, reconfigurando de dia para dia a construção social das nossas vidas e não permitindo ao legislador um acompanhamento efetivo dessas transformações. **As soluções jurídicas são facilmente ultrapassadas e tornadas obsoletas pela velocidade, alcance e complexidade dos desenvolvimentos tecnológicos e dos seus muitas vezes imprevisíveis impactos sociais, o que tem levado os decisores políticos a privilegiar os códigos de conduta, enquanto instrumentos normativos mais flexíveis e adaptáveis à evolução das novas tecnologias.** Essa foi, por exemplo, a justificação dada pela Comissão Europeia, em 1987, quando recomendou a adoção de um Código Europeu de Boa Conduta em Matéria de Pagamento Eletrónico (87/598/CEE), considerando ser "evidente que a tentativa de definir [de] um modo rígido e preciso o funcionamento de sistemas em plena mutação poderia levar ao estabelecimento de regras rapidamente ultrapassadas, que constituiriam mesmo obstáculo ao desenvolvimento tecnológico" e que uma "abordagem de incitação", tal como o Código de boa conduta, seria preferível.

O desencontro entre os tempos do Direito e da tecnologia é particularmente sensível no domínio do Direito Penal, porque da sua aplicação resultam restrições a direitos fundamentais, desde logo, a liberdade. Os avanços e recuos no Direito Penal – de neocriminalização ou descriminalização –, a interpretação das normas que o compõem e a sua imposição aos casos concretos obrigam a uma ponderação, reflexão e análise minuciosas, algo que só é possível num espaço e tempo suficientemente espraiados.

As dificuldades que as novas tecnologias criam ao Direito (e ao Direito Penal em particular, por força do princípio da tipicidade) refletem-se, desde logo, ao nível da descrição normativa, pelo léxico usado. **A realidade tecnológica é algo que o Direito tem dificuldade em incorporar ou transformar em letra de lei, seja porque se trata de um léxico completamente estranho ao Direito, seja pela transitoriedade desse mesmo léxico**. Por essa razão, uma das técnicas legislativas encontradas, em particular no Direito da União Europeia, tem sido a de redigir uma lista de definições relevantes para um determinado diploma, as quais "visando resistir ao desafio da temporalidade das tecnologias, consistem em redações terminológicas de um elevado grau de abstração" (Freitas & Novais, 2018). Por vezes, porém, a abstração traz consigo complexidade, opacidade e falta de clareza, minando o objetivo principal das definições, que é o de auxiliar o intérprete. O desafio que se coloca é, então, o de encontrar conceitos e definições suficientemente abstratos para resistir ao polimorfismo da evolução tecnológica e, ao mesmo tempo, suficientemente concretos, para que a leitura do texto legal se torne mais acessível.

Acresce ainda a problemática da hiperespecialização académica e profissional, que leva a que "os operadores judiciários, preparados quase que exclusivamente para as tarefas de leitura e interpretação da lei, não disponham, em regra, das capacidades técnicas e académicas para a compreensão do horizonte material que cada um dos termos técnicos relacionados com novas tecnologias implica na vida prática. Esta circunstância, fomentada pela falta de aposta na multidisciplinaridade da formação profissional e académica, redunda, a jusante, na impossibilidade de apreciação autónoma do caso que necessite de ser qualificado juridicamente" (Freitas & Novais, 2018).

1.4. Cibersegurança e proteção de valores fundamentais

Subjacente à relevância de preocupações éticas no campo da cibersegurança, está a necessidade de proteger determinados valores que se mostram estruturantes do Estado de Direito e de uma sociedade livre e democrática. O trabalho desenvolvido por aqueles a quem compete providenciar a segurança do (e no) cada vez mais denso e complexo ecossistema digital, sendo um trabalho técnico, é também um trabalho que se exerce no seio do intrincado tecido de valores, direitos e interesses que conformam aquele Estado de Direito e aquela sociedade livre e democrática. A necessidade de proteger e promover esse tecido, evitando ameaças e reagindo a comportamentos capazes de os pôr em causa, obriga a escolhas e a decisões que têm uma inequívoca dimensão ética. Nem sempre essas escolhas e essas decisões serão fáceis e muitos serão os dilemas com que os prestadores desse serviço terão que se confrontar. Haverá frequentemente a necessidade de operar a conciliação desses interesses, desses valores e desses direitos, de acordo com contextos fácticos concretos e de acordo com objetivos situados. Para adotar uma determinada estratégia em detrimento de outra, no sentido de alcançar o equilíbrio desejável entre os vários interesses em presença, será necessário empreender uma cuidadosa reflexão de que serão eixos, entre outros, valores como os da **fiabilidade**, da **transparência**, da **responsabilidade** e dos **direitos fundamentais**. Estes constituirão níveis em torno dos quais será possível agregar grande parte das preocupações éticas desencadeadas pelos desafios da cibersegurança, ainda que dificilmente gozem de plena autonomia no seio dos respetivos processos de reflexão e de decisão, dadas as conexões recíprocas que entre eles necessariamente se estabelecem.

Gerar **confiança** é um propósito-chave da cibersegurança. Trata-se não apenas de garantir a integridade das redes e sistemas digitais, protegendo-os contra ameaças e ataques maliciosos, mas também de assegurar a fidedignidade da informação divulgada *online*, a privacidade (e viabilidade) das comunicações e a fiabilidade das transações financeiras realizadas com recurso a meios digitais, porque disso depende a confiança dos cidadãos no funcionamento das instituições, sejam elas públicas ou privadas. Esta dupla vertente é particularmente visível em período de eleições, pelo potencial de ameaças à integridade do sistema informático de suporte ao ato eleitoral e pelos riscos associados à disseminação de notícias falsas sobre os candidatos, a condução do processo eleitoral e/ou a legitimidade dos resultados.

As notícias falsas (*fake news*) ocupam um lugar proeminente na agenda política europeia desde 2015, quando foi criada a East StratCom Task Force para lidar com campanhas de desinformação então em curso. Em 2017, o Parlamento Europeu solicitou à Comissão Europeia que avançasse com a criação de um novo quadro legislativo em matéria de notícias falsas e de discurso de ódio, com a indicação de que tal quadro deveria contemplar a responsabilização dos operadores das plataformas *online* de modo compatível com a liberdade de expressão, mas que não dispensasse os fornecedores de serviços de levar a cabo os controlos necessários e tecnicamente possíveis. Como acontece em tantos outros domínios da cibersegurança, a opção de adotar um instrumento jurídico vinculativo foi preterida em favor da definição de um conjunto de compromissos e boas práticas de adesão voluntária por parte das principais plataformas digitais e operadores publicitários, através do Código de Conduta da UE sobre Desinformação, de setembro de 2018. Os compromissos assumidos incluem, entre outros, o dever de (a) garantir que todos os anúncios publicitários são claramente distinguíveis do conteúdo editorial; (b) investir em meios tecnológicos para dar prioridade a informações pertinentes, autênticas e fidedignas nas pesquisas, nos *feeds* de notícias ou noutros canais de

distribuição com classificação automática; e (c) apoiar esforços independentes envidados de boa-fé para controlar a desinformação e compreender o seu impacto, incluindo a rede independente de verificadores de factos, uma vez criada, viabilizada pela Comissão Europeia. Na avaliação que fez do primeiro ano de vigência do Código de Conduta, em setembro de 2020 [SWD(2020) 180], a Comissão considerou que o Código constitui um instrumento valioso, por proporcionar o enquadramento para um diálogo estruturado entre as várias partes interessadas sobre a garantia de maior transparência das políticas adotadas pelas plataformas digitais no combate à desinformação, mas reconheceu também algumas limitações decorrentes do carácter autorregulatório do Código[3].

Num século em que a tecnologia domina, ademais, hábitos, relações e memórias, o valor da confiança mostra-se uma exigência nas relações que o cidadão estabelece com as estruturas e redes digitais. Não se pode perder de vista, no entanto, que a mesma confiança está dependente de variáveis que não se circunscrevem às intervenções tecnológicas, ou mesmo às estratégias e políticas de cibersegurança. A confiança do cidadão na integridade e fiabilidade das redes pode limitar-se a refletir uma inconsciência / ignorância face às potenciais ameaças ou aos eventuais riscos que as mesmas comportam, com uma consequente atitude que, mais do que confiança, traduzirá incúria. A confiança do cidadão dependerá não só da existência de adequadas práticas de cibersegurança como igualmente do adequado fomento de uma cultura cívica que, promovendo o seu nível de formação e de informação, contribua para a adoção de comportamentos eticamente responsáveis no ciberespaço.

Para gerar confiança é necessário assegurar a **transparência** dos procedimentos e a rápida comunicação de ameaças e incidentes aos indivíduos e entidades potencialmente afetados. Todos os planos de ação e códigos de conduta adotados sobre a matéria sublinham estes aspetos, ainda que não exista uma regra geral uniformemente aplicável aos diferentes cenários de cibersegurança. Caberá sempre aos operadores de cibersegurança avaliar em concreto, por exemplo, qual o momento adequado para divulgar a existência de vulnerabilidades ou a ocorrência de incidentes junto dos potenciais lesados e do público em geral, ponderando os riscos associados a uma divulgação precipitada (e.g. maximização do risco) e a uma divulgação tardia (e.g. quebra de confiança dos consumidores). O que seja uma notificação atempada é muito discutível e dependerá sempre das circunstâncias e da ponderação de interesses a fazer em cada caso concreto (Vallor, 2018: 11).

Os deveres de transparência incidem sobre diferentes aspetos, consoante a área ou setor em causa. Se se trata do armazenamento de dados pessoais, os operadores têm o dever de informar os consumidores quanto ao modo como os seus dados são usados, analisados e armazenados. Uma preocupação recorrente a respeito da partilha de informação no ciberespaço prende-se com a falta de transparência sobre o modo como os dados são usados pelas empresas e por terceiros, com prejuízo para a privacidade, a segurança e a autonomia dos consumidores (CANVAS, 2017a: 28). Se se trata de relações laborais, é necessário que os empregadores informem os seus empregados sobre o uso de meios informáticos de monitorização do desempenho e sobre as razões que justificam esse uso, com esclarecimentos quanto ao respetivo alcance e potenciais efeitos colaterais. No Código de Conduta da UE sobre Desinformação, por exemplo, a tónica é posta na garantia da transparência quanto à origem da informação e à forma como esta é produzida, divulgada, patrocinada e direcionada, o que implica o dever de escrutinar, controlar e limitar efetivamente a colocação de publicidade nas contas e nos sítios *Web* pertencentes a agentes desinformadores, bem como de informar os utilizadores quanto ao que é propaganda política e publicidade temática, de modo a que estes possam compreender a razão pela qual foram alvo de um determinado anúncio.

3 Informação disponível em https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement [21.12.2020].

A concretização de uma cultura de transparência em matérias relacionadas com a segurança do ciberespaço não é tarefa fácil, atenta a circunstância de se tratar de um domínio que é, por definição, extremamente técnico e cuja linguagem, não sendo cifrada, não deixa de ser críptica para os leigos e o público em geral. Por outro lado, nem sempre os interesses económicos dos agentes implicados vão ao encontro da efetiva implementação dessa cultura de transparência. Cabe aos responsáveis pela cibersegurança a compreensão deste desafio e o empenhamento ético em assegurar que os destinatários das informações prestadas em cumprimento dos seus deveres de transparência compreendem efetivamente o conteúdo dessas informações e ficam cientes dos riscos que enfrentam e das opções de que dispõem.

A **responsabilidade** é outro dos elementos estruturantes de uma qualquer "cultura global de cibersegurança", como a que vimos ser defendida pela Assembleia Geral das Nações Unidas em 2003. Todos os participantes no ciberespaço – Governos, empresas, organizações e utilizadores individuais – são, à sua medida, responsáveis pela segurança dos sistemas e redes de informação e pela fidedignidade da informação que circula *online*. Não surpreende, por isso, que as recomendações e orientações produzidas no quadro de organizações como a União Europeia e a Organização para a Cooperação e Desenvolvimento Económico (OSCE) se dirijam a todas as partes interessadas e ponham a tónica na responsabilidade[4]. É também esse o sentido da Norma ISO 26000, adotada em 2010, que é dirigida a empresas e a organizações de todo o mundo e que procura ajudá-las a compreender qual a sua **responsabilidade social** e de que modo este princípio pode ser traduzido em ações concretas[5].

Espera-se que as empresas de tecnologia assumam as suas responsabilidades na proteção do interesse público, lado a lado com os Governos dos Estados (Vallor, 2018: 3). A responsabilidade ética e deontológica dos profissionais de cibersegurança é explicitada num grande número de Códigos de Conduta adotados por empresas e organizações, como o *Information Systems Security Association (ISSA) Code of Ethics* e o *ACM Code of Ethics and Professional Conduct*. Por último, são cada vez mais frequentes as chamadas de atenção para a importância da tomada de consciência por parte dos indivíduos, enquanto trabalhadores, consumidores e utilizadores, da sua quota-parte de responsabilidade na manutenção de um ecossistema digital livre, seguro e fidedigno.

A cibersegurança assume uma clara dimensão ética precisamente pelos efeitos potencialmente devastadores que a insegurança no ciberespaço, por um lado, e os mecanismos de controlo cibernético, por outro, podem ter para a dignidade da pessoa humana. Os **direitos fundamentais** em risco incluem a privacidade, a liberdade, a propriedade, os direitos de participação política, a informação, a saúde e a própria vida dos indivíduos. A ponderação de interesses e direitos é um exercício ético constante para os decisores políticos, para as empresas e para os profissionais da cibersegurança e os quadros de referência éticos e jurídicos disponíveis não oferecem regras unívocas e prontas a usar em todos os contextos da vida real.

Nem sempre serão de fácil compatibilização, desde logo, as estratégias de cibersegurança adotadas para proteger os interesses privados de indivíduos e organizações e aquelas que visam proteger interesses governamentais, dirigindo-se à segurança nacional. A proteção de infraestruturas críticas de informação face

4 Considerem-se, por exemplo, as já referidas *Orientações Éticas para uma IA de Confiança* e a Recomendação do Conselho da OCDE sobre Inteligência Artificial, ambas de 2019. O texto da Recomendação está disponível em https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [21.12.2020].

5 Informação disponível em https://www.iso.org/iso-26000-social-responsibility.html [21.12.2020].

a ameaças externas tornou-se, especialmente após os ataques de 11 de setembro de 2001, uma prioridade global. A rede digital do Governo, mas também outras infraestruturas de informação públicas e privadas, como a internet ou a rede de telefones, viram-se submetidas a reforçadas medidas de segurança (Brey, 2007: 21-36). Isto implicou, e implica, um maior controlo por parte das instâncias governamentais sobre essas mesmas estruturas, com o risco de abrir as portas a uma vigilância massiva da vida e comportamentos dos cidadãos, e de pôr em causa a sua privacidade e autonomia. Sendo a privacidade um valor que, nas sociedades modernas, corresponde ao ideal de um indivíduo autónomo que é livre para agir e decidir o seu destino, o próprio valor da liberdade individual pode ser ameaçado pela híper-vigilância que é potenciada pelas práticas de cibersegurança.

Numa outra esfera, o combate à disseminação de notícias falsas e às campanhas de desinformação, por exemplo, deve ser levado a cabo sem prejuízo da liberdade de expressão e do direito à informação, pelo que as recomendações feitas às autoridades estatais são no sentido de que estas se abstenham de interferir e censurar conteúdos que não sejam ilegais e que procurem garantir um ambiente favorável a um debate inclusivo e pluralista (ERC, 2019: 3).

Em sociedades em rede, os dados sensíveis raramente ficam confinados ao contexto digital em que foram originalmente criados ou partilhados, representando esta circunstância um risco acrescido de potenciais acessos não consentidos aos mesmos. A quantidade avassaladora de dados pessoais armazenados nas redes digitais expõe diariamente o cidadão a comportamentos maliciosos, e eventualmente criminosos, que põem em risco tanto a sua privacidade como a sua propriedade (desde logo intelectual). Agentes não autorizados podem comprometer a confidencialidade de informação sensível acedendo-lhe indevidamente, manipulando-a, disseminando-a ou mesmo eliminando-a. Este quadro coloca sobre os fornecedores de serviços uma enorme pressão, tendo estes que encontrar soluções adequadas em cenários muito variáveis. Uma vez que o controlo pessoal de dados sensíveis é praticamente impossível de manter em contextos conectados, a responsabilidade ética de impedir danos irreparáveis à privacidade, propriedade e liberdade sai cada vez mais da esfera dos donos originais dos dados sensíveis para integrar os deveres de cuidado próprios do prestador de serviços. A qualidade técnica e ética dos assessores de segurança junto destas entidades mostra-se aqui uma fundamental linha de proteção.

Nas cidades inteligentes em que hoje vivemos, caracterizadas pela crescente aplicação da ciência e das TIC à governação pública, a adoção de uma adequada política de cibersegurança mostra-se igualmente vital para proteger a integridade física e a própria vida do cidadão. Isto é passível de acontecer, desde logo, ao nível das chamadas estruturas críticas de segurança, que integram sistemas digitais com uma componente de controlo em tempo real, e que podem ter um impacto direto na vida dos cidadãos. São exemplos os sistemas digitais de controlo de reatores nucleares, de aviões ou de tráfego aéreo, sistemas de mísseis ou redes de assistência médica. A falta de integridade de alguns outros tipos de sistema pode igualmente implicar consequências passíveis de ameaçar o valor da vida de modo mais indireto, incluídos aqui sistemas digitais vocacionados para o desenho, monitorização, diagnóstico ou tomada de decisões. Como exemplo, tomem-se os de sistemas empregados para desenho de pontes ou para diagnóstico médico (Brey, 2007: 21-36). Práticas deficitárias de cibersegurança podem assim revelar-se, mais do que ineficazes, verdadeiramente antiéticas, na medida em que, ora pecando por excesso ora por defeito, põem em risco valores e direitos fundamentais do cidadão, e com esses, um eixo central da preservação de uma sociedade livre e democrática.

DESTAQUES

A insegurança no ciberespaço e os mecanismos de controlo e proteção cibernéticos podem ter efeitos devastadores para a dignidade da pessoa humana, com o potencial de afetar valores como a privacidade, propriedade, liberdade, saúde ou mesmo a vida.

Os fundamentais desafios éticos com que se defronta a cibersegurança prendem-se com a necessidade de a mesma cumprir os seus propósitos no respeito pelos limites que constituem os valores subjacentes à proteção da dignidade da pessoa humana.

Os fornecedores de cibersegurança têm de lidar com os desafios éticos associados ao conhecimento dos limites da sua própria atuação: saber até onde devem ir para garantir os propósitos de segurança e integridade das redes, sem contender com os interesses e direitos fundamentais dos vários agentes envolvidos.

A heterogeneidade dos contextos em que atua a cibersegurança e a celeridade a que se verificam as transformações tecnológicas inviabilizam a implementação de diretrizes éticas estáveis e uniformes.

O legislador tem dificuldade em acompanhar em tempo útil as transformações tecnológicas. Em todo o caso, a ética não se esgota nas leis, nem se confunde com elas. Um comportamento lícito não é necessariamente um comportamento ético.

A definição de estratégias de cibersegurança deve atender à proteção de valores passíveis de congregação em torno dos eixos da confiabilidade, da transparência, da responsabilidade e dos direitos fundamentais.

A promoção da cultura de transparência e da ética de responsabilidade impende sobre as entidades prestadoras de serviços, públicas ou privadas, sobre os profissionais de cibersegurança e sobre os próprios cidadãos, enquanto utilizadores das plataformas e sistemas digitais.

É fundamental o papel desempenhado pelos cidadãos, informados e educados numa ética de responsabilidade, para o adequado funcionamento das estruturas e redes digitais.

2. GENEALOGIA LEGAL

2.1. A regulação da segurança no ciberespaço – panorama geral

O carácter transfronteiriço do ciberespaço e os riscos que os maus usos das TIC representam para a segurança da comunidade internacional no seu todo motivaram, a partir da década de 1990, um grande número de iniciativas dirigidas ao reforço da cooperação entre os Estados e à definição de princípios e regras comuns em matéria de cibersegurança. A primeira iniciativa deste tipo foi avançada no quadro da OCDE, em 1996, e consistiu numa proposta da França de adoção de uma Carta para a Cooperação Internacional na Internet, largamente decalcada das regras existentes de Direito Internacional do Mar (Mačák, 2016: 130). A proposta não foi acolhida, tal como não viria a ser acolhida a proposta de adoção de um tratado para proibir o uso de armas informáticas, avançada pela Rússia no quadro da ONU, em 1998. A proposta russa teve, em todo o caso, o efeito de colocar a regulação do ciberespaço na agenda da ONU, ao motivar a primeira resolução da Assembleia Geral sobre os "desenvolvimentos no setor da informação e telecomunicações no contexto da segurança internacional" (A/RES/53/70) e a subsequente constituição de um Grupo de Peritos Governamentais para estudar as ameaças oriundas do ciberespaço e as possíveis soluções jurídicas para as enfrentar (Eggenschwiler, 2019: 3). No seu relatório de 2013, o Grupo de Peritos concluiu que as normas de Direito Internacional já existentes – desde logo, a Carta da ONU – se aplicam ao ciberespaço (UN Doc A/68/98), uma pronúncia que, sem ser inteiramente esclarecedora quanto à substância e ao modo daquela aplicação, parece ter condenado quaisquer planos de adoção de um tratado internacional de âmbito mundial sobre cibersegurança num futuro próximo (Mačák, 2016: 128-130).

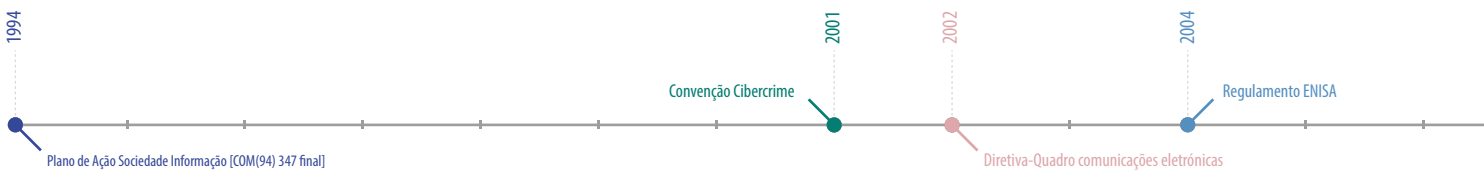
A opinião dominante entre os Estados ocidentais e as principais empresas de tecnologia tem sido a de que, atenta a velocidade dos avanços tecnológicos e a tendencial rigidez das soluções jurídicas, a regulação do ciberespaço não deve ser feita por meio de regras jurídicas vinculativas, mas sim por meio de recomendações e compromissos políticos a que as partes interessadas (Estados, empresas, organizações) adiram voluntariamente (Osula & Rõigas, 2016: 15-16). Neste processo, os Estados perderam o protagonismo na definição do quadro normativo aplicável, cedendo espaço à autorregulação das empresas de tecnologia e aos meios académicos (Mačák, 2016: 134-136; Eggenschwiler, 2019: 4-7). Entre as muitas iniciativas lançadas na última década, refiram-se apenas, a título de exemplo, o Manual Tallinn sobre as regras de Direito Internacional aplicáveis à guerra informática, publicado em 2013, o Manual Tallinn 2.0 sobre as regras de Direito Internacional aplicáveis às operações cibernéticas, publicado em 2017, e os Livros Brancos da Microsoft sobre normas internacionais de cibersegurança e a sua aplicação, publicados em 2014 e em 2016. A multiplicidade de iniciativas contribui para uma grande fragmentação do quadro normativo de referência sobre o que seja o comportamento responsável no

ciberespaço e alguma incerteza sobre as normas aplicáveis; uma incerteza para que também contribui a inexistência de consenso sobre o que sejam normas cibernéticas (*cyber norms*) e o facto de diferentes atores usarem a designação para referir, de forma aparentemente indistinta, normas jurídicas, políticas, técnicas e éticas (Osula & Rõigas, 2016: 11).

A popularidade dos Códigos de Conduta e demais instrumentos de *soft law não obsta, entretanto, a que tenham ocorrido alguns desenvolvimentos significativos no plano da* adoção de instrumentos jurídicos vinculativos, sobretudo de âmbito regional. Importa referir, desde logo, a adoção da Convenção sobre o Cibercrime (Convenção de Budapeste), em 23 de novembro de 2001. Apesar de ter sido adotada sob a égide do Conselho da Europa, a Convenção foi aberta à assinatura, não apenas dos Estados Membros desta organização, mas também dos países terceiros que participaram na sua redação (e.g. Argentina, Austrália, Cabo Verde, Canadá, Estados Unidos da América, Israel e Japão) e prevê expressamente a possibilidade de outros países terceiros virem a assiná-la, mediante solicitação ao Comité de Ministros do Conselho da Europa e acordo unânime dos Estados Parte. Em 2003, foi adotado um Protocolo Adicional à Convenção, relativo à incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos. Segundo um relatório do Gabinete de Cibercrime do Conselho da Europa, publicado em março de 2020, 106 Estados Membros da ONU (55%) dispõem já de legislação nacional que criminaliza agressões contra sistemas informáticos e através de meios informáticos, em linha com a Convenção de Budapeste.

No quadro da União Europeia, a atividade legislativa em matérias relacionadas com o ciberespaço tem sido incessante desde a adoção pela Comissão Europeia do seu primeiro Plano de Ação para a Sociedade da Informação, em 1994 [COM(94) 347], ainda que os esforços regulatórios tenham andado de par com o elogio à autorregulação da indústria das TIC e com incentivos à adoção de Códigos de Conduta [e.g. COM(96) 487]. O primeiro ato legislativo da UE no domínio da cibersegurança foi a Diretiva 2016/1148, relativa à segurança das redes e da informação (SRI), mas as preocupações com a cibersegurança estiveram presentes desde o início e são visíveis nos instrumentos legislativos adotados ao longo dos anos, em matérias como o tratamento de dados pessoais (e.g. Diretivas 1995/46/CE e 1997/66/CE, Regulamento UE 2016/679), a assinatura eletrónica (Diretiva 1999/93/CE), o comércio eletrónico (Diretiva 2000/31/CE), as comunicações eletrónicas (e.g. Diretivas 2002/21/CE, 2002/22/CE, 2018/1972) e o cibercrime (e.g. Diretiva 2013/40/UE).

A importância da cibersegurança na agenda política da UE levou à criação, em 2004, da Agência Europeia para a Segurança das Redes e da Informação (ENISA), com o propósito de ser um centro especializado a nível europeu, competente para orientar, dar pareceres e prestar assistência às instituições da União e aos Estados Membros, e para cooperar com a comunidade empresarial, a fim de garantir um nível de segurança das redes e da informação elevado e eficaz e com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas. Sucessivos instrumentos legislativos têm vindo a renovar o mandato e a reforçar as atribuições da ENISA, o mais recente dos quais o Regulamento (UE) 2019/881, que lhe conferiu um mandato por período indeterminado.

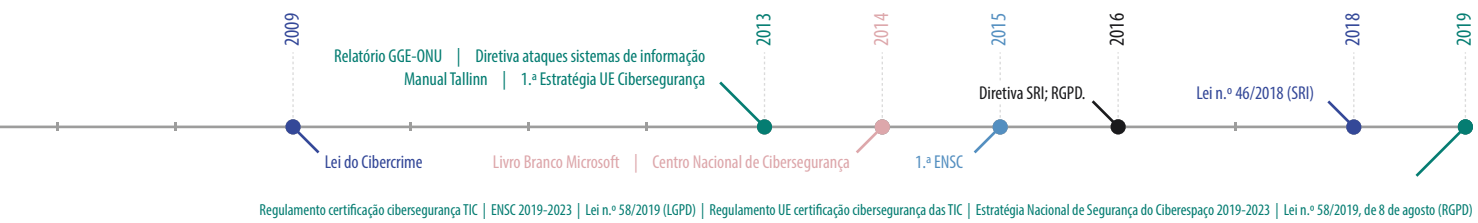


A Diretiva SRI resultou de uma proposta legislativa anexa à primeira Estratégia da União Europeia para a Cibersegurança, apresentada em 2013 numa comunicação conjunta da Comissão Europeia e da Alta Representante da UE para os Negócios Estrangeiros e a Política de Segurança [JOIN(2013) 1]. A Estratégia sublinhou as responsabilidades partilhadas por Governos, indústria e cidadãos e mapeou as ações necessárias por parte das instituições europeias, dos Estados e da indústria para "tornar o ambiente em linha na UE o mais seguro do mundo", incluindo medidas legislativas em matéria de cibercriminalidade (sobretudo por referência à Convenção de Budapeste) e de segurança das redes e da informação. Quanto a este último ponto, a Estratégia reconheceu os progressos alcançados com base em compromissos voluntários, mas identificou várias lacunas, pelo que avançou uma proposta legislativa sobre requisitos comuns para segurança das redes e da informação, com vista a obrigar os Estados Membros a adotarem estratégias nacionais e a designarem autoridades nacionais competentes sobre a matéria.

Entretanto, as questões da cibersegurança têm continuado a ocupar os decisores europeus, com novas estratégias [e.g. JOIN(2017) 450] e novos instrumentos legislativos. O "pacote de cibersegurança" avançado em 2017 incluiu uma proposta da Comissão Europeia para a criação de um quadro de certificação da cibersegurança a nível da UE [COM(2017) 477], o que veio a ser concretizado em 2019 com a adoção do Regulamento (UE) 2019/881, relativo à ENISA e à certificação da cibersegurança das TIC. Em 16 de dezembro de 2020, foi apresentada a Estratégia de cibersegurança da UE para a década digital [JOIN(2020) 18]. Em debate, neste momento, encontram-se, entre outras, as proposta da Comissão para um regulamento relativo a ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal [COM(2018) 225] e para um regulamento que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação [COM(2018) 630].

Em Portugal, as políticas públicas e os desenvolvimentos legislativos em matéria de cibersegurança têm vindo a acompanhar as diretrizes definidas pela União Europeia e os compromissos assumidos no quadro do Conselho da Europa. A Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, transpôs a Decisão-Quadro 2005/222/JAI, do Conselho da União Europeia, relativa a ataques contra sistemas de informação, e adaptou a ordem jurídica nacional à Convenção de Budapeste. A Lei n.º 46/2018, de 13 de agosto, transpôs a Diretiva SRI, estabelecendo o regime jurídico da segurança do ciberespaço. A Lei n.º 58/2019, de 8 de agosto, veio assegurar a execução, na ordem jurídica portuguesa, do Regulamento Geral sobre a Proteção de Dados, etc. No plano institucional, as matérias da cibersegurança caem sob a alçada de diferentes entidades, como o Gabinete Cibercrime do Ministério Público, a Polícia Judiciária e a Comissão Nacional de Proteção de Dados, mas a Autoridade Nacional de Cibersegurança é o Centro Nacional de Cibersegurança, criado em 2014, que funciona no âmbito do Gabinete Nacional de Segurança.

A primeira Estratégia Nacional de Segurança do Ciberespaço foi adotada em 2015, com o propósito de estabelecer, em sintonia com as linhas gerais da Estratégia da UE para a Cibersegurança, "objetivos e linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio". A Estratégia alicerça-se em cinco pilares – subsidiariedade, complementaridade,



cooperação, proporcionalidade e sensibilização – e desenvolvia-se em quatro objetivos estratégicos:

- promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
- proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
- fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; e
- afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

A Estratégia Nacional aprovada em 2019, para o período 2019-2023, continua a alicerçar-se nos princípios de subsidiariedade, complementaridade e proporcionalidade, assumindo agora como objetivos estratégicos maximizar a resiliência, promover a inovação e gerar e garantir recursos. Os eixos de intervenção definidos pela Estratégia para 2019-2023 cobrem

- a estrutura de segurança do ciberespaço
- a prevenção, educação e sensibilização
- a proteção do ciberespaço e das infraestruturas
- a resposta às ameaças e combate ao cibercrime
- a investigação, desenvolvimento e inovação, e
- a cooperação nacional e internacional.

Ambas as Estratégias sinalizam como prioritária a permanente avaliação das necessidades de revisão e atualização do quadro legislativo em vigor (sobretudo, em matéria penal e processual penal), de modo a "incorporar a evolução tecnológica e as novas práticas" e a assegurar a "máxima eficiência" dos preceitos legais.

DESTAQUES

Desde a década de 1990, as iniciativas dirigidas ao reforço da cooperação entre os Estados e à definição de princípios e regras comuns em matéria de cibersegurança multiplicaram-se em vários *fora* (OCDE, ONU, Conselho da Europa, União Europeia, meios académicos, etc.).

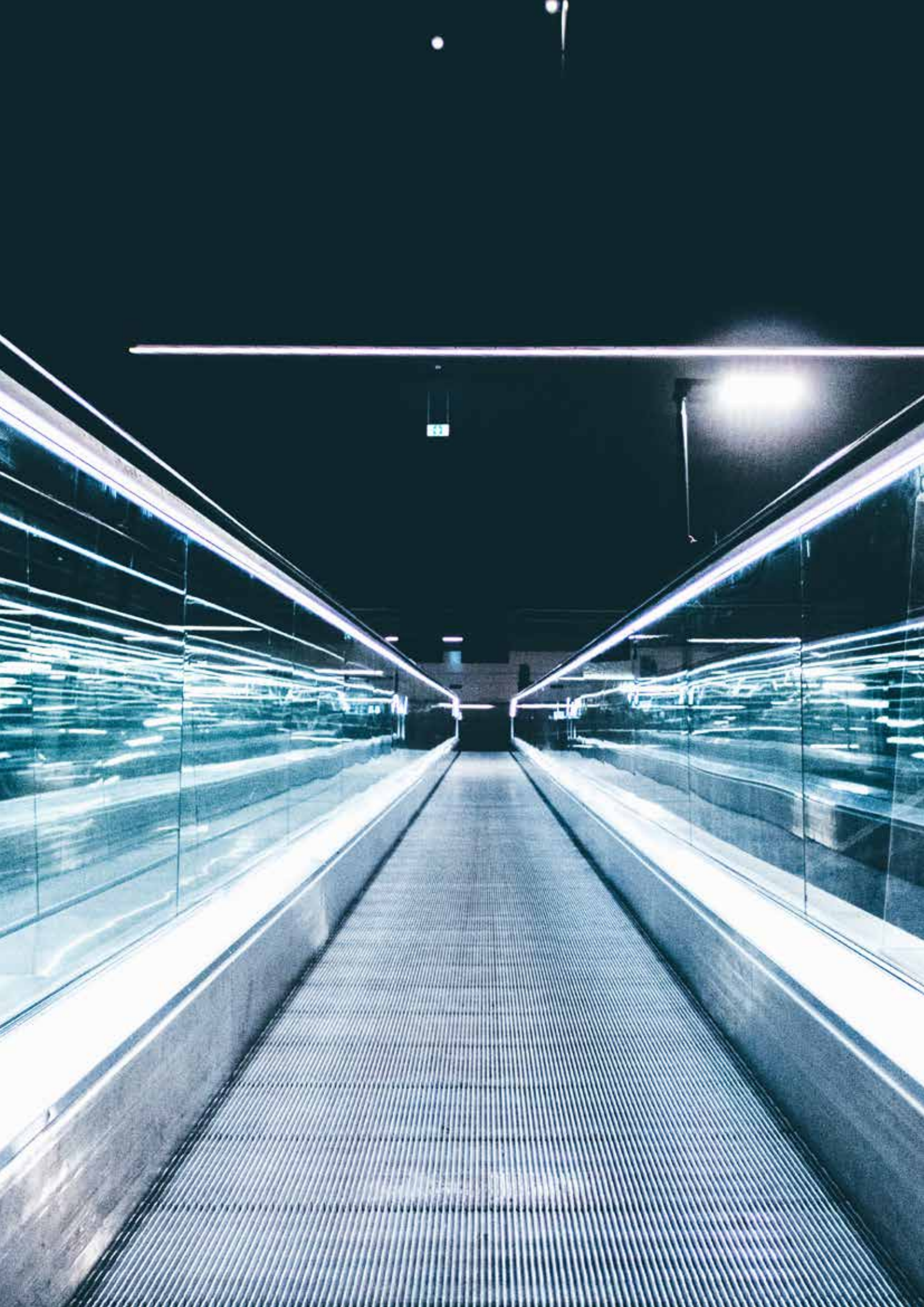
Em 2013, um Grupo de Peritos da ONU concluiu que as normas de Direito Internacional já existentes – desde logo, a Carta da ONU – se aplicam ao ciberespaço, o que contribuiu para adiar *sine die* quaisquer planos de adoção de um tratado internacional de âmbito mundial sobre cibersegurança.

A opinião dominante entre os Estados ocidentais e as principais empresas de tecnologia tem sido a de que, atenta a velocidade dos avanços tecnológicos e a tendencial rigidez das soluções jurídicas, a regulação do ciberespaço não deve ser feita por meio de regras jurídicas vinculativas, mas sim por meio de recomendações e compromissos políticos a que as partes interessadas (Estados, empresas, organizações) adiram voluntariamente.

A popularidade dos Códigos de Conduta e demais instrumentos de *soft law* não obsta a que tenham ocorrido alguns desenvolvimentos significativos no plano da adoção de instrumentos jurídicos vinculativos, sobretudo de âmbito regional, destacando-se a Convenção de Budapeste sobre o Cibercrime, adotada em 2001, no quadro do Conselho da Europa, e os numerosos Regulamentos e Diretivas da União Europeia.

O primeiro ato legislativo da União Europeia no domínio da cibersegurança foi a Diretiva 2016/1148, relativa à segurança das redes e da informação (SRI), mas as preocupações com a cibersegurança estiveram presentes desde o início e são visíveis nos instrumentos legislativos adotados ao longo dos anos, em matérias como o tratamento de dados pessoais, a assinatura eletrónica, o comércio eletrónico, as comunicações eletrónicas e o cibercrime.

Em Portugal, as políticas públicas e os desenvolvimentos legislativos em matéria de cibersegurança têm vindo a acompanhar as diretrizes definidas pela União Europeia e os compromissos assumidos no quadro do Conselho da Europa.



2.2. Quadro institucional de referência

Agência da União Europeia para a Cibersegurança (ENISA)

Foi criada, em 2014, para funcionar como um centro especializado de apoio às instituições europeias e aos Estados Membros em matéria de cibersegurança. Hoje, exerce as atribuições que lhe são conferidas pelo Regulamento (UE) 2019/881, nos termos do qual passou a ter um mandato permanente, e pelos demais atos jurídicos da União no domínio da cibersegurança, o que inclui, nomeadamente, a contribuição para a elaboração e a execução da política e do Direito da União em matéria de cibersegurança; a prestação de assistência para reforço das capacidades dos Estados Membros e das instituições e organismos da UE; o apoio à cooperação operacional entre Estados Membros, instituições da UE e outras partes interessadas; o apoio à elaboração e execução da política da União em matéria de certificação da cibersegurança dos produtos, serviços e processos de TIC; a produção de conhecimento e informação; a organização de campanhas de sensibilização e educação; a contribuição para a agenda estratégica da investigação e inovação ao nível da UE no domínio da cibersegurança; a contribuição para os esforços de cooperação da União com países terceiros e organizações internacionais. A ENISA tem sede em Atenas, na Grécia. É composta por um conselho de administração, uma comissão executiva, um diretor executivo, um grupo consultivo e uma rede de agentes de ligação nacionais e é assistida por um Comité[6].

Computer Emergency Response Team for the EU Institutions (CERT.EU)

Equipa de resposta a emergências informáticas, responsável pela segurança dos sistemas informáticos das instituições, agências e organismos da UE. Foi instituída de modo permanente, em setembro de 2012, em cumprimento da Agenda Digital para a Europa lançada pela Comissão Europeia em 2010. A equipa é composta por peritos de segurança informática das principais instituições da UE (Comissão Europeia, Secretariado Geral do Conselho, Parlamento Europeu, Comité

6 Mais informações disponíveis em https://www.enisa.europa.eu/ [12.12.2020].

das Regiões e Comité Económico e Social). A CERT.EU colabora de forma estreita com equipas congéneres nos Estados Membros e em países terceiros, bem como com empresas especializadas em segurança informática. Prevê-se que a CERT.EU venha a alargar gradualmente os serviços prestados, em resposta às necessidades dos seus utilizadores e tendo em atenção os recursos e competências disponíveis[7].

Centro Europeu da Cibercriminalidade (EC3)

Criado em 2013, por proposta da Comissão Europeia [COM(2012) 140], para funcionar como ponto de convergência da luta contra a cibercriminalidade na UE. Faz parte da Europol e tem sede em Haia, Países Baixos. O Centro tem como alvos preferenciais três categorias de cibercrimes: (a) os praticados por grupos criminosos organizados, em especial os que envolvam grandes lucros, como a fraude *online*; (b) os que causem danos graves às vítimas, como a exploração sexual de crianças *online*; e (c) os que afetem as infraestruturas críticas e os sistemas de informação da UE. As funções do Centro incluem a recolha de informações sobre cibercriminalidade, para identificar tendências e ameaças; o apoio ao reforço das capacidades dos Estados Membros, centrado na formação de agentes da polícia e de titulares do poder judicial; o apoio operacional aos Estados Membros, através da criação de equipas de investigação conjunta e do intercâmbio de informações; e, de um modo geral, a atuação como interlocutor coletivo dos investigadores europeus de cibercrimes a nível das autoridades policiais e do poder judicial, nas discussões com o setor das TIC e outras empresas do setor privado, com a academia e as organizações da sociedade civil[8].

Gabinete Nacional de Segurança (GNS)

Serviço central da administração direta do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro. O seu diretor-geral é, por inerência, a Autoridade Nacional de Segurança, que é quem exerce, em exclusivo, a proteção, o controlo e a salvaguarda da informação classificada. Nos termos do Decreto-Lei n.º 3/2012, de 16 de janeiro (versão dada pelo Decreto-Lei n.º 136/2017, de 6 de novembro), o Gabinete tem por missão garantir a segurança da informação classificada

7 Mais informações disponíveis em https://cert.europa.eu/cert/plainedition/en/cert_about.html [12.12.2020].

8 Mais informações disponíveis em https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [12.12.2020].

no âmbito nacional e das organizações internacionais de que Portugal é membro, bem como exercer a função de autoridade de credenciação de pessoas singulares ou coletivas para o acesso e manuseamento de informação classificada, de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas (SCEE) e de entidade credenciadora por força da lei que regula a disponibilização e a utilização das plataformas eletrónicas de contratação pública. As suas atribuições incluem, entre outras, a garantia da articulação e harmonização dos procedimentos relativos à segurança da informação classificada em todos os serviços, organismos e entidades, públicos ou privados, e no âmbito de organizações e atividades internacionais em que Portugal participe; o registo, distribuição e controlo da informação classificada; a avaliação, acreditação e certificação da segurança de produtos e sistemas de comunicações, a promoção do estudo, da investigação e da difusão das normas e procedimentos de segurança aplicáveis à proteção e salvaguarda da informação classificada[9].

Centro Nacional de Cibersegurança (CNCS)

O Centro Nacional de Cibersegurança funciona no âmbito do Gabinete Nacional de Segurança e foi criado em 2014. Tem por missão contribuir para que Portugal utilize o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais. As competências e o funcionamento do CNCS encontram-se definidos no Decreto-Lei n.º 3/2012, de 16 de janeiro (versão dada pelo Decreto-Lei n.º 136/2017, de 6 de novembro), e na Lei n.º 46/2018, de 13 de agosto, que transpôs a Diretiva SRI e que reforçou o papel do CNCS enquanto Autoridade Nacional de Cibersegurança. Nos termos da Lei n.º 46/2018, o CNCS (a) é o ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições da Polícia Judiciária relativas a cooperação internacional em matéria penal; (b) exerce funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias nos termos das suas competências, cabendo-lhe, nomeadamente, emitir parecer

9 Mais informações disponíveis em https://www.gns.gov.pt/ [12.12.2020].

prévio sobre qualquer disposição legal de cibersegurança, receber notificações de incidentes com impacto para a segurança das redes e dos sistemas de informação e instruir os processos de contraordenação; (c) tem o poder de emitir instruções de cibersegurança e de definir o nível nacional de alerta de cibersegurança. O CNCS atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, bem como com a Comissão Nacional de Proteção de Dados[10].

Conselho Superior de Segurança do Ciberespaço

Criado, em 2017, na sequência da aprovação da primeira Estratégia Nacional de Segurança do Ciberespaço de 2015, para funcionar como "grupo de projeto", na dependência do Primeiro-Ministro, com a missão de assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional e respetiva revisão (Resolução do Conselho de Ministros n.º 115/2017). A Lei n.º 46/2018, de 13 de agosto, que transpôs a Diretiva SRI, introduziu algumas alterações à composição e competências do Conselho, que passou a ser definido como o órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço. O Conselho é presidido pelo membro do Governo responsável pela área da cibersegurança e integra, entre muitos outros, a Autoridade Nacional de Segurança, o Coordenador do CNCS, o Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária, um representante do Ministério Público e um representante da Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática. Compete-lhe assegurar a coordenação político-estratégica para a segurança do ciberespaço; pronunciar-se previamente sobre a Estratégia Nacional para a Segurança do Ciberespaço e verificar a sua implementação, incluindo pela elaboração de relatórios anuais de avaliação da execução; propor a aprovação de decisões de caráter programático relacionadas com a definição e a execução da Estratégia Nacional; emitir parecer sobre matérias relativas à segurança do ciberespaço; e responder a solicitações por parte do Primeiro-Ministro no âmbito das suas competências.

10 Mais informações disponíveis em https://www.cncs.gov.pt/ [12.12.2020].

Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária (UNC3T)

Unidade operacional especializada da Polícia Judiciária (PJ), inspirada no modelo adotado pelo EC3 da Europol e criada, em 2016, em substituição da Unidade Nacional da Investigação da Criminalidade Informática. As suas competências incluem: (a) a prevenção, deteção e investigação dos crimes previstos na Lei do Cibercrime, bem como dos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos, nomeadamente, no regime legal de proteção de dados pessoais e no Código dos Direitos de Autor e Direitos Conexos; (b) a prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistema informático, de devassa por meio da informática, de burla informática e nas comunicações, de interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais, de espionagem através de programa informático e de ciberterrorismo; (c) a centralização e tratamento de informação criminal relativa aos crimes da sua competência; (d) a recolha e tratamento de dados estatísticos; (e) a elaboração do Plano Nacional da Polícia Judiciária para a Prevenção e o Combate ao Cibercrime, em articulação com o CNCS; (f) a celebração de protocolos de colaboração técnica e científica com entidades públicas e privadas, nacionais ou estrangeiras; (g) colaborar e participar na formação inicial e contínua sobre cibercrime aos quadros do pessoal de investigação criminal e de apoio da Polícia Judiciária. A UNC3T assegura, no âmbito da cooperação internacional, o ponto de contacto operacional permanente previsto na Lei do Cibercrime[11].

11 Mais informações disponíveis em https://www.policiajudiciaria.pt/unc3t/. [12.12.2020].

Gabinete de Coordenação da Atividade do Ministério Público na Área da Cibercriminalidade

Criado em 2011, o Gabinete Cibercrime funciona na direta dependência da Procuradoria-Geral da República e tem como missão a coordenação interna do Ministério Público na área da cibercriminalidade, a formação específica de Magistrados do Ministério Público nesta matéria, a interação com o setor privado, através do estabelecimento de canais de comunicação com fornecedores de serviço de acesso às redes de comunicação para fins de facilitação da sua colaboração na investigação criminal, a interação com os órgãos de polícia criminal e, residualmente, o acompanhamento de processos concretos. A partir da entrada em vigor da Lei n.º 68/2019, de 27 de agosto, que aprovou o novo Estatuto do Ministério Público, passou a prever-se na lei a existência de gabinetes de coordenação nacional (artigo 55.º). Em execução desta previsão legal, dando continuidade à estrutura anterior, o Conselho Superior do Ministério Público deliberou formalmente constituir o Gabinete Cibercrime, por deliberação da reunião plenária de 20 de outubro de 2020. O Gabinete é dirigido por um Procurador da República e mantém uma rede de pontos de contacto em todo o território nacional, formada preferencialmente por magistrados com experiência de condução de inquéritos sobre crimes previstos na Lei do Cibercrime ou em que existam especiais exigências na obtenção de prova digital ou em que se trate de factualidades especialmente complexas devido ao uso de tecnologias[12].

Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT)

Serviço integrante do CNCS que coordena a resposta a incidentes ocorridos no ciberespaço nacional envolvendo entidades do Estado, operadores de serviços essenciais, operadores de infraestruturas críticas nacionais e prestadores de serviços digitais. Nos termos da Lei n.º 46/2018, o CERT.PT é também competente para monitorizar os incidentes com implicações a nível nacional; ativar mecanismos de alerta rápido; intervir na reação, análise e mitigação de incidentes; proceder à análise dinâmica dos riscos; assegurar a cooperação com entidades públicas e privadas; promover a utilização de práticas comuns ou normalizadas; participar nos *fora* nacionais de cooperação de equipas de resposta

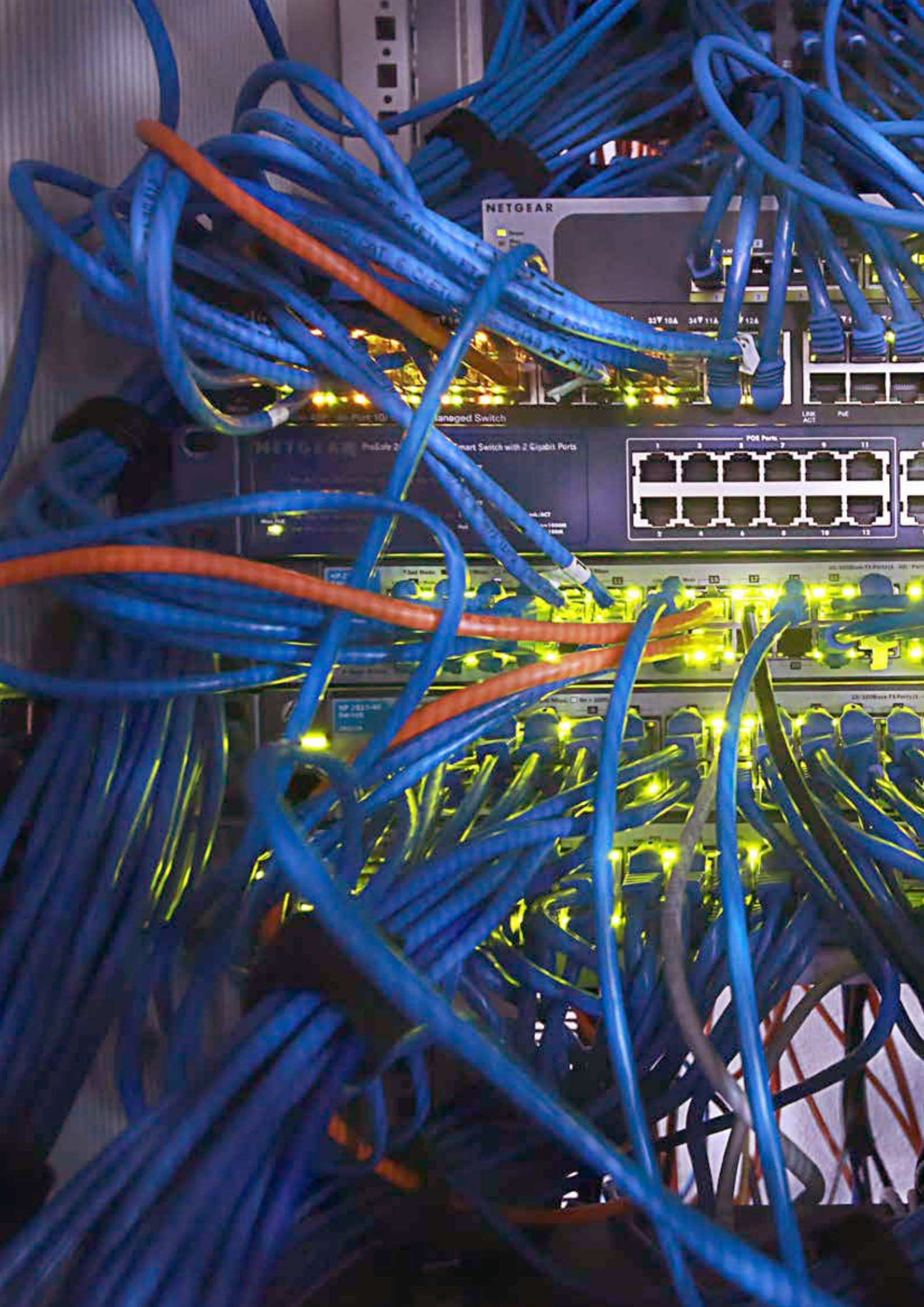
12 Mais informações disponíveis em http://cibercrime.ministeriopublico.pt/ [12.12.2020].

a incidentes de segurança informática; assegurar a representação nacional nos *fora* internacionais de cooperação de equipas de resposta a incidentes de segurança informática; e participar em eventos de treino nacionais e internacionais. O CERT.PT é membro da Rede Nacional de CSIRT e representante nacional na Rede Europeia de CSIRT, estabelecida pela Diretiva SRI. É também membro acreditado do Trusted Introducer e Full Member do Forum of Incident Response and Security Teams (FIRST).

Comissão Nacional de Proteção de Dados (CNPD)

Entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República. É a Autoridade Nacional de Controlo de Dados Pessoais para efeitos do Regulamento Geral de Proteção de Dados (RGPD) da UE e da Lei n.º 58/2019, de 8 de agosto. A CNPD tem como atribuição genérica controlar e fiscalizar o cumprimento do RGPD e da Lei n.º 58/2019, bem como das demais disposições legais e regulamentares que versem sobre a proteção de dados pessoais, com o fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito do tratamento de dados pessoais. Enquanto autoridade nacional de controlo, a CNPD tem as atribuições definidas pelo artigo 57.º do RGPD, que incluem a promoção da sensibilização do público quanto aos riscos e dos responsáveis pelo tratamento quanto às suas obrigações; o aconselhamento ao Parlamento, ao Governo e a outras entidades a respeito de medidas legislativas e administrativas relacionadas com o tratamento de dados; a prestação de informações e a colaboração com autoridades de outros Estados Membros; o incentivo à elaboração de códigos de conduta e ao estabelecimento de procedimentos de certificação de proteção de dados, etc. Tem também os poderes de controlo enunciados no artigo 58.º do RGPD, que lhe permitem, designadamente, exigir a prestação de informações por parte dos responsáveis pelo tratamento de dados; realizar auditorias; fazer advertências e repreensões; e ordenar a satisfação de pedidos de exercício de direitos apresentados pelos titulares dos dados[13].

13 Mais informações disponíveis em https://www.cnpd.pt/ [12.12.2020].


NETGEAR
POE Ports

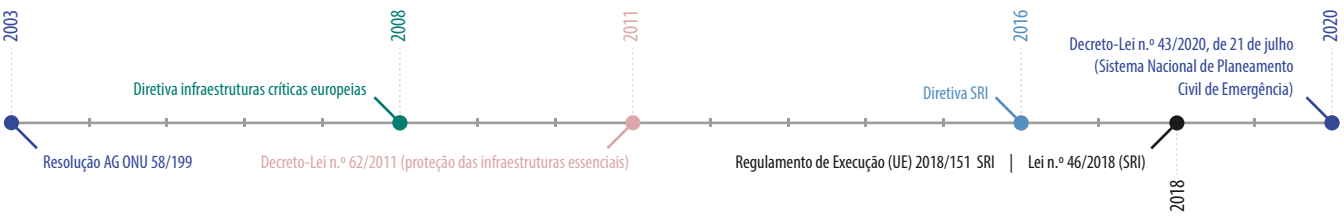
2.3. Análise setorial

2.3.1. Infraestruturas críticas e serviços essenciais

O aumento das ligações (e da dependência) entre as infraestruturas críticas dos Estados – i.e. as usadas para a geração, transmissão e distribuição de energia, o transporte marítimo e aéreo, os serviços bancários e financeiros, o abastecimento de água, a distribuição de alimentos, a saúde pública, etc. – e as redes e os sistemas e serviços de informação trouxe novos riscos e vulnerabilidades para a segurança dos Estados. Na agenda da ONU, a preocupação com a proteção das infraestruturas críticas foi manifestada pela Assembleia Geral, em 2003, com a Resolução 58/199 sobre a criação de uma cultural global de cibersegurança e a proteção das infraestruturas críticas de informação. Apesar de reconhecer que cabe a cada Estado identificar as respetivas infraestruturas críticas, a Assembleia Geral apelou à cooperação internacional nesta matéria e identificou um conjunto de elementos necessários para a proteção das infraestruturas críticas, incluindo a existência de redes de alerta de vulnerabilidades, ameaças e incidentes; a criação e manutenção de redes de resposta a crises, sujeitas a testes frequentes para garantir a sua segurança e estabilidade em situações de emergência; a adoção de legislação adequada à investigação de ataques a infraestruturas críticas e subsequente ação penal, etc.

Na União Europeia, a primeira intervenção legislativa sobre esta matéria teve lugar com a Diretiva 2008/114/CE, de 18 de dezembro, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção. Esta Diretiva teve como objeto estabelecer um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, atenta a relevância de certas infraestruturas para a segurança das pessoas e para a segurança das principais atividades sociais e económicas. "Infraestrutura crítica" foi definida como o elemento, sistema ou parte deste situado nos Estados Membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado Membro, dada a impossibilidade de continuar a assegurar essas funções. A Diretiva introduziu ainda o conceito de "infraestrutura crítica europeia", para designar as infraestruturas críticas situadas nos Estados Membros cuja perturbação ou destruição teria um impacto significativo em, pelo menos, dois Estados Membros.

Esta Diretiva foi transposta para o ordenamento jurídico português pelo Decreto-Lei n.º 62/2011, de 9 de maio, que veio estabelecer os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes. No setor da energia, foram identificadas como prioritárias as infraestruturas e instalações de produção e transporte de eletricidade; as infraestruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos; e as infraestruturas de produção, refinação, tratamento, armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido. No setor dos transportes, foram considerados prioritários os transportes rodoviários, os transportes ferroviários, os transportes aéreos, os transportes por vias navegáveis interiores, os transportes marítimos (incluindo os de curta distância) e os portos.



Em 2016 foi adotada a Diretiva 2016/1148, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em todo o espaço da União Europeia (Diretiva SRI), que veio promover uma cultura de gestão dos riscos e definir requisitos mínimos comuns de segurança. A responsabilidade partilhada entre entidades públicas e privadas foi a pedra de toque deste diploma, consagrando-se também um *standard* mínimo comum de segurança para operadores de serviços essenciais e prestadores de serviços digitais.

A Diretiva SRI inclui na definição de "operadores de serviços essenciais" as entidades públicas ou privadas pertencentes a um dos tipos referidos no seu Anexo II:

- entidades que operem no setor da energia (Eletricidade, Petróleo; Gás);
- entidades que operem no setor dos transportes (transportes aéreos, transportes ferroviários, transportes marítimos e por vias navegáveis interiores, transportes rodoviários);
- entidades do setor bancário e infraestruturas do mercado financeiro;
- entidades do setor da saúde (instalações de prestação de cuidados de saúde, nomeadamente hospitais e clínicas privadas);
- entidades de fornecimento e distribuição de água potável;
- infraestruturas digitais (pontos de troca de tráfego, prestadores de serviços de DNS e registo de nomes de domínio de topo).

Por outro lado, por prestadores de serviços digitais entende-se uma pessoa coletiva que presta um serviço pertencente a um dos tipos enumerados no Anexo III da Diretiva: mercados *online*, motores de pesquisa *online* e serviços de computação em nuvem.

Para a concreta identificação dos operadores de serviços essenciais, foi elencado ainda um conjunto de critérios que se prendem com a atividade social e/ou económica crucial desenvolvida, com a dependência das redes e sistemas de informação para a prestação desse serviço, e com os efeitos perturbadores na prestação desse serviço que um incidente possa causar. Estes efeitos perturbadores serão considerados atendendo ao número de utilizadores que dependem dos serviços prestados, o (possível) impacto dos incidentes sobre as atividades económicas e sociais e sobre a segurança pública, as quotas de mercado e distribuição geográfica da zona que pode ser afetada, e a importância da entidade em causa para a manutenção (ou não) de um nível suficiente do serviço.

Para alcançar um elevado nível comum de segurança das redes e dos sistemas de informação em todo o território da União, é estabelecido um conjunto de medidas, incluindo a criação de um grupo de cooperação (composto por representantes dos Estados Membros, da Comissão Europeia e da ENISA, a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados Membros) e de uma rede de equipas de resposta a incidentes de segurança informática (Rede CSIRT, composta por representantes das CSIRT nacionais, dos Estados Membros e da CERT.UE). As CSIRT têm competência para monitorizar incidentes a nível nacional, ativar mecanismos de alerta rápido, fazer comunicações e divulgar informações, intervir em caso de incidentes, analisar os riscos e

participar na Rede de CSIRT. Cabe-lhes também estabelecer relações de cooperação com o setor privado, promovendo a utilização de práticas comuns ou normalizadas relativas aos procedimentos de gestão de riscos e incidentes e aos sistemas de classificação de incidentes, de risco e de informações.

Cabe a cada Estado designar as autoridades nacionais competentes, os pontos de contacto únicos (com funções de ligação para assegurar a cooperação transfronteiriça) e as CSIRT, ainda que os Estados Membros possam solicitar a cooperação da ENISA para desenvolver as suas CSIRT. Cada Estado Membro deverá ainda adotar uma estratégia nacional de segurança das redes e informação, promovendo a cooperação entre o setor público e o setor privado, identificando medidas de preparação, resposta e recuperação, promovendo programas de ensino, sensibilização, formação e investigação em matérias de cibersegurança.

Para além disso, cada Estado Membro deverá assegurar que os operadores de serviços essenciais e os prestadores de serviços digitais adotam as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos e evitar incidentes que afetem a segurança das redes e dos sistemas de informação. A Diretiva SRI estabelece que os Estados Membros deverão incentivar, em pleno respeito pelo princípio da neutralidade tecnológica, a utilização de normas e especificações europeias internacionalmente aceites, aplicáveis à segurança das redes e sistemas de informação, podendo a ENISA formular recomendações e orientações sobre os domínios técnicos a considerar.

Os Estados Membros devem garantir que os prestadores de serviços essenciais e os prestadores de serviços digitais notificam as autoridades competentes ou as CSIRT, sem demora injustificada, dos incidentes com impacto importante na continuidade dos serviços por si prestados. As entidades que não tenham sido identificadas como operadores de serviços essenciais ou prestadores de serviços digitais são, de todo o modo, convidadas a participar no esforço coletivo com vista à segurança das redes e sistemas de informação, através da figura da notificação voluntária dos incidentes com impacto importante na continuidade dos serviços prestados.

Está já em preparação uma revisão da Diretiva SRI, anunciada na comunicação conjunta da Comissão Europeia e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, como parte da Estratégia de cibersegurança da UE para a década digital [JOIN(2020) 18]. Segundo o documento, a revisão é necessária para "diminuir as incoerências no conjunto do mercado único, mediante um alinhamento dos requisitos relativos ao âmbito de aplicação, à segurança e à comunicação de incidentes, da supervisão e aplicação ao nível nacional e das atribuições das autoridades competentes". Para assegurar uma abordagem coerente, a proposta de diretiva revista [COM(2020) 823] foi apresentada juntamente com uma proposta de revisão da legislação em matéria de resiliência das infraestruturas críticas [COM(2020) 829].

A Diretiva SRI foi transposta para a ordem jurídica portuguesa pela Lei n.º 46/2018, de 13 de agosto, que definiu a estrutura nacional de segurança do ciberespaço, fixou deveres de notificação de incidentes e estabeleceu um regime sancionatório, nomeadamente, para o incumprimento dos deveres de notificação.

A estrutura de segurança do ciberespaço integra o Conselho Superior de Segurança do Ciberespaço, como órgão específico de consulta do Primeiro-Ministro para estas matérias; o CNCS, como Autoridade Nacional de Cibersegurança; a Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT); os operadores de serviços essenciais; e os prestadores de serviços digitais.

A Lei n.º 46/2018 elencou os setores, subsetores e tipos de entidades dos operadores de serviços essenciais – a partir das categorias fixadas pela Diretiva SRI – e incumbiu o CNCS de identificar os operadores de serviços essenciais, com atualizações anuais. Impôs também que as entidades do setor das infraestruturas digitais comuniquem de imediato ao CNCS o exercício da respetiva atividade (artigo 29.º).

Nos termos dos artigos 21.º e seguintes, o CNCS tem competências de fiscalização, de instrução dos processos de contraordenação e de aplicação de sanções em caso de incumprimento

- da obrigação de implementar requisitos de segurança;
- de instruções de cibersegurança emitidas pelo CNCS;
- da obrigação de notificar o CNCS da ocorrência de incidentes;
- da obrigação de notificar o CNCS do exercício de atividade no setor das infraestruturas digitais;
- da obrigação de notificar o CNCS da identificação como prestador de serviços digitais.

A Lei n.º 46/2018 definiu uma obrigação genérica de que a Administração Pública e os operadores de infraestruturas críticas cumpram as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, para evitar incidentes e para reduzir ao mínimo o seu impacto quando ocorram (artigo 14.º). Semelhante obrigação genérica é definida para os operadores de serviços essenciais pelo artigo 16.º. A definição dos requisitos de segurança das redes e dos sistemas de informação foi remetida para legislação própria (artigo 12.º) e o mesmo aconteceu para a definição dos requisitos de notificação de incidentes (artigo 13.º). A legislação própria a que aludem estas disposições ainda não foi adotada, pelo que o regime instituído pela Lei n.º 46/2018 permanece parcialmente inaplicável.

A definição dos requisitos de segurança aplicáveis aos prestadores de serviços digitais foi remetida, pelo artigo 18.º, para o Regulamento de Execução (UE) 2018/151 da Comissão, de 30 de janeiro, que estabelece normas de execução da Diretiva (UE) 2016/1148 no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação, bem como à especificação pormenorizada dos parâmetros para determinar se o impacto de um incidente é substancial.

O Decreto-Lei n.º 43/2020, de 21 de julho, estabeleceu o Sistema Nacional de Planeamento Civil de Emergência e, dentro deste, o Conselho Nacional de Planeamento Civil de Emergência, para atuar sob dependência direta do Primeiro-Ministro (ou, por delegação deste, do membro do Governo responsável pela área da Administração Interna), com competência para identificar, designar e promover a resiliência e a proteção das infraestruturas críticas situadas em território nacional [6.º, alínea *l*)].

DESTAQUES

O aumento das ligações (e da dependência) entre as infraestruturas críticas dos Estados e as redes e os sistemas e serviços de informação trouxe novos riscos e vulnerabilidades para a segurança dos Estados, motivando a adoção de medidas destinadas a assegurar a proteção das redes e infraestruturas.

A Diretiva 2008/114/CE, de 18 de dezembro, estabeleceu um procedimento de identificação e designação das Infraestruturas Críticas Europeias (ICE) e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção.

O Decreto-Lei n.º 62/2011, de 9 de maio, que transpôs a Diretiva 2008/114/CE, estabeleceu os procedimentos de identificação e de proteção das infraestruturas essenciais nos sectores da energia e transportes.

A Diretiva 2016/1148, de 6 de julho (Diretiva SRI), veio promover uma cultura de gestão dos riscos, com partilha de responsabilidades entre entidades públicas e privadas, e consagrar um *standard* mínimo comum de segurança para operadores de serviços essenciais e prestadores de serviços digitais.

Para além dos setores da energia e dos transportes, a Diretiva SRI identifica como operadores de serviços essenciais as entidades públicas ou privadas do setor bancário e infraestruturas do mercado financeiro, do setor da saúde, do setor do fornecimento e distribuição de água potável e as infraestruturas digitais.

Para a concreta identificação dos operadores de serviços essenciais, a Diretiva SRI elenca um conjunto de critérios que se prendem com a atividade social e/ou económica crucial desenvolvida, com a dependência das redes e sistemas de informação para a prestação desse serviço, e com os efeitos perturbadores na prestação desse serviço que um incidente possa causar.

Para alcançar um elevado nível comum de segurança das SRI em todo o território da União, a Diretiva cria um grupo de cooperação e uma rede de equipas de resposta a incidentes de segurança informática (Rede Europeia de CSIRT).

A Diretiva SRI foi transposta para a ordem jurídica portuguesa pela Lei n.º 46/2018, de 13 de agosto, que estabeleceu o regime jurídico da segurança do ciberespaço, fixou deveres de notificação de incidentes e estabeleceu um regime sancionatório para o incumprimento, nomeadamente, dos deveres de notificação.

A Lei n.º 46/2018, de 13 de agosto, remeteu para legislação complementar a definição dos requisitos de segurança das redes e dos sistemas de informação e a definição dos requisitos de notificação de incidentes. Esta legislação ainda não foi adotada, pelo que o regime instituído pela Lei n.º 46/2018 irá evoluir significativamente num futuro próximo.

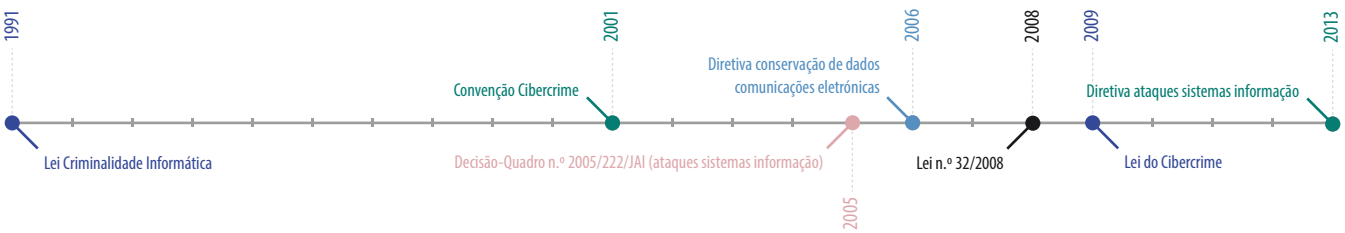
2.3.2. Cibercrime e prova digital

A lei de referência em Portugal sobre o cibercrime é a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), que resulta da transposição para a ordem jurídica interna da Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e da adaptação da ordem jurídica portuguesa à Convenção do Conselho da Europa sobre o Cibercrime, de 2001, que Portugal assinou em 2001 e ratificou em 2009.

O primeiro destes instrumentos, a Decisão-Quadro, entretanto substituída pela Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação, procurou aproximar as ordens jurídicas nacionais dos Estados Membros ao estabelecer um *standard* mínimo de incriminação de determinados comportamentos lesivos dos sistemas de informação. O objetivo último desta aproximação não era simplesmente o de alcançar uma harmonização normativa mínima, mas também criar as condições necessárias para uma cooperação mais estreita entre as autoridades judiciárias, policiais e outras entidades competentes dos diversos Estados Membros. Diante de um tipo de criminalidade complexo, organizado e essencialmente transnacional como é o cibercrime, a investigação e repressão não podem confinar-se às fronteiras físicas de um Estado, tendo de haver necessariamente uma resposta concertada e articulada entre os vários Estados afetados. Por intermédio da Decisão-Quadro de 2005, a União Europeia impôs aos Estados Membros que previssem na sua legislação, pelo menos, os crimes de acesso ilegal aos sistemas de informação, interferência ilegal no sistema e interferência ilegal nos dados, crimes pelos quais deveriam ser responsabilizados quer os seus autores imediatos, mediatos ou coautores, quer os seus instigadores ou cúmplices.

A Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001, sob a égide do Conselho da Europa, foi um pouco mais longe do que a Decisão-Quadro, tanto no seu âmbito de aplicação territorial (já que se aplica a um maior número de Estados), como no seu alcance normativo. Do ponto de vista do Direito Penal material, a Convenção contempla crimes como os de acesso ilícito, interceção ilícita, dano provocado nos dados, sabotagem informática, utilização indevida de dispositivos, falsificação informática, burla informática, pornografia infantil, e ainda crimes contra direitos de autor e direitos conexos. De um ponto de vista processual, que a Decisão-Quadro não contempla, a Convenção do Conselho da Europa prevê um conjunto de medidas processuais que deverão estar ao dispor das autoridades nacionais para a investigação dos crimes mencionados na Convenção, de outros crimes que hajam sido cometidos por meio de um sistema informático, ou quando, independentemente do modo de execução, seja necessário obter prova eletrónica relativa a uma infração penal. Medidas que vão desde a conservação expedita de dados informáticos armazenados até a injunções para a sua comunicação, passando ainda pela busca e apreensão de dados informáticos armazenados e a recolha, em tempo real, de dados de tráfego e interceção de dados de conteúdo.

A Lei do Cibercrime constitui a referência legislativa nacional em matéria de cibercrime, quer porque aí se concentra a incriminação de grande parte dos cibercrimes, quer ainda por prever meios de obtenção de prova digital, de especial relevância para a investigação da cibercriminalidade.



Relativamente ao Direito substantivo, temos previstos na Lei do Cibercrime os crimes de falsidade informática (artigo 3.º), dano relativo a programas ou outros dados informáticos (artigo 4.º), sabotagem informática (artigo 5.º), acesso ilegítimo (artigo 6.º), interceção ilegítima (artigo 7.º) e reprodução ilegítima de programa protegido (artigo 8.º).

Retira-se da leitura destes artigos que o legislador português, na senda aliás do que acontece ao nível europeu, enveredou por um caminho tecnologicamente neutro aquando da redação dos tipos legais de crime, de modo a "resistir ao desafio da temporalidade das tecnologias" (Freitas & Novais, 2018) e a abarcar toda a amplitude de novas realidades sociotecnológicas. Isso fica exemplarmente demonstrado com a evolução normativa de conceitos como "sistema informático" e "rede informática", que, na Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto), revogada pela Lei do Cibercrime, eram definidos autonomamente e de um modo muito mais simples. "Sistema informático" era definido como "conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados", enquanto "rede informática" era definida como "conjunto de dois ou mais computadores interconectados". Com a Lei do Cibercrime, os dois conceitos subsumem-se a um só, o de "sistema informático", definido agora como "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção" [artigo 2.º, alínea *a)*, da Lei do Cibercrime].

A simplicidade definitória empregada na Lei da Criminalidade Informática explica-se, em parte, pela circunstância de, no momento da sua entrada em vigor, muitas das tecnologias que hoje temos por adquiridas estarem no início da sua conceção ou difusão. Os telemóveis haviam sido lançados no mercado há menos de dez anos (Motorola DynaTAC 8000X, em 1983) e o nascimento, na Europa, da *World Wide Web* foi praticamente contemporâneo da lei (1989). Em 2009, era já evidente que um sistema informático não se identificava exclusivamente com computadores e periféricos.

Para além de um Direito substantivo atualizado, 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 (artigo 12.º), revelação expedita de dados de tráfego (artigo 13.º), injunção para apresentação ou concessão do acesso a dados (artigo 14.º), pesquisa de dados informáticos (artigo 15.º), apreensão de dados informáticos (artigo 16.º), apreensão de correio eletrónico e registos de comunicações de natureza semelhante (artigo 17.º), interceção de comunicações (artigo 18.º) e ações encobertas (artigo 19.º). Com a 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 Lei do Cibercrime, 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 Lei do Cibercrime.

O legislador português decidiu tratar a prova digital na Lei do Cibercrime, mas manteve inalteradas as soluções jurídicas já previstas no Código de Processo Penal, que, pelo menos parcialmente, se debruçam sobre aspetos

idênticos. Esta opção não segue o exemplo de ordenamentos jurídicos próximos, como o espanhol (*Ley de Enjuiciamiento Criminal*), o italiano (*Codice di Procedura Penale*) ou o alemão (*Strafprozeßordnung*), que constituem, noutros casos, referências relevantes para o legislador nacional, e tem sido criticada na doutrina, para além de suscitar dúvidas na prática judicial, como será analisado na secção deste relatório dedicada à aplicação do quadro legal.

A Lei do Cibercrime inclui ainda disposições sobre cooperação internacional. Os artigos 20.º a 26.º preveem o estabelecimento de um ponto de contacto permanente (24/7) na Polícia Judiciária, com a finalidade de cooperação com as autoridades estrangeiras competentes. Esta cooperação inclui a prestação de aconselhamento técnico a outros pontos de contacto; a preservação expedita de dados nos casos de urgência ou perigo na demora; a recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora; e a localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora. Em determinados casos, são impostas limitações ao alcance da assistência do ponto de contacto português com outros pontos de contacto estrangeiros. Veja-se, a título de exemplo, o pedido de preservação ou de revelação expeditas de dados informáticos armazenados em sistema informático. Embora possam ser realizados quanto a crimes previstos na Lei do Cibercrime ou de outros crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, pode acontecer que, à luz do Direito português, estes digam respeito a infração de natureza política ou infração conexa. Se assim for, o pedido de colaboração é recusado. O mesmo acontece quando o pedido atente contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos, e quando o Estado terceiro requisitante não ofereça garantias adequadas de proteção dos dados pessoais. Também quando se queira recorrer ao acesso a dados informáticos ou à interceção de comunicações em cooperação internacional, é necessário verificar se se trata de uma situação em que isso será viável num caso nacional semelhante. Estas limitações não beliscam, no entanto, a importância e a efetividade da cooperação internacional em matéria de cibercriminalidade e prova digital, imprescindível, de resto, na investigação de um tipo de criminalidade que recorrentemente extravasa fronteiras.

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. A compatibilidade do regime jurídico fixado pela Lei n.º 32/2008 com o Direito da União Europeia tem sido discutida na doutrina portuguesa, em face das pronúncias do Tribunal de Justiça da União Europeia (TJUE) sobre soluções legislativas congéneres de outros Estados Membros, um ponto desenvolvido na secção relativa à aplicação do quadro legal.

Igualmente controversa é a concretização da transposição da Diretiva 2013/40/UE, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação, que substituiu a Decisão-Quadro 2005/222/JAI. Em 10 de outubro de 2019, a Comissão Europeia enviou uma carta de notificação a Portugal em virtude da "incorreta implementação de certas normas da Diretiva relativa a ataques contra os sistemas de informação"[14]. Não restam dúvidas de que a maioria das soluções previstas na Diretiva já constava da Lei do Cibercrime, operando como que uma transposição por antecipação, mas o mesmo não se pode sustentar quanto às sanções aplicáveis [artigo 9.º, n.º 4, alínea *a)*, da Diretiva 2013/40/UE] e a determinados procedimentos de cooperação internacional previstos no artigo 13.º da referida Diretiva. Teremos de aguardar a conclusão do procedimento formal de infração iniciado pela Comissão Europeia, com o número 20192242, que ainda está em curso.

É também expectável que, num futuro próximo, surja o segundo protocolo adicional à Convenção de Budapeste a versar sobre o acesso a prova digital pelas autoridades judiciárias e policiais[15]. O prazo para conclusão da redação deste novo tratado, que foi originariamente o de dezembro de 2019, foi prorrogado para maio de 2021.

14 Cf. https://ec.europa.eu/commission/presscorner/detail/en/INF_19_5950 [12.12.2020].

15 O andamento dos trabalhos preparatórios podem ser acompanhado em https://www.coe.int/en/web/cybercrime/t-cy-drafting-group [12.12.2020].

DESTAQUES

A lei de referência em Portugal sobre o cibercrime é a Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), que resulta da transposição para a ordem jurídica interna da Decisão-Quadro 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e da adaptação da ordem jurídica portuguesa à Convenção do Conselho da Europa sobre o Cibercrime, de 2001, que Portugal assinou em 2001 e ratificou em 2009.

Para além de tipos legais de crime atualizados face à Lei da Criminalidade Informática, de 1991, a Lei do Cibercrime introduziu, no ordenamento jurídico português, um conjunto de disposições processuais relativas à prova digital.

A interpretação e a aplicação da Lei do Cibercrime e demais normas aplicáveis em matéria de cibercrime e prova digital têm suscitado dúvidas na jurisprudência e na doutrina portuguesas, sobretudo no que respeita à articulação entre a Lei do Cibercrime e o Código de Processo Penal, mas também quanto à compatibilidade do regime jurídico relativo à conservação de dados gerados ou tratados no contexto de comunicações eletrónicas (Lei n.º 32/2008, de 17 de julho) com o Direito da União Europeia.

Aguarda-se a conclusão do procedimento formal de infração movido pela Comissão Europeia contra Portugal relativo à transposição da Diretiva 2013/40/UE, de 12 de agosto, relativa a ataques contra os sistemas de informação, que substituiu a Decisão-Quadro 2005/222/JAI.

2.3.3. Proteção de dados pessoais

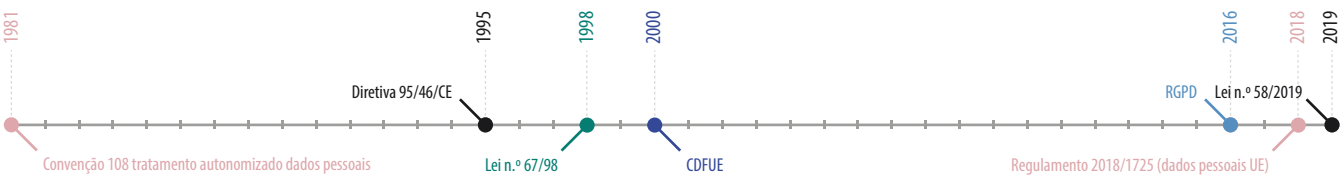
A proteção de dados pessoais tem uma longa tradição no Direito internacional dos direitos humanos, enquanto dimensão da proteção da intimidade da vida privada e familiar, consagrada na Declaração Universal dos Direitos Humanos (artigo 12.º) e no Pacto Internacional sobre os Direitos Civis e Políticos (artigo 17.º), por exemplo. Aí se prevê que ninguém "sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação", e que todos têm direito à proteção da lei contra tais intromissões ou ataques. A nível regional, no âmbito do Conselho da Europa, a proteção de dados pessoais também tem sido considerada abrangida pelo direito à intimidade da vida privada e familiar, previsto no artigo 8.º da Convenção Europeia dos Direitos Humanos (CEDH), como resulta, entre outros, dos acórdãos do Tribunal Europeu dos Direitos Humanos (TEDH) *Leander contra a Suécia*, de 1987, *Gaskin contra Reino Unido*, de 1989, e *Amann contra Suíça*, de 2000[16]. O Conselho da Europa adotou, para além disso, um tratado específico sobre proteção de dados – a Convenção 108, de 28 de janeiro de 1981, relativa à proteção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais, que foi justificada pela necessidade de ter em consideração "o fluxo crescente, através das fronteiras, de dados de caráter pessoal suscetíveis de tratamento automatizado" e de, ao mesmo tempo, promover os valores fundamentais do respeito pela vida privada e a livre circulação de informação entre os povos.

Na União Europeia, a proteção de dados pessoais constitui um valor ancilar e um direito fundamental. O artigo 16.º do Tratado sobre o Funcionamento da União Europeia determina que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito e incumbe o Parlamento Europeu e o Conselho de adotarem normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. Esta importância foi reforçada pela **consagração do direito à proteção de dados pessoais, como direito autónomo do direito à intimidade da vida privada e familiar, no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia** (CDFUE), de 2000. A primeira Diretiva sobre a matéria fora adotada em 1995 – Diretiva 95/46/CE, de 24 de outubro – e visara promover uma tendencial harmonização da proteção de dados pessoais em todo o território da União e no contexto de cada um dos seus Estados Membros. Esta Diretiva foi transposta para a ordem jurídica portuguesa pela Lei n.º 67/98, de 26 de outubro.

A necessidade de encontrar **soluções que assegurassem a proteção de dados pessoais e, simultaneamente, viabilizassem a sua circulação segundo padrões elevados de proteção** foi assumida pela Comissão Europeia, em 2015, na Comunicação intitulada "Estratégia para um Mercado Único Digital na Europa" [COM(2015) 192 final], onde se constatava que a economia mundial estava rapidamente a tornar-se digital e que o setor das TIC tinha deixado de ser um setor específico para a ser a base de todos os sistemas económicos modernos, o que abria inúmeras oportunidades para a inovação, o crescimento e o emprego.

Na sequência desta Comunicação, a matéria da proteção de dados pessoais foi objeto de nova intervenção legislativa, com a adoção do Regulamento (UE) 679/2016, relativo à proteção das pessoas singulares no que diz respeito ao

16 *Leander contra Suécia* (queixa n.º 9248/81), de 26 de março de 1987; *Gaskin contra Reino Unido* (queixa n.º 10454/83), de 7 de julho de 1989; *Amann contra Suíça* (queixa n.º 27798/95), de 16 de fevereiro de 2000.



tratamento de dados pessoais e à livre circulação desses dados, comummente designado Regulamento Geral de Proteção de Dados (RGPD). Segundo o texto preambular do Regulamento, os objetivos e os princípios da Diretiva 95/46/CE continuavam a ser válidos, mas a Diretiva não conseguira evitar a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistiam riscos significativos para a proteção das pessoas singulares, nomeadamente no que dizia respeito às atividades por via eletrónica. As diferenças de nível de proteção, nomeadamente no que dizia respeito ao tratamento dos dados nos Estados Membros, poderiam impedir a livre circulação de dados pessoais na União, criando obstáculos ao exercício das atividades económicas, com distorção da concorrência, e impedindo as autoridades de cumprir as obrigações que decorrem do Direito da União. **O RGPD veio assegurar às pessoas singulares de todos os Estados Membros o mesmo nível de direitos suscetíveis de proteção judicial, impondo obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes e um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados Membros**.

As preocupações com a cibersegurança têm estado sempre presentes na regulação da proteção dos dados pessoais. A Convenção 108 do Conselho da Europa estabeleceu, no seu artigo 7.º, sob a epígrafe "segurança dos dados", que, para a proteção dos dados de caráter pessoal registados em ficheiros automatizados devem ser tomadas medida de segurança apropriadas contra a destruição, acidental ou não autorizada, e a perda acidental e também contra o acesso, a modificação ou a difusão não autorizados. A evolução tecnológica entretanto verificada determinou a emergência de soluções mais adequadas ao tratamento de dados pessoais, quer em termos físicos, quer em termos tecnológicos e digitais. No RGPD, a preocupação com a cibersegurança como princípio geral subjacente ao tratamento dos dados pessoais ficou patente na exigência de que os dados pessoais sejam tratados "de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas ('integridade e confidencialidade')" [artigo 5.º, n.º 1, alínea *f*)]. Cabe ao responsável pelo tratamento e ao subcontratante a aplicação de medidas técnicas e organizativas adequadas a assegurar um nível de segurança ajustado ao risco, o que pode requerer, nomeadamente:

- a pseudonimização e a cifragem dos dados
- a demonstração de capacidade para assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas e dos serviços de tratamento
- a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e
- a implementação de um processo para testar, apreciar e avaliar regularmente a eficácia das medidas adotadas (artigo 32.º, n.º 1).

Sempre que se tome conhecimento de uma violação, cabe ao responsável pelo tratamento comunicá-la à autoridade de controlo (artigo 33.º do RGPD) e ao titular dos dados, quando a violação implicar risco elevado para os direitos e liberdades de pessoas singulares (artigo 34.º do RGPD).

O RGPD é diretamente aplicável na ordem jurídica portuguesa, mas, para assegurar a sua execução em Portugal, o legislador português adotou a Lei n.º 58/2019, de 8 de agosto, designada Lei da Proteção de Dados Pessoais, que assume uma função instrumental de concretização e operacionalização das disposições do RGPD. O artigo 11.º da Lei n.º 58/2019 especifica as funções do Encarregado de proteção de dados, sublinhando que lhe cabe sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança. Atenta a necessidade de promover um tratamento de dados de saúde e de dados genéticos de forma particularmente segura, o artigo 29.º determina a necessidade de tais dados serem tratados por um profissional obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação. Concretizando o regime sancionatório decorrente do artigo 83.º do RGPD [que deve ser lido à luz do seu artigo 58.º, n.º 2, alínea *i)*], o artigo 38.º da Lei n.º 58/2019 estabelece que se configurará como contraordenação grave a violação das regras de segurança previstas no artigo 32.º do RGPD. O artigo 47.º da Lei n.º 58/2019 estabelece dois tipos legais de crime: (a) o crime de acesso indevido, imputável a quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais; e (b) o crime de desvio de dados, imputável a quem, copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento, independentemente da finalidade prosseguida. Em ambos os casos, a pena pode ser agravada para o dobro nos seus limites quando o acesso tenha sido conseguido através da violação de regras técnicas de segurança.

DESTAQUES

A proteção de dados pessoais tem uma longa tradição no Direito internacional dos direitos humanos, enquanto dimensão da proteção da intimidade da vida privada e familiar. No Direito da União Europeia, a proteção de dados pessoais constitui um direito fundamental autónomo, consagrado no artigo 8.º da CDFUE.

O Regulamento Geral sobre a Proteção de Dados, adotado em 2016, veio assegurar às pessoas singulares de todos os Estados Membros o mesmo nível de direitos suscetíveis de proteção judicial, impondo obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes e um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados Membros.

No RGPD, a preocupação com a cibersegurança está patente na exigência de que os dados pessoais sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

A Lei n.º 58/2019, de 8 de agosto (Lei da Proteção de Dados Pessoais), que assegura a execução do RGPD em Portugal, prevê o regime aplicável ao responsável pelo tratamento dos dados e especifica as funções do encarregado de proteção de dados. Também estabelece os regimes de proteção administrativa e judicial do titular de dados pessoais e os regimes de responsabilidade civil e sancionatória, contraordenacional e penal, para a violação das disposições do Regulamento.

2.3.4. Comunicações eletrónicas

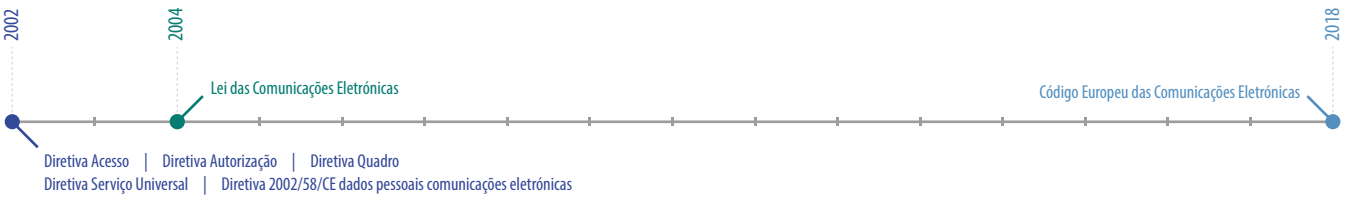
A União Europeia começou a dar maior atenção à regulação jurídica das comunicações eletrónicas a partir de 2002, altura em que foi adotado um pacote legislativo composto pelos seguintes atos:

- 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 2002/21/CE, relativa a um quadro regulamentar comum para as 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.

Ao tempo, a preocupação estava em **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 um conjunto de regras mínimas, nomeadamente, no que dizia respeito às relações entre as autoridades reguladoras nacionais e os prestadores desses serviços e às relações estabelecidas entre estes últimos e os consumidores.

A Diretiva 2002/22/CE visou assegurar aos consumidores um serviço universal no âmbito das comunicações eletrónicas, proporcionando a disponibilidade em toda a União Europeia de serviços acessíveis ao público, de boa qualidade, através de uma concorrência e de uma possibilidade de escolha efetivas, atendendo às situações em que as necessidades dos utilizadores finais não fossem convenientemente satisfeitas pelo mercado. Para o efeito, a Diretiva 2002/22/CE estabelecia um conjunto mínimo de serviços de qualidade especificada a que todos os utilizadores deveriam ter acesso, a um preço razoável e sem que a concorrência entre os prestadores dos serviços sofresse distorções. Naquela altura, tais requisitos mínimos exigiram que os vários Estados Membros assegurassem, no quadro dos serviços prestados no âmbito das comunicações eletrónicas:

- a oferta de acesso à rede telefónica em local fixo, permitindo a realização de chamadas telefónicas e viabilizando o acesso à Internet;
- a disponibilização de listas telefónicas (impressas e/ou em suporte eletrónico), sujeitas a regular atualização; e
- a colocação de postos públicos (i.e., de telefone acessível ao público em geral, cuja utilização pudesse ser paga com moedas e/ou cartões de pré-pagamento, incluindo cartões a utilizar com códigos de marcação).



Estes serviços deveriam caracterizar-se por uma acessibilidade das tarifas aplicadas, mediante controlo prévio pelas autoridades reguladoras nacionais. No contexto português, a Autoridade Nacional de Comunicações (ANACOM) foi identificada como a autoridade reguladora nacional e ficou responsável pelo seu desenvolvimento e pelo acompanhamento do mercado. O Estado português, tentando dar cumprimento às obrigações decorrentes deste pacote legislativo europeu, adotou a Lei n.º 5/2004, de 10 de fevereiro, designada como Lei das Comunicações Eletrónicas.

A partir da adoção do pacote legislativo de 2002, **verificou-se uma europeização da regulação das comunicações eletrónicas, pautada por preocupações de regulação social, associadas ao estabelecimento de um serviço universal a observar em todos os Estados Membros e que pressupunha, numa perspetiva de ubiquidade geográfica, a disponibilização de serviços considerados essenciais, tentando mitigar as assimetrias entre populações**. Reconhece-se, no entanto, que o conceito de serviço universal deve ser dinâmico, para poder adequar-se aos avanços tecnológicos, ao desenvolvimento do mercado e às modificações na procura dos serviços por parte dos utilizadores. Uma nova Diretiva sobre comunicações eletrónicas foi adotada em 2009 – a Diretiva 2009/136/CE, que, entre outros atos normativos, alterou a Diretiva 2002/22/CE, de forma a promover uma **maior inclusão dos consumidores, sublinhando a necessidade de facultar serviços de qualidade a utilizadores com necessidades especiais em situações de equivalência relativamente aos demais consumidores**.

Atento o impacto da globalização nas comunicações eletrónicas, viabilizadas numa escala planetária, a Comissão Europeia fez, em 2016, um levantamento das necessidades de reforma legislativa em matéria de comunicações eletrónicas, que sintetizou na sua Comunicação "Conectividade para um Mercado Único Digital Concorrencial – rumo a uma sociedade europeia a Gigabits" [COM(2016) 05879]. A Comissão observou como a transformação digital vinha a repercutir-se sobre o setor das comunicações eletrónicas desde 2009, **com mudanças nos padrões e nas necessidades de consumo resultantes da transição da telefonia vocal para o acesso fixo e móvel à Internet através de uma série de dispositivos** (*smartphones*, *tablets*, computadores e televisões), concluindo ser **necessário um desempenho mais apurado das redes através das quais tais serviços eram prestados**. Segundo a Comissão, o potencial associado à transformação digital só poderia ser aproveitado se o espaço da União Europeia fosse capaz de assegurar a implantação e a adoção generalizadas de redes com capacidade muito elevada, quer em zonas urbanas, quer em zonas rurais. Assim sendo, a Comissão definiu três objetivos estratégicos a atingir até 2025:

- no domínio do crescimento e emprego na Europa, implementar uma conectividade a *gigabits* nos locais que promovem o desenvolvimento socioeconómico;
- no domínio da competitividade europeia, promover a cobertura 5G em todas as zonas urbanas e grandes vias de transporte terrestre; e
- no domínio da coesão europeia, promover o acesso de todos os agregados familiares europeus a uma ligação de Internet com uma velocidade mínima de 100Mbps.

Estes objetivos foram tidos em consideração na adoção, a 11 de dezembro de 2018, da Diretiva (UE) 2018/1972, que estabelece o Código Europeu das Comunicações Eletrónicas.

Atentos os objetivos de potenciação da conectividade na União Europeia, a preocupação com a cibersegurança tem sido constante. **O estabelecimento das infraestruturas de conectividade exige a fiabilidade das redes, sob pena de o avanço tecnológico não se revelar tão apetecível aos prestadores de serviços associados às comunicações eletrónicas e aos consumidores de tais serviços.** Afinal, a Internet viabilizou o surgimento de serviços de comunicações *online*, com grandes benefícios para os utilizadores finais, mas **o mercado interno das comunicações eletrónicas só poderá prosperar se se assegurar "uma proteção adequada em domínios como a segurança"**. Estas preocupações são evidentes na Diretiva 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, respetivamente, e impedir ou minimizar o impacto dos incidentes de segurança, "tendo em conta os progressos técnicos mais recentes". As **medidas de segurança** deverão ter em conta, no mínimo, os seguintes aspetos:

- em matéria de **segurança das redes e instalações**, as medidas deverão observar padrões de segurança física e ambiental, de segurança no fornecimento, de controlo do acesso às redes e de integridade das redes;
- em matéria de **gestão de incidentes de segurança**, deverão ser adotados procedimentos de gestão que potenciem a capacidade de deteção de incidentes de segurança e a implementação de relatórios necessários à comunicação de incidentes de segurança;
- em matéria de **gestão da continuidade operacional**, deverá ser implementada uma estratégia vocacionada à continuidade do serviço e à adoção de planos de emergência, que determine as capacidades de recuperação em casos de desastres; e
- em matéria de **monitorização, auditorias e testes**, cabe implementar políticas de monitorização e de registo, processando os exercícios relativos aos planos de emergência, de realização de testes da rede e dos serviços, viabilizando a realização de avaliações de segurança e de controlo do cumprimento e do respeito por padrões normativos, nomeadamente de caráter internacional.

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, inclusivamente nos casos em que o incidente de segurança comunicado pelo fornecedor tenha resultado de vulnerabilidades conhecidas de *software* ou *hardware* para as quais o fabricante ou o programador tenham emitido correções.

Portugal está obrigado a transpor a Diretiva (UE) 2018/1972, que estabelece o Código Europeu das Comunicações

Eletrónicas, até ao dia 21 de dezembro de 2020. Para dar cumprimento a esta obrigação, o Governo criou um grupo de trabalho com a incumbência de proceder ao estudo e à análise da nova legislação das comunicações eletrónicas e de elaborar um anteprojeto legislativo de transposição do Código Europeu das Comunicações Eletrónicas, com inclusão e consolidação da demais legislação sectorial (Despacho n.º 303/2020, de 9 de janeiro). Em 31 de julho de 2020, a ANACOM aprovou, para envio à Assembleia da República e ao Secretário de Estado Adjunto e das Comunicações, um anteprojeto de diploma para transposição do Código Europeu das Comunicações Eletrónicas e o conjunto de propostas de alterações pontuais de outra legislação em vigor.

DESTAQUES

Na União Europeia, tem havido a preocupação em assegurar que todos os Estados Membros se dotem de redes e serviços de comunicações eletrónicas de boa qualidade, sendo as operações daí decorrentes sujeitas a competente regulação pelas autoridades reguladoras nacionais (no caso português, a ANACOM).

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" suficientemente dinâmico para se adequar aos desenvolvimentos no âmbito tecnológico e digital.

A transformação digital determinou a transição da telefonia vocal para o acesso à Internet, o que motivou a adoção da Diretiva (UE) 2018/1972 que estabelece o Código Europeu das Comunicações Eletrónicas.

O Código Europeu das Comunicações Eletrónicas visa assegurar a liberdade de oferta de serviços e redes de comunicações eletrónicas que observem um nível particularmente elevado de segurança.

Os padrões de segurança exigíveis são de segurança física e ambiental, de fornecimento, de controlo de acesso às redes e de integridade dessas redes; a adoção de procedimentos de gestão que permitam detetar e minimizar incidentes de segurança; uma capacidade de continuidade operacional e a implementação de políticas de monitorização, de auditoria e de condução de testes.

A Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas tem como prazo de transpoição pelo Estado português o dia 21 de dezembro de 2020.

2.3.5. Comércio eletrónico, pagamentos eletrónicos e identificação eletrónica

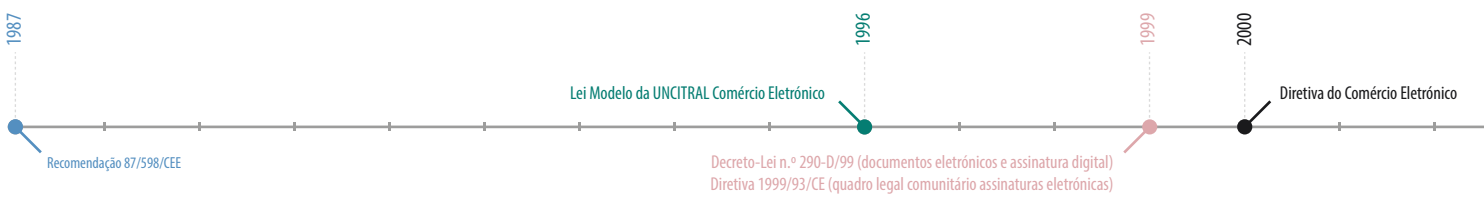
Toda a produção legislativa em matéria de comércio eletrónico, pagamentos eletrónicos e identificação eletrónica sofreu um impulso inicial e decisivo por parte da União Europeia. Em 1987, o Conselho das Comunidades Europeias instituiu o programa TEDIS (*Trade Electronic Data Interchange Systems*), relativo à transferência eletrónica de dados (EDI) nas áreas do comércio, da indústria e da administração (Decisão 87/499/CEE, de 5 de outubro), de que resultou, entre outras coisas, a preparação de um projeto de acordo-tipo EDI europeu, o que viria a ser concretizado com a Recomendação 94/820/CE da Comissão, de 19 de outubro, relativa aos aspetos jurídicos da transferência eletrónica de dados. Tratava-se na altura de definir um modelo que pudesse ser adotado pela indústria no sentido de acompanhar os desenvolvimentos e crescente utilização, na área empresarial, de novos instrumentos de contratação e pagamentos eletrónicos, nomeadamente com o incremento de utilização da EDI. Pretendia-se melhorar o quadro jurídico através de uma abordagem uniforme das questões jurídicas, aumentar a segurança jurídica para os parceiros comerciais e reduzir as incertezas surgidas com a EDI, bem como evitar a duplicação de trabalho para as empresas, dispensando-as de elaborar o seu próprio acordo de transferência.

O acordo-tipo EDI europeu espelha bem a necessidade de uma abordagem assente em diferentes especificações, a saber, uma especificação técnica, uma especificação de segurança e uma especificação jurídica. Relativamente às questões de segurança, havia já a preocupação de adotar um conjunto de procedimentos que assegurassem a confidencialidade das mensagens eletrónicas, tentando evitar a ocorrência de fraudes, pirataria, interceção ilícita e adulteração de mensagens ou qualquer acesso indevido aos sistemas informáticos. No acordo-tipo, era dada particular importância a questões como o aviso de receção de mensagens, o seu não repúdio, métodos e procedimentos de segurança (sobretudo no que se referia à integridade e confidencialidade das mensagens), responsabilidades pelos procedimentos de segurança e acordos entre as partes no tocante ao registo e arquivamento de mensagens. A utilização de técnicas de criptografia assimétrica era já encarada como um importante fator de segurança nas comunicações eletrónicas.

Para além de continuar a produzir recomendações e comunicações sobre estas matérias, a Comissão Europeia encetou, a partir de 1994, um conjunto de iniciativas legislativas que resultaram em Diretivas e Regulamentos sobre três eixos fundamentais: (a) identificação eletrónica, assinaturas eletrónicas e certificação eletrónica; (b) serviços da sociedade da informação, em particular o comércio eletrónico; e (c) pagamentos eletrónicos.

A Diretiva 1999/93/CE, de 13 de dezembro, relativa a um quadro legal comunitário para as **assinaturas eletrónicas**, foi adotada com o objetivo de facilitar a utilização das assinaturas eletrónicas e contribuir para o seu reconhecimento legal. A Diretiva trouxe alguns desenvolvimentos importantes, entre os quais a identificação de três tipos diferenciados de assinatura eletrónica (de acordo com níveis diferentes de segurança e confiança na sua utilização), a assunção clara de um princípio de neutralidade tecnológica e a eliminação da obrigatoriedade de sujeição a autorização administrativa para o exercício da atividade dos prestadores de serviços de certificação.

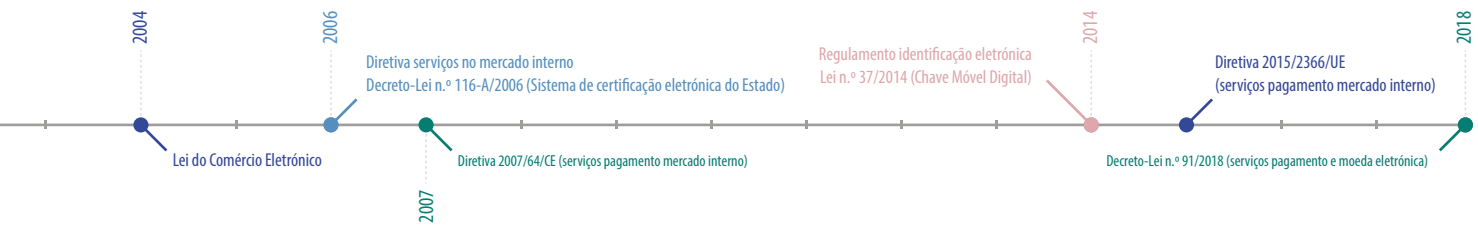
Este normativo teve um profundo impacto na ordem jurídica portuguesa. O Decreto-Lei n.º 290-D/1999, de 2 de agosto, que aprovou o regime jurídico dos documentos eletrónicos e da assinatura digital, dando o primeiro passo no sentido da consagração legal das assinaturas eletrónicas em Portugal, acolheu expressamente as soluções



constantes da proposta de diretiva avançada pela Comissão Europeia. Com a transposição da Diretiva 1999/93/CE, pelo Decreto-Lei n.º 62/2003, de 3 de abril, o Decreto-Lei n.º 290-D/1999 passou a adotar uma terminologia tecnologicamente neutra e a usar o conceito mais amplo de assinatura eletrónica, enquanto resultado de um processamento eletrónico de dados suscetível de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico. Quanto às entidades certificadoras, a lei portuguesa manteve a possibilidade (ou ónus) de as empresas certificadoras, emitentes de certificados de assinatura eletrónica qualificada, solicitarem a sua credenciação junto da entidade credenciadora, conferindo-se às assinaturas baseadas em tais certificados a força probatória equivalente a assinatura manuscrita. Este regime, que se pautava por uma grande exigência em termos de fiabilidade e controlo do processo de emissão e certificação de assinaturas eletrónicas, pecava por criar um regime de desigualdade entre assinaturas eletrónicas qualificadas. Para além disso, verificou-se um vazio legal que impediu, durante alguns anos, a emissão de certificados qualificados nos termos então previstos, porque o Sistema de Certificação Eletrónica do Estado só viria a ser criado em 2006, pelo Decreto-Lei n.º 116-A/2006, de 16 de junho, que designou a Autoridade Nacional de Segurança como autoridade credenciadora nacional.

Na sequência da criação do Sistema de Certificação Eletrónica do Estado, o Decreto-Lei n.º 88/2009, de 9 de abril, veio harmonizar o regime dos documentos eletrónicos e da assinatura eletrónica com a necessidade de utilização de certificados qualificados por entidades públicas, introduzindo ao mesmo tempo um regime sancionatório mais rigoroso com efeitos preventivos e persuasivos relativamente ao (in)cumprimento das normas legais pelos operadores que atuam no mercado da certificação. Abriu-se ainda a possibilidade de emissão de certificados para entidades certificadoras atuando fora do Sistema de Certificação Eletrónica do Estado, de modo a assegurar o reconhecimento internacional dos respetivos certificados, bem como a interoperabilidade entre as diferentes estruturas de chaves públicas a nível europeu, assim se assegurando uma menor desigualdade entre os operadores. No entanto, o regime português continuou a estabelecer, até à entrada em vigor do Regulamento (UE) 910/2014, de 23 de julho, um regime de desigualdade entre os operadores que emitiam certificados qualificados e os operadores credenciados (pela Entidade de Certificação Eletrónica do Estado) que também emitiam certificados qualificados, mas que podiam assegurar um valor probatório diferente (valor equivalente ao de assinatura manuscrita).

A necessidade de assegurar a interoperabilidade entre os produtos de assinatura eletrónica e os serviços de certificação eletrónica a nível europeu, muitas vezes inviabilizada por força de regimes diferenciados nos vários Estados Membros, e a constatação de avanços tecnológicos que permitiam oferecer um conjunto de novos serviços no que concerne à identificação eletrónica e aos serviços de confiança para as transações eletrónicas, levaram o legislador europeu a uma profunda revisão do quadro jurídico nesta matéria, através do Regulamento (UE) 910/2014, de 23 de julho, também conhecido como Regulamento eIDAS (*Electronic Identification, Authentication and Trust Services*). Este Regulamento veio colocar a tónica nas questões da identificação eletrónica (englobando os tradicionais métodos de autenticação eletrónica e os métodos de assinatura eletrónica) e da criação de um quadro legal de confiança na prestação de serviços e nas transações eletrónicas no mercado interno.



O Regulamento eIDAS – diretamente aplicável – revogou a Diretiva 1999/93/CE, com o que contribuiu para criar um quadro normativo mais uniforme entre todos os Estados Membros e para garantir a necessária interoperabilidade na prestação dos serviços. Por outro lado, manteve o conceito amplo e tecnologicamente neutro de assinatura eletrónica, abrindo caminho para uma possível utilização de novas tecnologias de assinatura, como será o caso das assinaturas dinâmicas, integrando novos desenvolvimentos das tecnologias biométricas comportamentais com os requisitos de segurança das assinaturas digitais. A expressa e clara distinção entre "autenticação" e "assinatura" abriu também o espaço à utilização de novos métodos de autenticação, como é o caso, em Portugal, das Chaves Móveis Digitais (previstas na Lei n.º 37/2014, de 26 de junho)[17], utilizadas no relacionamento dos cidadãos com a Administração Pública.

O Regulamento introduziu novos serviços de segurança jurídica eletrónica, como são os selos eletrónicos (de evidente interesse para as pessoas coletivas), os selos temporais (um importante instrumento de prova de que um documento eletrónico existia num determinado momento), o serviço de envio registado eletrónico (que possibilita a prova de envio e receção de um documento eletrónico) e o certificado de autenticação de sítio *web* (para determinar que um sítio *web* é o sítio autêntico de certa pessoa ou entidade e não uma qualquer falsificação, eventualmente movida por intenções maliciosas ou ilícitas).

Pela abrangência dos novos serviços de segurança que prevê, o Regulamento eIDAS tem potencial para impulsionar um quadro de maior segurança para operadores e utilizadores dos serviços da sociedade da informação[18]. É, em todo o caso, sobretudo com a definição, nos seus anexos I a IV, dos requisitos aplicáveis aos certificados qualificados de assinatura eletrónica, aos dispositivos qualificados de criação de assinaturas eletrónicas, aos certificados qualificados de selos eletrónicos e aos certificados qualificados de autenticação de sítios que o Regulamento eIDAS mais contribui para o aumento da cibersegurança e da confiança dos cidadãos na utilização das tecnologias e na prestação de serviços da sociedade da informação.

Em matéria de regulação dos serviços da sociedade da informação, em particular no respeitante ao **comércio eletrónico**, o quadro legal teve uma evolução mais lenta e revelou-se dotado de uma muito mais evidente estabilidade. No final da década de 1990, com a generalização do uso da Internet e da perceção da sua relevância para a prestação de novos serviços e do desenvolvimento de atividades comerciais *online*, a Comissão Europeia preparou o que veio a ser a Diretiva 2000/31/CE, de 8 de junho, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno ("Diretiva do Comércio Eletrónico"), com o objetivo de proteger os consumidores mas também de estimular o crescimento económico e o investimento na inovação.

Esta Diretiva assumiu como princípio-base a liberdade de estabelecimento e, consequentemente, a não sujeição dos operadores a qualquer tipo de autorização prévia, mas estabeleceu um conjunto de deveres de informação, por parte dos prestadores de serviços, no sentido de assegurar a transparência do exercício e a informação dos

17 E na Portaria n.º 189/2014, que veio regulamentar a aplicação da Lei.

18 A expressão "serviços da sociedade da informação" é a que consta do título da Diretiva 2000/31/CE e da Lei n.º 7/2004, de 7 de janeiro, que transpôs a Diretiva para o ordenamento jurídico português.

clientes e consumidores. Por outro lado, como contrapartida dessa liberdade de estabelecimento, foi delineado um quadro de responsabilidade dos prestadores de serviços, em larga medida em benefício dos mesmos, com o objetivo de incentivar o estabelecimento de prestadores de serviços *online*. A Diretiva teve o cuidado, em todo o caso, de distinguir as diferentes situações e intervenientes nessa prestação de serviços, desde o mero facultar de acesso à rede até ao serviço de transmissão ou de armazenamento de mensagens, estabelecendo-se como regra geral a de ausência de um dever geral de vigilância pelos prestadores de serviços. Questão relevante que a Diretiva timidamente abordou, quer em termos comerciais quer em termos de proteção de direitos e legítimos interesses dos cidadãos e empresas, foi a das chamadas "comunicações não solicitadas", apontando-se num momento inicial para uma solução *opt-out tout court*, mas com expressa previsão de que os Estados Membros poderiam permitir, ou não, a comunicação comercial não solicitada por correio eletrónico.

O Decreto-Lei n.º 7/2004, de 7 de janeiro, que transpôs a Diretiva para o Direito português (comummente referido como "Lei do Comércio Eletrónico"), veio regular os vários aspetos já enunciados na Diretiva, nalguns casos desenvolvendo o seu regime, abordando questões não abordadas na Diretiva e até inovando claramente nalguns aspetos. Tal foi o caso da abordagem do legislador português às regras da contratação eletrónica, distinguindo claramente as situações de contratação por meio de comunicação individual (contratação interpessoal), de celebração de contratos *online* (contratação interativa) e, inovação máxima do legislador português, em consonância com a realidade da contratação através de EDI e com o que já vinha sendo discutido no Direito norte-americano, a introdução no nosso Direito da "contratação sem intervenção humana" (ou contratação intersistémica). Relativamente às comunicações não solicitadas, este diploma introduziu um regime misto, com o *opt-in* como regra, mas prevendo um regime *opt-out* para a comunicação entre as empresas e os seus clientes e para o caso de envio de mensagens a pessoas coletivas. Estas regras sobre comunicações não solicitadas[19] vieram trazer alguma estabilidade e confiança no domínio das relações entre prestadores de serviços e clientes/utilizadores.

Nos vinte anos que decorreram desde a adoção da Diretiva, houve um vasto conjunto de alterações do panorama tecnológico e social que convidam a uma revisão deste quadro normativo. Novas realidades, como a Computação em Nuvem, a Internet das Coisas, os Ambientes Inteligentes, a progressiva introdução da Inteligência Artificial, os *drones* (autónomos ou não) e a *Blockchain*, para só referir os casos mais evidentes, vêm impor uma nova abordagem e uma profunda revisão do quadro atual. Um outro aspeto que se tornou evidente nos últimos anos, e que impõe uma profunda revisão dos quadros legais, é a da cada vez maior relevância das plataformas eletrónicas nas mais diversas atividades, incluindo os serviços da sociedade da informação e o comércio eletrónico. A este propósito, o Parlamento Europeu anunciou, em outubro de 2020, a sua intenção de estabelecer novas regras para a regulação das plataformas *online* e funcionamento de mercados *online*, tendo para o efeito sido apresentados os termos de uma iniciativa legislativa tendente à aprovação de um ato legislativo sobre "serviços digitais". Particular atenção será dada à necessidade de combater os conteúdos ilegais *online*, o que previsivelmente obrigará a uma revisão dos atuais quadros de responsabilidade dos prestadores de serviços da sociedade da informação.

19 Mais tarde alteradas pelo Decreto-Lei n.º 62/2009, de 10 de março, e pelo Decreto-Lei n.º 46/2012, de 24 de fevereiro.

Em matéria de **pagamentos eletrónicos**, o impulso inicial partiu da Recomendação da Comissão Europeia sobre um Código Europeu de Boa Conduta em matéria de Pagamento Eletrónico, de 1987 (Recomendação 87/598/CEE, de 8 de dezembro). Ao tempo, o que estava em causa eram, essencialmente, os pagamentos efetuados por cartão com pista magnética ou micro processador através de um equipamento terminal de pagamento eletrónico (TPE) ou de um terminal ponto de venda (TPV). No ano seguinte, a Comissão avançou com uma recomendação sobre sistemas de pagamento e, em especial, às relações entre o titular e o emissor de cartões (Recomendação 88/590/CEE, de 17 de novembro). Em ambos os documentos, a tónica foi posta na segurança e na defesa dos consumidores, nomeadamente no que toca à proteção de dados. Mais tarde, já em 1997, a Comissão Europeia, atenta à ampla realização de transações através de instrumentos de pagamento eletrónico, incluindo cartões de pagamento e serviços de banca no domicílio e de banca telefónica (incluindo já a utilização de cartões de pagamento e de instrumentos de moeda eletrónica), e visando assegurar um elevado grau de defesa do consumidor no domínio dos instrumentos de pagamentos eletrónicos, veio recomendar um conjunto de regras aplicáveis à transferência de fundos e pagamento de numerário através de instrumentos de pagamento eletrónico (Recomendação 97/489/CE, de 30 de julho). Continuava-se, em todo o caso, no domínio das normas não vinculativas, com recomendações de boas práticas que visavam tornar mais transparente a relação entre os prestadores de serviços e os consumidores.

Pouco depois da publicação da Diretiva do Comércio Eletrónico, referida antes, foi aprovada a Diretiva 2000/46/CE, de 18 de setembro, que veio regular o acesso à atividade das instituições de moeda eletrónica bem como a sua atividade. Esta Diretiva apresenta alguns conceitos importantes para a segurança das transações financeiras, como o conceito de "instituição de moeda eletrónica", enquanto empresa ou pessoa coletiva que emite meios de pagamento sob a forma de moeda eletrónica, sendo esta entendida como um valor monetário, representado por um crédito sobre o emitente, armazenado num suporte eletrónico e emitido contra a receção de fundos de um valor não inferior ao valor monetário emitido e que seja aceite como meio de pagamento por outras empresas que não a emitente. A matéria dos serviços de pagamento no mercado interno viria a ser regulada apenas com a Diretiva 2007/64/CE, de 13 de novembro, que estabeleceu regras em matéria de transparência das condições e requisitos de informação aplicáveis aos serviços de pagamento.

Os anos seguintes à aprovação da Diretiva 2007/64/CE foram plenos de novidades tecnológicas e de uma ainda maior generalização da utilização de meios eletrónicos de pagamento, com o rápido crescimento da sua utilização e com a generalização do uso de dispositivos móveis e novos tipos de serviços de pagamento disponíveis no mercado. Entre as preocupações que conduziriam à alteração do quadro regulatório estiveram sempre as de proporcionar um quadro seguro em que os prestadores de serviços pudessem lançar serviços digitais inovadores, seguros e de fácil utilização, e que os consumidores pudessem dispor de meios de pagamento eficazes, práticos e seguros em todo o território da União. Havia uma clara perceção de que o volume crescente de pagamentos eletrónicos à escala mundial e o constante surgimento de novos tipos de serviços traziam riscos associados que havia de enfrentar, com a consciência de que a existência de serviços de pagamentos seguros constitui condição indispensável para o bom funcionamento do mercado. Com esta perspetiva e preocupações viria a ser aprovada a Diretiva 2015/2366/UE, de 25 de novembro, relativa aos serviços de pagamento no mercado interno.

Partindo de uma abordagem tecnologicamente neutra, a Diretiva 2015/2366/UE introduziu uma definição neutra de "aceitação de serviços de pagamento", garantindo a mesma proteção independentemente do serviço de pagamento utilizado. Houve, no entanto, o cuidado de separar, na previsão normativa, os serviços técnicos fornecidos aos prestadores de serviços de pagamento, dos modelos de aceitação de pagamentos propriamente ditos. Outro aspeto importante abordado pela Diretiva 2015/2366/UE é o que se refere a um conjunto de exclusões que eram previstas na Diretiva 2007/64/CE, nomeadamente no que respeitava aos chamados serviços de valor acrescentado, que eram aplicadas de forma diferente nos Estados Membros, o que conduzia a uma falta de segurança jurídica para os consumidores e para os operadores.

Aspeto importante da segurança dos pagamentos eletrónicos, a que a Diretiva expressamente se refere, é o que se prende com as credenciais de segurança personalizada – "elementos personalizados fornecidos pelo prestador de serviços de pagamento a um utilizador de serviços de pagamento para efeitos de autenticação" (artigo 4.º, n.º 31, da Diretiva) – utilizadas para a autenticação segura do cliente e cujo uso é necessário para minimizar os riscos de mistificação da interface (*phishing*) e outras atividades fraudulentas. Coloca-se aqui, mais uma vez, em relevo a questão da utilização de sistemas de encriptação, "que podem gerar códigos de autenticação tais como senhas de utilização única, podem reforçar a segurança das operações de pagamento".

Em termos de segurança do funcionamento dos serviços de pagamentos eletrónicos, a Diretiva é clara ao afirmar a responsabilidade dos prestadores de serviços de pagamentos pela adoção de medidas de segurança "proporcionadas em relação aos riscos de segurança em causa". A este respeito, é particularmente relevante a previsão de que os prestadores de serviços de pagamento deverão estabelecer um quadro para mitigar os riscos e manter procedimentos eficazes de gestão de incidentes e de que deverá ser criado um mecanismo de comunicação regular, a fim de assegurar que os prestadores de serviços de pagamento apresentem periodicamente às autoridades competentes uma avaliação atualizada dos seus riscos em matéria de segurança e das medidas por eles adotadas em resposta a esses riscos". Para além disso, os prestadores de serviços serão obrigados "a comunicar sem demora indevida às autoridades competentes os incidentes graves em matéria de segurança".

Existem discrepâncias na utilização do conceito técnico-jurídico de "autenticação", que, na Diretiva 2015/2366/UE, é entendida como "um procedimento que permite ao prestador de serviços de pagamento verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador", enquanto, no Regulamento (UE) 910/2014 (Regulamento eIDAS), "autenticação" é "o processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado em formato eletrónico a confirmar". Refira-se, no entanto, que a especificidade da matéria dos pagamentos eletrónicos e as suas implicações em termos de segurança levaram o legislador europeu a introduzir na Diretiva 2015/2366/UE o conceito de "autenticação forte do cliente", ou seja "uma autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação".

A Diretiva 2015/2366/UE foi transposta para a ordem jurídica portuguesa pelo Decreto-Lei n.º 91/2018, de 12 de novembro, que veio aprovar um novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica. Este diploma regulou o acesso e condições gerais de atividade dos prestadores de serviços de pagamento e dos emitentes de moeda eletrónica, prevendo a prestação de dois novos tipos de serviços de pagamento, a saber, serviços de iniciação de pagamento e serviços de informação sobre contas. Foram ainda definidas regras relativas ao acesso a sistemas e contas de pagamento e sobre gestão de riscos operacionais e de segurança. De acordo com o previsto pela Diretiva 2015/2366/UE, o Decreto-Lei n.º 91/2018 veio expressamente salientar a exigência de uma autenticação forte, prevendo a adoção de medidas de segurança suficientes para proteger a confidencialidade e integridade das credenciais de segurança personalizadas dos utilizadores de serviços de pagamento. Especial atenção foi ainda dada à necessidade de a autenticação do utilizador, nos serviços de pagamento, incluir "elementos que associem de forma dinâmica a operação a um montante e beneficiário específicos, de modo que o utilizador esteja sempre informado do que está a autorizar".

O Decreto-Lei n.º 91/2018 atribui competências de supervisão prudencial e comportamental ao Banco de Portugal, incluindo competências de fiscalização e de instauração de processos contraordenacionais e de aplicação de sanções, bem como de emitir recomendações e determinações específicas. Em caso de incidentes operacionais e de segurança de caráter severo, os prestadores de serviços deverão notificar sem demora o Banco de Portugal (artigo 71.º, n.º 1). Enquanto autoridade de supervisão, o Banco de Portugal cooperará com as autoridades de supervisão dos restantes Estados Membros, com o Banco Central Europeu e com os bancos centrais. As entidades prestadoras de serviços de pagamento deverão estabelecer "um quadro com medidas de mitigação e mecanismos de controlo adequados para gerir os riscos operacionais e de segurança, relacionados com os serviços de pagamento por si prestados", incluindo "procedimentos eficazes de gestão de incidentes, inclusive para a deteção e classificação de incidentes operacionais e de segurança de caráter severo" (artigo 70.º, n.ºs 1 e 2), devendo o Banco de Portugal estabelecer "as normas regulamentares respeitantes à definição, à aplicação e à monitorização das referidas medidas de segurança" (artigo 70.º, n.º 4). No que respeita ao conceito de "incidentes operacionais e de segurança de caráter severo", a eles se refere a Instrução n.º 1/2019 do Banco de Portugal, que remete para o documento da European Bank Authority (EBA) intitulado *Orientações sobre a comunicação de incidentes de caráter severo ao abrigo da DSP2* (EBA/GL/2017/10).

DESTAQUES

Em matéria de identificação eletrónica, assinaturas eletrónicas e certificação eletrónica, os momentos decisivos na evolução do regime jurídico foram a adoção da Diretiva 1999/93/CE, que estabeleceu o princípio da neutralidade tecnológica e definiu as regras essenciais do sistema de certificação eletrónica nos Estados Membros, e a adoção do Regulamento (UE) 910/2014 (eIDAS), que colocou a tónica na questão da identificação eletrónica (autenticação e assinatura) e introduziu um conjunto de novos serviços da sociedade da informação tendentes a garantir um nível mais elevado de segurança na prestação de serviços e nas transações eletrónicas e a interoperabilidade na prestação de serviços.

Em matéria de comércio eletrónico, o diploma de referência continua a ser a Diretiva 2000/31/CE, que estabelece regras de transparência e deveres de informação a cargo dos prestadores de serviços da sociedade da informação. O desenvolvimento tecnológico dos últimos anos virá certamente impor uma nova abordagem e uma profunda revisão do quadro atual. A regulação e funcionamento das plataformas e mercados *online* já foram anunciados como temas sobre os quais versarão, em breve, novas iniciativas legislativas

Em matéria de pagamentos eletrónicos, os marcos na evolução do regime jurídico são a Diretiva 2007/64/CE, que estabeleceu regras em matéria de transparência das condições e requisitos de informação aplicáveis aos serviços de pagamento, e a Diretiva 2015/2366/EU, que reforçou a segurança dos pagamentos eletrónicos, com a introdução de conceitos novos como as credenciais de segurança personalizada e de autenticação forte e com a responsabilização dos prestadores de serviços de pagamento pelo estabelecimento de medidas para mitigar os riscos e manutenção de procedimentos eficazes de gestão de incidentes.

2.3.7. Propriedade intelectual

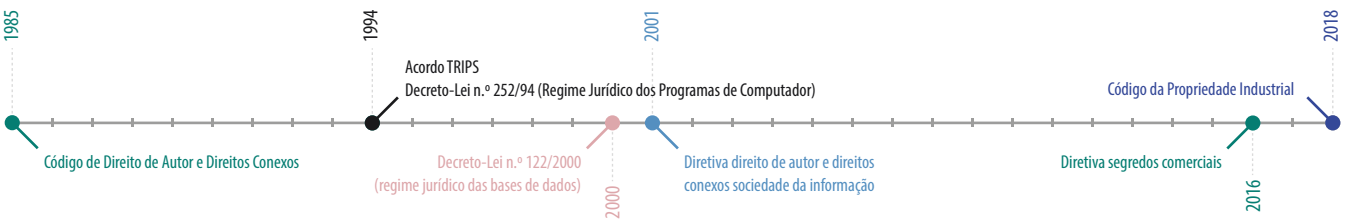
Os primeiros esforços de harmonização internacional em matéria de proteção da propriedade intelectual – e.g. Convenção de Berna, de 1886, relativa à proteção de obras literárias e artísticas; Convenção de Paris para a proteção da propriedade industrial, de 1883; Convenção de Roma, de 1961, para proteção dos artistas intérpretes ou executantes, dos produtores de fonogramas e dos organismos de radiodifusão; e Convenção de Bruxelas, de 1974, para proteção dos sinais transmitidos por satélites de comunicação – são anteriores à década de 1990 e à sociedade da informação, pelo que não é de estranhar que não reflitam uma preocupação especial com a cibersegurança. **A preocupação central na aplicação destes tratados tem sido a harmonização internacional da propriedade intelectual e a cooperação internacional para a sua efetividade.**

Só nos instrumentos mais recentes, como o Acordo sobre os aspetos dos direitos de propriedade intelectual relacionados com o comércio (Acordo TRIPS), constante do anexo 1C do Tratado que cria a Organização Mundial do Comércio, de 1994, encontramos uma preocupação com os riscos da globalização para a tutela e efetividade dos direitos de propriedade intelectual, que podemos associar, ainda que indiretamente, aos riscos dos mercados digitais globais potenciados pela sociedade da informação.

Para Portugal, é naturalmente muito relevante o esforço da União Europeia de harmonização dos direitos de propriedade intelectual, em grande medida relacionados com a transição para o mercado digital. Desde logo, o reconhecimento de tutela a bens tipicamente digitais, com a Diretiva 96/9/CE, de 11 de março, relativa à proteção jurídica das bases de dados, e com a Diretiva 2009/24/CE, de 23 de abril, relativa à proteção jurídica dos programas de computador[20]. Para as obras tradicionais, é relevante a Diretiva 2001/29/CE, de 22 de maio, que promoveu uma harmonização de certos aspetos do direito de autor e dos direitos conexos na sociedade da informação[21]. Especificamente relacionados com a tutela de direitos de autor e direitos conexos na sociedade da informação são ainda relevantes a recente Diretiva 2019/789/UE, de 17 de abril, que estabelece normas sobre o exercício dos direitos de autor e direitos conexos aplicáveis a determinadas transmissões *online* dos organismos de radiodifusão e à retransmissão de programas de televisão e de rádio, e a Diretiva 2014/26/UE, de 26 de fevereiro, relativa à gestão coletiva dos direitos de autor e direitos conexos e à concessão de licenças multiterritoriais de direitos sobre obras musicais para utilização *online* no mercado interno. Do lado da propriedade industrial assume particular relevância a harmonização efetuada por um conjunto de diretivas, nomeadamente, a Diretiva 87/54/CEE, de 16 de dezembro, relativa à proteção jurídica das topografias de produtos semicondutores; a Diretiva 98/44/CE, de 6 de julho, relativa à proteção jurídica das invenções biotecnológicas; a Diretiva 98/71/CE, de 13 de outubro, relativa a desenhos ou modelos; a Diretiva 2004/48/CE, de 29 de abril, relativa ao respeito dos direitos de propriedade intelectual; a Diretiva 2008/95/CE, de 22 de outubro de 2008, que aproxima as legislações dos Estados Membros em matéria de marcas; e a Diretiva 2015/2436, de 16 de dezembro, sobre marcas. Importa ainda referir o Regulamento (CE) 40/94, de 20 de dezembro, sobre marca comunitária, e o Regulamento (CE) 6/2002 do Conselho, de 12 de dezembro de 2001,

20 Que veio revogar a Diretiva 91/250/CEE.

21 Alterada pela Diretiva 2017/1564/UE, de 13 de setembro, e pela Diretiva 2019/790/UE, de 17 de abril.



relativo aos desenhos e modelos comunitários[22]. Por fim, com um âmbito mais abrangente, abarcando todos os direitos de propriedade intelectual, importa referir o Regulamento (UE) 608/2013, de 12 de junho, relativo à intervenção das autoridades aduaneiras para assegurar o cumprimento da legislação sobre os direitos de propriedade intelectual.

Há, em grande parte do esforço de harmonização legislativa da União Europeia relacionada com os direitos de propriedade intelectual e concorrência desleal, uma clara preocupação de adaptação do regime aos bens e riscos da sociedade da informação.

A preocupação com a cibersegurança não é, por isso, alheia a algumas das soluções jurídicas adotadas pela União Europeia nesta matéria. Com particular interesse para a questão da cibersegurança, é a Diretiva 2016/943/UE, de 8 de junho, relativa à proteção de *know-how* e de informações confidenciais (segredos comerciais) contra a sua obtenção, utilização e divulgações ilegais. Logo nos seus considerandos iniciais se salienta que "[a]s empresas inovadoras estão cada vez mais expostas a práticas desonestas que visam a apropriação indevida de segredos comerciais, como o roubo, a cópia não autorizada, a espionagem económica ou a violação de requisitos de confidencialidade, quer dentro, quer fora da União". Em conformidade, a Diretiva prevê um conjunto de medidas de reforço da tutela dos segredos comerciais. Embora nenhuma delas verse especificamente sobre a questão da cibersegurança, estas medidas refletem as questões da dificuldade de deteção, pesquisa, prova e restrição contra atos lesivos de exclusivos de propriedade intelectual e/ou concorrência desleal.

Em Portugal, a matéria dos direitos de autor e direitos conexos encontra-se compilada no Código de Direito de Autor e Direitos Conexos (CDADC), aprovado pelo Decreto-Lei n.º 63/85, de 14 de março[23]. Fora deste Código ficou o regime jurídico dos programas de computador, aprovado pelo Decreto-Lei n.º 252/94, de 20 de outubro[24], bem como o regime jurídico das bases de dados, aprovado pelo Decreto-Lei n.º 122/2000, de 4 de julho. A técnica legislativa é um pouco incoerente, já que deixa partes dos respetivos regimes dentro do Código e parte nestes diplomas avulsos. Importante também é a Lei n.º 26/2015, de 14 de abril, que regula as entidades de gestão coletiva do direito de autor e dos direitos conexos, inclusive quanto ao estabelecimento em território nacional e à livre prestação de serviços das entidades previamente estabelecidas noutro Estado Membro da União Europeia ou do Espaço Económico Europeu.

No âmbito da tutela dos direitos de autor e direitos conexos, uma nota especial para o regime de proteção das *medidas de carácter tecnológico e das informações para a gestão eletrónica dos direitos*, previstas nos artigos 217.º a 228.º do CDADC, que resultam da transposição das medidas previstas no artigo 6.º da Diretiva 2001/29/CE, no artigo 11.º do Tratado da OMPI sobre Direito de Autor e no artigo 18.º do Tratado da OMPI sobre Interpretações ou Execuções e Fonogramas. Estas medidas dividem-se entre as medidas de

22 Alterado pelo Regulamento (CE) 1891/2006, de 18 de dezembro de 2006.

23 O Código tem sido sucessivamente alterado. As últimas alterações são as resultantes da Lei n.º 36/2017, de 2 de junho, e do Decreto-Lei n.º 100/2017, de 23 de agosto.

24 Alterado pelo Decreto-Lei n.º 334/97, de 27 de novembro.

caráter tecnológico, entendidas como "toda a técnica, dispositivo ou componente que, no decurso do seu funcionamento normal, se destinem a impedir ou restringir atos relativos a obras, prestações e produções protegidas" (artigo 217.º, n.º 2, CDADC) e a informação para a gestão eletrónica dos direitos, entendida como "toda a informação prestada pelos titulares dos direitos que identifique a obra, a prestação e a produção protegidas a informação sobre as condições de utilização destes, bem como quaisquer números ou códigos que representem essa informação" (artigo 223.º, n.º 2, CDADC). Este regime determina, não só a legitimidade destas medidas tecnológicas, no confronto com os sempre sensíveis direitos de acesso à cultura e à informação, mas também a tutela civil e penal contra a sua violação. **A tutela destas medidas tecnológicas visa assegurar a cibersegurança do exclusivo de exploração digital das obras, prestações e produções protegidas por direito de autor e direitos conexos.**

O Código da Propriedade Industrial (CPI) em vigor, aprovado pelo Decreto-Lei n.º 110/2018, de 10 de dezembro, incorpora já todas as medidas propostas pelos tratados internacionais e pelos instrumentos de Direito da União Europeia. Entre as inovações mais relevantes do CPI, por transposição da Diretiva (UE) 2016/943, foi precisamente a autonomização do ilícito de violação dos segredos comerciais (artigo 331.º CPI), face ao ilícito de concorrência desleal (artigo 332.º CPI), dentro da tutela contraordenacional da lealdade da concorrência que se encontra tradicionalmente prevista no Direito português dentro de um regime abrangente de propriedade industrial.

A tutela da confidencialidade de informações comerciais e industriais (*know-how*) enquanto elemento essencial da competitividade das empresas e da lealdade da concorrência é, seguramente, o ponto do regime da propriedade industrial que encontra maior conexão com as questões da cibersegurança. Não se pode ignorar que, nas híper informatizadas sociedades modernas, o sistema informático – sobretudo, bases de dados digitais – é o repositório natural do *know-how* da empresa. Acresce, como risco para a segurança das informações comerciais e industriais, que cada vez mais estas bases de dados se encontram armazenadas em "nuvens digitais", que mais não são do que aluguer de espaço em megaestruturas de discos rígidos em armazéns físicos deslocalizados em territórios alheios à titularidade dos dados. O recente aumento do teletrabalho (por força das restrições impostas pelas medidas de combate à pandemia COVID-19) veio criar um risco acrescido para os segredos de negócio, com a dispersão das redes empresariais por micro postos de trabalho móveis conectados pela Internet, exponenciando o risco de penetração/interceção nos sistemas informáticos empresariais. Nessa medida, na sociedade da informação, a tutela da confidencialidade dos segredos de negócios é, em grande medida, a tutela da cibersegurança dos sistemas informáticos onde tais dados são armazenados e processados. Também aqui, como nas medidas tecnológicas encontradas no CDADC, a preocupação do legislador centrou-se em medidas para obtenção, preservação e conservação de prova, mas a previsão não está especificamente direcionada para o ambiente digital. Podemos, ainda assim, argumentar que algumas destas medidas, previstas de forma genérica, são suscetíveis de aplicação em ambiente digital, com as devidas adaptações.

De salientar ainda que a Lei do Cibercrime, no seu artigo 6.º, n.º 4, agrava o crime de acesso ilegítimo a sistema informático quando, através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei. Tutela-se aqui criminalmente também os segredos de negócio, embora a mesma agravante não esteja prevista para a interceção ilegítima de dados informáticos, que constitui um ilícito sobre a segurança dos sistemas informáticos que coloca em igual risco de violação os segredos comerciais e industriais. Ainda assim, pode dizer-se que a Lei do Cibercrime vem acrescer, à tutela contraordenacional dada pelo CPI, uma tutela penal sobre a confidencialidade dos segredos de negócio especificamente no âmbito da sociedade da informação. Há aqui, inequivocamente, uma preocupação com a cibersegurança dos segredos de negócio face à crescente e quase universalização da digitalização da informação empresarial.

A ubiquidade inerente à qualidade "imaterial" da criação tutelada pela propriedade intelectual torna o seu objeto particularmente vulnerável à violação do respetivo exclusivo patrimonial em ambientes digitais em exponencial crescimento e de âmbito transnacional.

A preocupação da legislação de propriedade intelectual e de concorrência desleal tem-se centrado em três pontos essenciais: (1) a harmonização internacional dos objetos tutelados e regimes jurídicos; (2) a criação de medidas cautelares, de investigação e de prova contra potenciais violações; e (3) a criação de mecanismos de cooperação internacional. A questão da cibersegurança, enquanto garantia da fiabilidade dos sistemas informáticos que albergam objetos protegidos por propriedade intelectual e concorrência desleal, ainda não se encontra firmada nos instrumentos legais vigentes. Parece, no entanto, ser uma questão central para a prevenção da violação de direitos de propriedade intelectual e da prática de atos de concorrência desleal. Exceção a esta situação encontra-se, do lado do direito de autor e direitos conexos, o regime de proteção das medidas de carácter tecnológico e das informações para a gestão eletrónica dos direitos, previsto nos artigos 217.º a 228.º do CDADC. E, do lado da concorrência desleal, associada à tutela da propriedade industrial, a consideração da violação da confidencialidade de segredos de negócios protegidos como um elemento de agravação do crime de acesso ilegítimo a sistema informático (artigo 6.º, n.º 4, da Lei do Cibercrime).

Como insuficiência do regime pode apontar-se, desde logo, que, no âmbito da criminalidade informática, se deveria prever a violação de segredos de negócio como um elemento de agravação não só do crime de acesso ilegítimo, mas também, pelo menos, do crime de interceção ilegítima. Na verdade, também no caso dos crimes de dano informático e sabotagem informática, quando do ato resultar a "perda" de segredo de negócio para o lesado, se poderia ponderar uma tutela penal reforçada da propriedade intelectual e segredos comerciais e industriais. Por último, verifica-se que os direitos de autor, direitos conexos e direitos privativos de propriedade industrial não surgem como elementos de agravação dos crimes informáticos, o que, em abstrato, seria também uma tutela penal reforçada passível de ser considerada face ao especial potencial lesivo que a criminalidade informática tem para estes bens jurídicos.

DESTAQUES

A matéria da propriedade intelectual encontra-se harmonizada internacionalmente através de um conjunto nuclear de tratados cuja preocupação central, a par da harmonização internacional da propriedade intelectual, tem sido a promoção da sua efetividade, essencialmente, pela criação de medidas cautelares, de investigação e de prova contra potenciais violações, associados a mecanismos de cooperação internacional.

A ubiquidade inerente à qualidade "imaterial" da criação tutelada pela propriedade intelectual torna o seu objeto particularmente vulnerável à violação do respetivo exclusivo patrimonial em ambientes digitais transnacionais.

Na área do Direito de Autor, tem sido aprovada legislação sobre medidas tecnológicas de proteção e gestão, com o fim de assegurar a cibersegurança do exclusivo de exploração digital das obras, prestações e produções protegidas por direito de autor e direitos conexos.

Na área da propriedade industrial e concorrência desleal, é na tutela da confidencialidade de informações comerciais e industriais (*know-how*), enquanto elemento essencial da competitividade das empresas e da lealdade da concorrência, que a preocupação com a cibersegurança dos sistemas informáticos empresariais se torna mais relevante.

Há ainda um caminho a fazer na tutela da propriedade intelectual no âmbito da cibercriminalidade, já que estes bens jurídicos ainda não se encontram devidamente valorizados como elementos agravantes dos crimes informáticos.

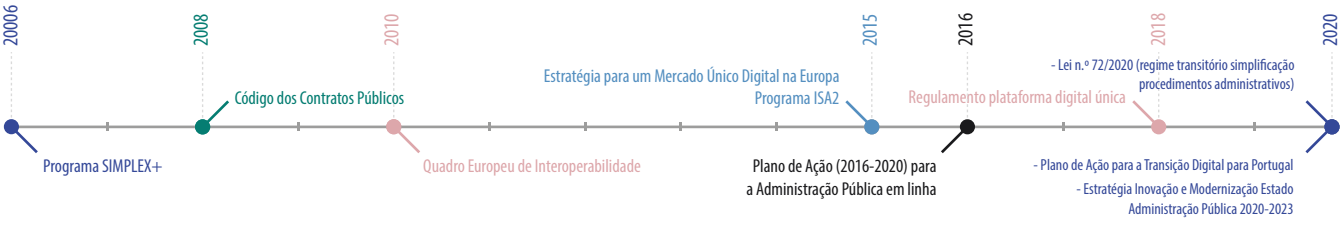
2.3.8. Transição digital da Administração Pública

Com a "Estratégia para um Mercado Único Digital na Europa" [COM(2015) 192 final], já referida, a Comissão Europeia assumiu que, sendo o setor das TIC a base de todos os sistemas económicos modernos, o Mercado Único Digital deveria ser um mercado em que fosse assegurada a livre circulação de mercadorias, pessoas, serviços e capitais e em que os cidadãos e as empresas pudessem beneficiar de um acesso sem descontinuidades a atividades *online* e desenvolver essas atividades em condições de concorrência leal e com um elevado nível de proteção dos consumidores e dos seus dados pessoais, independentemente da sua nacionalidade ou local de residência. Entre as ações concretas a adotar para atingir este objetivo, a Comissão identificou a **necessidade de criar uma Administração Pública em linha, como as que já estavam a ser desenvolvidas em diferentes Estados Membros, assegurando que esses serviços fossem comunicáveis entre si**. A interoperabilidade administrativa – já pensada através do Quadro Europeu de Interoperabilidade, de 2010 [COM(2010) 744] – foi, deste modo, escolhida como o método a seguir para a concretização de uma Administração Pública em linha e como um vetor essencial ao estabelecimento do Mercado Único Digital.

A cibersegurança figura como uma prioridade no documento de trabalho que acompanhou a Estratégia [SWD(2015) 100], sublinhando-se a necessidade de promover um nível elevado de segurança das redes e da informação e a essencialidade da segurança pública *online* em toda a UE, em vista do aumento alarmante de incidentes de cibersegurança e dos riscos associados para o fornecimento de serviços essenciais que são entendidos como certos, como os de fornecimento de água, de cuidados de saúde, de eletricidade, de transporte ou de serviços móveis. A Comissão Europeia defendeu, a este respeito, que "uma aproximação comum pela UE em matéria de certificação de segurança das [TIC], partindo da experiência decorrente de esquemas nacionais e voluntários, contribuiria para um elevado padrão de segurança e poderia providenciar uma escala necessária ao mercado para produtos e serviços digitais seguros".

No **Plano de Ação para a Administração Pública em linha 2016-2020** [COM(2016) 179], que definiu logo a seguir, a Comissão enunciou um conjunto de princípios estruturantes para vigorarem lado a lado com os tradicionais princípios gerais da atividade administrativa:

- *Princípio do digital por defeito*, para dar preferência à prestação de serviços públicos digitais, embora mantendo outros canais abertos para quem não utiliza a via eletrónica por preferência ou necessidade;
- *Princípio da declaração única*, para que as administrações públicas reutilizem dados internamente (assegurando a proteção dos dados pessoais) para evitar sobrecarregar cidadãos e empresas com a necessidade de prestar repetidas vezes a mesma informação;
- *Princípio da inclusividade e da acessibilidade*, para que os serviços públicos sejam desenvolvidos de forma a promover um acesso intuitivo, fácil e simplificado, capaz de suprir demandas de inclusão, nomeadamente associadas a idosos e a pessoas portadoras de deficiência;



- *Princípio da abertura e transparência*, para que as administrações públicas partilhem informações entre si, permitindo aos administrados aceder, controlar e corrigir os dados sobre si mantidos, sendo-lhes ainda possível acompanhar os respetivos procedimentos e, inclusivamente, interagir e criar um clima de confiança na conceção e na prestação dos serviços;
- *Princípio do transfronteiriço por definição*, para que os serviços públicos sejam concebidos de forma a viabilizar a sua disponibilização transfronteiriça, facilitando a observância das liberdades de circulação no contexto do Mercado Interno da União;
- *Princípio da interoperabilidade por definição*, para que sejam concebidos sistemas operativos e bases de dados interconexionados digitalmente, visando a livre circulação de dados e a prestação de serviços públicos digitais em todo o contexto da União;
- ***Princípio da credibilidade e da segurança*, para que os esforços de modernização digital da Administração Pública se norteiem pela observância do quadro jurídico em sede de proteção de dados e de privacidade, assegurando a segurança informática desde a fase de conceção dos serviços, já que esta constitui uma condição prévia relevante para criar um clima de confiança nos serviços digitais**.

A interoperabilidade administrativa é promovida através do Programa ISA[2] – estabelecido pela Decisão 2015/2240 – que cria soluções de interoperabilidade e quadros comuns para as Administrações Públicas, as empresas e os cidadãos europeus como um meio para modernizar o setor público, com vista a "facilitar uma interação eletrónica transfronteiriça e intersectorial eficiente e eficaz entre as administrações públicas europeias, por um lado, e entre estas e as empresas e os cidadãos, por outro, e contribuir para o desenvolvimento de uma administração eletrónica mais eficiente, mais simplificada e mais intuitiva à escala nacional, regional e local" [artigo 1.º, n.º 1, alínea *b)* da Decisão]. O princípio da segurança deverá ser observado em todas as ações desenvolvidas ao abrigo deste Programa, por força do artigo 4.º, alínea *b)*, da Decisão.

Na revisão intercalar da estratégia relativa ao Mercado Único Digital [COM(2017) 228], a Comissão Europeia avançou o propósito de dotar a União Europeia de uma Plataforma Digital Única, de modo a assegurar que os administrados ultrapassam mais facilmente exigências administrativas quando exercem liberdades de circulação. Este objetivo foi atingido com o **Regulamento (UE) 2018/1724, de 2 de outubro, relativo à criação de uma plataforma digital única para a prestação de acesso a informações, a procedimentos e a serviços de assistência e de resolução de problemas**.

As preocupações com a cibersegurança – desde logo, com a necessidade de estabelecer uma plataforma segura em que os incidentes de segurança sejam minorados – são visíveis em vários pontos do Regulamento:

- **os meios e mecanismos aqui estabelecidos para aceder à Plataforma Única Digital deverão operar com base nos meios de identificação eletrónica de pessoas singulares e coletivas definidos pelo Regulamento (UE) 910/2014, para assegurar as maiores condições de segurança e imprimir maior credibilidade à estrutura digital**;
- os Estados Membros são incentivados a reforçar a coordenação, o intercâmbio e a colaboração entre si, de forma a desenvolverem soluções de cibersegurança, nomeadamente a segurança das transações, para assegurar um nível de confiança suficiente nos meios eletrónicos, podendo tomar medidas, de acordo com o Direito da União, para assegurar a cibersegurança e para prevenir a fraude de identidade e outras formas de fraude;

- no intercâmbio transfronteiriço de elementos de prova e de informações, a aplicação do Regulamento deverá respeitar todas as regras aplicáveis em matéria de proteção de dados e o princípio da segurança, sendo que o sistema técnico deve, nomeadamente, assegurar a confidencialidade e a integridade dos elementos de prova e assegurar um nível elevado de segurança para a transmissão e o tratamento dos elementos de prova (artigo 14.º, n.º 3);

- na criação e estabelecimento da Plataforma, ao adotar atos de execução que estabeleçam as especificações para esse sistema técnico, a Comissão Europeia deverá ter em devida conta as normas e as especificações técnicas elaboradas pelas organizações e pelos organismos europeus e internacionais de normalização [e.g. Comité Europeu de Normalização (CEN), Instituto Europeu de Normalização das Telecomunicações (ETSI), Organização Internacional de Normalização (ISSO), União Internacional das Telecomunicações (UIT)], bem como as regras do RGPD e do Regulamento que estabelece a proteção de dados perante as instituições, órgãos e organismos da União Europeia [Regulamento (UE) 2018/1725];

- a Comissão Europeia deve articular-se com as autoridades nacionais quando surjam incidentes de segurança e quando estes tenham de ser resolvidos;

- é constituído um grupo de coordenação da Plataforma, composto por um coordenador nacional por cada Estado Membro e presidido por um representante da Comissão, ao qual cabe, entre outras funções, a de debater a aplicação dos princípios de segurança e de privacidade desde a conceção (artigo 30.º, n.º 1).

Em convergência com o plano europeu no domínio digital, os Estados Membros têm vindo a adotar diversas estratégias de transição digital, abrangendo soluções tecnológicas que permitem ao Estado garantir a interoperabilidade entre sistemas públicos e promover a difusão de informação, de forma livre e transparente.

Em Portugal, a estratégia de modernização e simplificação administrativa tem sido traçada há vários anos, através de diversos Programas, Planos, Estratégias e instrumentos vários de políticas de agilização procedimental, procurando-se adaptar o modelo de funcionamento do setor público às novas realidades tecnológicas e aos desafios da chamada Administração Pública em linha (*e-Government*). Refira-se, a título de exemplo, o Programa SIMPLEX+, lançado em 2006, que contempla mais de mil medidas de simplificação administrativa e legislativa para tornar mais fácil a vida dos cidadãos e das empresas na sua relação com a Administração, assim como contribuir para aumentar a eficiência interna dos serviços públicos. Reforçado em 2016, o Programa SIMPLEX inclui 255 medidas de simplificação administrativa e legislativa e de modernização dos serviços públicos.

Entre as diversas soluções de transição digital em Portugal, avulta o **Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro[25], que colocou o país na linha da frente na contratação pública através de meios exclusivamente eletrónicos**, sendo completada a digitalização com a possibilidade de consulta *online* de todos os contratos públicos em relação aos quais as entidades adjudicantes têm o dever de publicitar através do Portal dos Contratos Públicos (Portal BASE), nos termos do artigo 465.º do Códigos dos Contratos Públicos e da Portaria

25 Objeto de sucessivas alterações, a última das quais operada pela Resolução da Assembleia da República n.º 16/2020, de 19 de março.

n.º 57/2018, de 26 de fevereiro. O Portal Base, que é gerido pelo Instituto dos Mercados Públicos, do Imobiliário e da Construção (IMPIC), assegura a transparência e a legalidade na contratação pública, permitindo a sindicância e o controlo democrático dos elementos referentes à formação e à execução dos contratos públicos. Em 2009, foi estabelecida a obrigatoriedade da contratação pública eletrónica e criado um mercado privado de prestadores certificados de serviços de plataformas de contratação pública, duas soluções pioneiras a nível mundial.

O enquadramento legal das plataformas eletrónicas de contratação pública começou por ser dado pelo Decreto-Lei n.º 143-A/2008, de 25 de julho, que consagrou a opção por procedimentos de contratação pública baseados em comunicações, troca e arquivo de dados através da utilização de plataformas eletrónicas, e pela Portaria n.º 701-G/2008, de 29 de julho, que definiu os requisitos e condições de utilização das plataformas eletrónicas pelas entidades adjudicantes no processo de formação dos contratos públicos. A segurança foi então identificada como "condição absolutamente nuclear neste novo suporte[,] no sentido de que as tecnologias usadas sejam fiáveis, robustas e propiciadoras de procedimentos nos quais participem e só tenham acesso as pessoas autorizadas". O Decreto-Lei n.º 143-A/2008 e a Portaria n.º 701-G/2008 foram revogados pela Lei n.º 96/2015, de 17 de agosto, que veio regular a disponibilização e a utilização das plataformas eletrónicas de contração pública, estabelecendo os requisitos e as condições a que as mesmas devem obedecer e a obrigação de interoperabilidade com o Portal dos Contratos Públicos e com outros sistemas de entidades públicas. A Lei n.º 96/2015 fixa um conjunto de deveres para as empresas gestoras de plataformas eletrónicas, no que respeita, nomeadamente, à contratação de recursos humanos próprios e de auditores de segurança externos, à sua interação com os utilizadores e ao seu relacionamento com o Instituto dos Mercados Públicos, do Imobiliário e da Construção e com o Gabinete Nacional de Segurança (GNS), que é a entidade credenciadora das plataformas eletrónicas e dos respetivos auditores de segurança.

Refira-se, ainda, a alteração introduzida ao Código do Procedimento Administrativo (CPA), aprovada pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, que consagrou o princípio da administração eletrónica. A importância da segurança é sublinhada pelo artigo 14.º, n.º 2, do CPA, onde se estabelece que "os meios eletrónicos utilizados devem garantir a disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade, a conservação e a segurança da informação". A Lei n.º 72/2020, de 16 de novembro, reforçou a simplificação procedimental e a respetiva digitalização, incluindo os procedimentos em que estejam envolvidas as autarquias locais, e introduziu novas regras sobre o funcionamento dos órgãos colegiais telemáticos.

O **Plano de Ação para a Transição Digital para Portugal (PATD),** aprovado pela Resolução do Conselho de Ministros n.º 30/2020, de 21 de abril, assenta em três pilares estratégicos – capacitação e inclusão digital, transformação digital do tecido empresarial e digitalização do Estado – e **prevê medidas agrupadas em seis catalisadores, incluindo o da "regulação, privacidade, cibersegurança e ciberdefesa"**, no âmbito do qual se prevê:

- o acompanhamento da Estratégia Nacional de Segurança do Ciberespaço, pelo CNCS;
- a gestão de ações de suporte aos desafios da cibersegurança, nos termos do programa Indústria 4.0, a ser coordenada pela Associação Empresarial para a Inovação (COTEC);

- a capacitação e ajuste organizacional da estrutura nacional de Data Protection Officer (DPO), de forma a garantir a evolução do quadro jurídico de proteção de dados pessoais, envolvendo a CNPD;
- a elaboração do Livro Verde do Futuro do Trabalho.

Na sequência do PATD, o Governo português adotou a **Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023** (Resolução do Conselho de Ministros n.º 55/2020, de 31 de julho), que tem, entre outros objetivos, o de (a) reforçar a governação global das tecnologias; (b) melhorar a interoperabilidade e a integração de serviços, e (c) gerir o ecossistema de dados com segurança e transparência. A Medida 8.4. – definida para prossecução do objetivo estratégico de reforçar a governação global das tecnologias – consiste, precisamente, em reforçar os níveis de cibersegurança dos organismos da Administração Pública, através do Quadro Nacional de Referência para a Cibersegurança que foi desenvolvido pelo CNCS.

DESTAQUES

A necessidade de criar uma Administração Pública em linha, assente no princípio da interoperabilidade, foi assumida pela Comissão Europeia, em 2015, como um vetor essencial ao estabelecimento do Mercado Único Digital.

O *Princípio da credibilidade e da segurança* é um dos princípios estruturantes do Plano de Ação para a Administração Pública em linha 2016-2020, exigindo que os esforços de modernização digital da Administração Pública se norteiem pela observância do quadro jurídico em sede de proteção de dados e de privacidade, assegurando a segurança informática desde a fase de conceção dos serviços.

O objetivo da Comissão Europeia de dotar a UE de uma Plataforma Digital Única foi prosseguido com o Regulamento (UE) 2018/1724, de 2 de outubro, relativo à criação de uma plataforma digital única para a prestação de acesso a informações, a procedimentos e a serviços de assistência e de resolução de problemas.

Em 2020, foram aprovados o Plano de Ação para a Transição Digital e a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, ambos com objetivos e medidas em matéria de cibersegurança. Está ainda em curso o desenvolvimento da Estratégia para a Transformação Digital da Administração Pública 2021-2023, que, com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, completará este conjunto de políticas públicas na área do digital para o Estado.

3. APLICAÇÃO DO QUADRO NORMATIVO

3.1. Na prática dos tribunais

3.1.1. Tribunal de Justiça da União Europeia

A jurisprudência do TJUE sobre matérias atinentes à cibersegurança – prova digital, comunicações eletrónicas e proteção de dados pessoais – foi fundada pelo acórdão *Digital Rights Ireland*, de 8 de abril de 2014[26], que declarou a invalidade da Diretiva 2006/24/CE, transposta para a ordem jurídica portuguesa pela Lei n.º 32/2008, de 17 de julho. Em resposta a pedidos de decisão prejudicial endereçados pela High Court irlandesa e pelo Verfassungsgerichtshof austríaco, o TJUE concluiu que a Diretiva era incompatível com os artigos 7.º e 8.º da CDFUE, por implicar uma ingerência de "grande amplitude" e "particularmente grave" nos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais.

O Tribunal notou que os dados de tráfego e de localização eram "suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados". Apesar de reconhecer que a Diretiva prosseguia um objetivo de interesse geral da União Europeia, *i.e.* o de "contribuir para a luta contra a criminalidade grave e, assim, em última análise, para a segurança pública", o Tribunal entendeu que os termos adotados não respeitavam o princípio da proporcionalidade, por as obrigações de conservação abarcarem todos os meios de comunicação eletrónica e todos os assinantes e utilizadores registados, sem qualquer diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves, o que representava uma ingerência nos direitos fundamentais de quase toda a população europeia. Segundo o Tribunal, a Diretiva pecava ainda por não conter critérios objetivos que limitassem o acesso e utilização dos dados pelas autoridades nacionais competentes, nem as condições materiais e processuais em que isso deveria ocorrer, e por não prever critérios objetivos para a determinação do período de conservação dos dados.

Dois anos mais tarde, o TJUE teve oportunidade de voltar a debruçar-se sobre esta matéria no acórdão *Tele2 Sverige AB*, de 21 de dezembro de 2016, na sequência de dois pedidos de decisão prejudicial formulados pelo Kammarrätten i Stockholm (Suécia) e pelo Court of Appeal (Reino Unido), onde se pergunta, *inter alia*, se: "É compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta, uma obrigação geral de conservar dados de tráfego relativos a todas as pessoas, a todos os meios

26 Acórdão do Tribunal de Justiça (Grande Secção), de 8 de abril de 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, processos apensos C293/12 e C594/12, disponível em https://eur-lex.europa.eu [12.12.2020].

de comunicação eletrónica e a todos os dados de tráfego, sem quaisquer distinções, limitações ou exceções, para efeitos do objetivo de combate à criminalidade"[27].

O TJUE retomou algumas das considerações já tecidas em *Digital Rights Ireland* sobre a natureza dos dados em causa, acrescentando que os dados fornecem os meios para determinar o perfil das pessoas em causa, "informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações". Também aqui o Tribunal entendeu que a conservação e acesso a estes dados constituía uma ingerência ampla e particularmente grave nos direitos consagrados pelos artigos 7.º e 8.º da CDFUE, para além de poder ter impacto sobre o exercício da liberdade de expressão previsto no artigo 11.º da CDFUE. O Tribunal concluiu que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que preveja, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica. Acrescentou, em todo o caso, que o mesmo artigo 15.º não se opõe a uma "conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos de luta contra a criminalidade grave, desde que a conservação dos dados seja limitada ao estritamente necessário, no que se refere às categorias de dados a conservar, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada".

Decorre igualmente deste acórdão que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, "deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União".

Em 2 de outubro de 2018, no acórdão *Ministerio Fiscal*, o TJUE respondeu a um pedido de decisão prejudicial em que se questionava quais os critérios a adotar para determinar a gravidade dos crimes em que se torna possível, para a sua investigação criminal, recorrer ao acesso a dados de tráfego[28]. O TJUE reiterou a posição assumida nos acórdãos anteriores, mas notou que, enquanto uma ingerência grave só pode ser justificada, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, por um objetivo de luta contra a criminalidade grave, uma ingerência não grave pode ser justificada por um objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral. Como no processo em apreço apenas estavam em causa dados que permitiam "identificar os titulares dos cartões SIM ativados durante um período de 12 dias, com o código IMEI do telemóvel roubado", o TJUE entendeu que a ingerência nos direitos consagrados nos artigos 7.º e 8.º da CDFUE não deveria ser considerada grave, pelo que esse acesso não devia ser limitado à luta contra a criminalidade grave.

O TJUE voltou a pronunciar-se sobre a Diretiva 2002/58/CE, no acórdão *Privacy International*, de 6 de outubro de 2020, na sequência de um pedido de decisão prejudicial formulado pelo Investigatory Powers Tribunal do Reino

27 Acórdão do Tribunal de Justiça (Grande Secção), de 21 de dezembro de 2016, *Tele2 Sverige AB contra Post- och telestyrelsen e Secretary of State for the Home Department contra Tom Watson e o.*, processos apensos C-203/15 e C-698/15, disponível em http://curia.europa.eu [12.12.2020].

28 Acórdão do Tribunal de Justiça (Grande Secção), de 2 de outubro de 2018, *Ministerio Fiscal*, processo C-207/16, disponível em http://curia.europa.eu [12.12.2020].

Unido, no âmbito de processo em que é parte a Privacy International, uma organização não-governamental, contra o Ministro dos Negócios Estrangeiros e da Commonwealth, o Ministro da Administração Interna e serviços de segurança e de informações como o GCHQ, o MI5 e o MI6[29].

Uma das questões dirigidas ao TJUE foi a de saber se "o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz do artigo 4.º, n.º 2, TUE, e dos artigos 7.º, 8.º e 11.º e do artigo 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações". O TJUE recordou que as limitações aos direitos consagrados nos artigos 7.º, 8.º e 11.º da CDFUE devem obedecer ao requisito de proporcionalidade, o que exige que as regulamentações nacionais neste domínio prevejam normas claras e precisas e imponham requisitos mínimos, "de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso".

Segundo o TJUE, a transmissão de dados de tráfego e de localização realizada de modo generalizado e indiferenciado é suscetível de gerar "no espírito das pessoas em causa a sensação de que a sua vida privada é objeto de constante vigilância" e "tem por efeito tornar na regra a derrogação à obrigação de princípio de garantir a confidencialidade dos dados, ao passo que o sistema instituído pela Diretiva 2002/58 exige que essa derrogação continue a ser a exceção". Para além disso, a "mera conservação dos referidos dados pelos prestadores de serviços de comunicações eletrónicas comporta riscos de abuso e de acesso ilícito". Tudo somado, o Tribunal concluiu que "o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz do artigo 4.º, n.º 2, TUE, e dos artigos 7.º, 8.º e 11.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações".

Em matéria de proteção de dados pessoais, são ainda relevantes os acórdãos *Schrems I*, de 2015, e *Schrems II*, de 2020. No acórdão *Schrems I*, o TJUE declarou inválida a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, que considerara que os Estados Unidos da América asseguravam um nível adequado de proteção dos dados pessoais transferidos a partir da CE, e acrescentou que, em qualquer caso, uma decisão deste tipo não obsta a que uma autoridade de controlo de um Estado Membro examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que tenham sido transferidos de um Estado Membro para o país terceiro em causa, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado[30]. No acórdão *Schrems II*, o TJUE voltou a invalidar uma Decisão da Comissão sobre o nível de proteção nos Estados Unidos da América, neste caso, a Decisão de Execução (UE) 2016/1250, de 12 de julho, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UEEUA. O TJUE notou que o RGPD abrange a transferência de dados pessoais efetuada para fins comerciais por operador económico estabelecido num Estado Membro para outro operador económico estabelecido num país terceiro, "não obstante o facto de, no decurso ou na

29 Acórdão do Tribunal de Justiça (Grande Secção), de 6 de outubro de 2020, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, processo C-623/17, disponível em http://curia.europa.eu [12.12.2020].

30 Acórdão do Tribunal de Justiça (Grande Secção), de 6 de outubro de 2015, *Maximillian Schrems contra Data Protection Commissioner*, processo C-362/14, disponível em http://curia.europa.eu [12.12.2020].

sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do Estado", o que implica que os direitos das pessoas cujos dados pessoais são transferidos beneficiam de um nível de proteção substancialmente inferior ao garantido na União pelo RGPD lido à luz da CDFUE. Assim sendo, a menos que exista uma decisão de adequação validamente adotada pela Comissão Europeia, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro, fundada em cláusulastipo de proteção de dados adotadas pela Comissão, se considerar que essas cláusulas não são ou não podem ser respeitadas no país terceiro e que a proteção dos dados transferidos exigida pelo Direito da União não pode ser assegurada por outros meios[31].

3.1.2. Tribunais portugueses

Na prática judicial portuguesa, têm surgido **dúvidas a respeito da articulação entre a Lei do Cibercrime e o Código de Processo Penal**. Como referido no capítulo anterior, as disposições processuais sobre prova digital não estão, na sua grande maioria, incorporadas no Código de Processo Penal, mas antes na Lei do Cibercrime. O problema reside no facto de o artigo 189.º do Código de Processo Penal estender o regime das escutas telefónicas (artigos 187.º e 188.º do Código) às "conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceção das comunicações entre presente", e estabelecer que "a obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo". O artigo 189.º do Código de Processo Penal incide, deste modo, sobre algumas das realidades concretas que a Lei do Cibercrime veio regular, como são as cobertas pelos artigos 17.º (apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 19.º (interceção de comunicações).

Sendo a Lei do Cibercrime posterior ao Código de Processo Penal, as decisões judiciais neste domínio tendem a sustentar uma revogação implícita ou tácita, pelo menos parcial, do artigo 189.º do Código de Processo Penal. Emblemático é, a este respeito, a acórdão do Tribunal da Relação de Évora, de 6 de janeiro de 2015, onde se lê que as "Leis n.º 32/2008, de 17-07 e 109/2009, de 15-09 (Lei do Cibercrime) revogaram a extensão do regime das escutas telefónicas, previsto nos artigos 187.º a 190.º do Código de Processo Penal, às áreas das 'telecomunicações electrónicas', 'crimes informáticos' e 'recolha de prova electrónica'"[32]. No mesmo sentido vai uma decisão mais recente do mesmo tribunal, de 8 de outubro de 2019, segundo a qual "o regime processual das comunicações telefónicas previsto nos artigos 187.º a 190.º do Código de Processo Penal deixou de ser aplicável por extensão às 'telecomunicações eletrónicas', 'crimes informáticos' e 'recolha de prova eletrónica (informática)' desde a entrada em vigor da Lei n.º 109/2009, de 15.09 (Lei do Cibercrime), como regime regra"[33].

---

31 Acórdão do Tribunal de Justiça (Grande Secção), de 16 de julho de 2020, *Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems*, processo C-311/18, disponível em http://curia.europa.eu [12.12.2020].

32 Tribunal da Relação de Évora, acórdão de 6 de janeiro de 2015, prolatado no processo n.º 6793/11.2TDLSB-A.E1, disponível em www.dgsi.pt [12.12.2020].

33 Tribunal da Relação de Évora, acórdão de 8 de outubro de 2019, prolatado no processo n.º 180/19.1GHSTC.E1, disponível em www.dgsi.pt [12.12.2020]. Cf., igualmente, Tribunal da Relação do Porto, acórdão de 20 de novembro de 2019, prolatado no processo n.º 54/19.6GDSTS-A.P1.

Mais complexa é a questão de saber qual a **validade jurídica da Lei n.º 32/2008, de 17 de julho, que transpôs para a ordem jurídica portuguesa a Diretiva 2006/24/CE**. A obrigatoriedade de conservação generalizada de dados de tráfego e de localização tem sido posta em causa pela sua possível incompatibilidade com o Direito da União Europeia, depois de a Diretiva 2006/24/CE ter sido declarada inválida pelo TJUE no acórdão *Digital Rights Ireland*, de 8 de abril de 2014, analisado antes. A Comissão Nacional de Proteção de Dados, que é a entidade responsável pela tramitação dos processos contraordenacionais decorrentes de violações da Lei n.º 32/2008, emitiu a Deliberação n.º 641/2017 onde, invocando os acórdãos *Digital Rights Ireland* e *Tele2*, recomendou a revisão da lei e, pouco tempo depois, a Deliberação n.º 1008/2017, onde anunciou que deixaria de aplicar a Lei n.º 32/2008 devido à incompatibilidade deste diploma com a CDFUE e com a Constituição da República Portuguesa (CRP). O Gabinete Cibercrime da Procuradoria-Geral da República, por seu turno, tem por adquirido que a Lei n.º 32/2008 permanece válida, uma vez que o legislador nacional fora "muito para lá das exigências da Diretiva" e considerara no Direito interno "a maior parte das exigências que vieram a ser feitas" pelo TJUE (Nota Prática n.º 7/2015, de 30 de dezembro).

Em 22 de janeiro de 2019, a Provedora de Justiça, Maria Lúcia Amaral, recomendou à Ministra da Justiça que "promova a alteração à Lei n.º 32/2008, de 17 de julho, a fim de que o regime nela inscrito se venha a conformar com as exigências decorrentes da Carta dos Direitos Fundamentais da União Europeia, tal como foram tais exigências interpretadas pela jurisprudência pertinente do Tribunal de Justiça". O Ministério da Justiça, em resposta à solicitação da Provedora de Justiça, transmitiu a convicção de que a Lei n.º 32/2008 oferece as garantias suficientes para se darem por respeitados os direitos fundamentais que aqui poderiam ser postos em causa, nomeadamente porque o acesso aos dados de tráfego e de localização só é autorizado por despacho fundamentado do juiz instrução, mediante requerimento do Ministério Público, e em relação a um catálogo de crimes previamente definido.

Em 26 de agosto de 2019, a Provedora de Justiça requereu ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade da Lei n.º 32/2008, "por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e ao sigilo das comunicações (artigo 34.º, n.º 1) e por violação do direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1)". O Tribunal Constitucional ainda não se pronunciou sobre este requerimento, mas já teve oportunidade para se pronunciar sobre casos em que a Lei n.º 32/2008 foi chamada à colação.

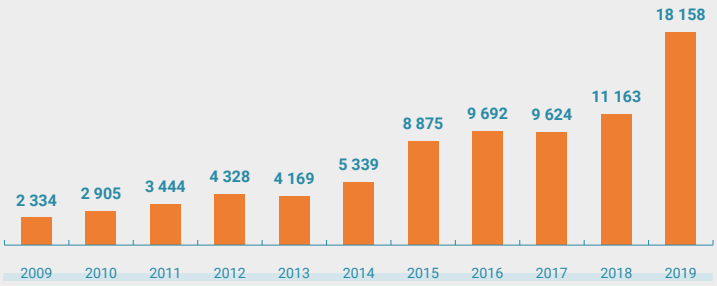
O acórdão n.º 420/2017, de 13 de julho, proferido no âmbito do processo n.º 917/16, apreciou a validade do indeferimento de um pedido formulado pelo Ministério Público para aceder a dados de base, no âmbito de uma investigação criminal da prática de crime de pornografia de menores[34]. A 1.ª Secção de Instrução Criminal da Instância Central da Comarca de Lisboa havia indeferido o pedido com o argumento de que o artigo 6.º da Lei n.º 32/2008 estaria ferido da inconstitucionalidade, por violar os artigos 18.º e 34.º, n.º 4, da CRP. Tendo o Ministério Público interposto recurso desta decisão para o Tribunal Constitucional, o Tribunal constatou que "não é correto basear a invalidade da lei nacional numa transposição do juízo efetuado pelo Tribunal de Justiça sobre a globalidade do texto da diretiva que esta transpõe, sem proceder a uma análise específica e autónoma da norma nacional que esteja em causa e, no presente caso, sem atender à natureza dos dados de base". Atendendo ao facto de se tratarem de dados de base, o Tribunal entendeu que o princípio da proporcionalidade estava integralmente cumprido: "a medida em causa cumpre os requisitos

34 Acórdão do Tribunal Constitucional n.º 420/2017, de 13 de julho, prolatado no processo n.º 917/16, disponível em http://www.tribunalconstitucional.pt [12.12.2020].

de idoneidade, pois a conservação de dados de base é uma medida adequada para permitir a identificação do utilizador registado, a quem o endereço do protocolo IP estava atribuído, suspeito de autoria de um dos crimes graves referidos, e de necessidade, na medida em que não é possível configurar um meio menos restritivo para as autoridades competentes procederem à referida identificação". O Tribunal Constitucional decidiu, por isso, que a obrigatoriedade de conservação de dados de base, prevista no artigo 6.º e no artigo 4.º da Lei n.º 32/2008, não era inconstitucional, no que se manteve coerente com a jurisprudência firmada nos acórdãos n.os 486/2009 e 403/2015.

O Tribunal Constitucional ainda não se pronunciou, no entanto, especificamente sobre a conservação e transmissão de dados de tráfego e localização. No acórdão n.º 464/2019, o Tribunal reconheceu que, apesar de a declaração da invalidade da Diretiva 2006/24/CE não pôr imediatamente em causa a Lei n.º 32/2008, isso não obsta a que se considere imperativo avaliar a conformidade desta com o Direito da União Europeia, em especial com a CDFUE, ainda que tenha acabado por não fazer esta avaliação nesse processo, uma vez que o problema da validade da Lei n.º 32/2008 à luz da CRP não havia sido suscitado[35].

FIG. 1 - EVOLUÇÃO DOS CIBERCRIMES 2009-2019



Fonte: Direção-Geral da Política de Justiça (2020)

No que respeita à **prática de cibercrimes**, os dados da Direção-Geral de Política da Justiça indicam que os cibercrimes registados sofreram um crescimento acentuado desde a entrada em vigor da Lei do Cibercrime, na ordem dos 600%, o que facilmente se explica pela digitalização crescente das atividades humanas e maior acesso e utilização da Internet e sistemas de informação. O número total de cibercrimes registados pelas autoridades policiais em 2019 foi 18.158, o que corresponde a 5.41% do total de crimes registados no território nacional nesse mesmo ano.

Quanto aos tipos de cibercrimes registados em 2019, segundo a mesma fonte, o crime de burla informática

35 Acórdão do Tribunal Constitucional n.º 464/2019, de 21 de outubro, prolatado no processo n.º 26/2018, disponível em http://www.tribunalconstitucional.pt [12.12.2020]. Sobre esta matéria, há uma decisão do Tribunal da Relação de Lisboa, acórdão de 28 de novembro de 2018, prolatado no processo n.º 8617/17.8T9LSB-A.L1-3, disponível em www.dgsi.pt [12.12.2020], onde se lê que "[a] declaração de invalidade da Directiva 2006/24/CE (transposta para ordem interna na Lei nº 32/2008 de 17/07) não tem uma consequência automática sobre a validade do acto legislativo interno que a transpôs, porquanto o acto legislativo nacional tem uma fonte autónoma de validade e legitimidade, pois não se limitou a transpor tal Directiva, antes a densificando e aperfeiçoando ao direito interno, sendo que a análise do Tribunal de Justiça apenas incidiu sobre o texto da Directiva".

é o mais frequente (16.310, correspondentes a 89,22%), seguido pelos crimes de acesso e de interceção ilegítimos, que, em conjunto, chegam a 617 (34,0% do total dos cibercrimes), conforme a tabela que se segue[36].

TABELA 1

Tipo de crime (nível 1)	Tipo de crime (nível 2)	Tipo de crime (nível 3)	2019
(CP) Contra as pessoas	**Contra reserva da vida privada**	Devassa p/meio de informática	529
(CP) Contra o património	**Contra o património em geral**	Burla informática/comunicações	16310
Legislação avulsa	**Informáticos**	Reprodução programa protegido	8
		Acesso/interceção ilegítimos	617
		Viciação/destruição/dano relativo a dados/ programas	28
		Falsidade informática	346
		Sabotagem informática	273
		Outros informáticos	47
	Informáticos Total		**1 319**
Total Geral			**18 158**

Fonte: Direção-Geral da Política de Justiça (2020)

A evolução do número de cibercrimes registados pelas autoridades nacionais confirma a ideia de que não estamos perante um fenómeno de reduzida importância ou meramente transitório. É antes um tipo de criminalidade cujo crescimento acompanha a maior digitalização da nossa sociedade. Por isso se percebe que, no âmbito da política criminal, o legislador português tenha destacado a cibercriminalidade como uma das áreas de prevenção prioritária – artigo 4.º, alínea d), da Lei n.º 55/2020, de 27 de agosto – e de investigação prioritária – artigo 5.º, alínea e), do mesmo diploma.

36 Optou-se por fazer referência apenas aos crimes mencionados no Relatório Anual de Segurança Interna 2019 como pertencentes ao domínio da cibercriminalidade (Sistema de Segurança Interna, 2020: 48).

3.2. Na prática administrativa

3.2.1. Processos contraordenacionais

Cabe ao CNCS instruir os processos de contraordenação por incumprimento dos deveres impostos pelos artigos 12.º e seguintes da Lei n.º 46/2018 e aplicar as respetivas coimas. Não existem, até ao momento, registos de processos de contraordenação instruídos pelo CNCS, o que se explica pelo facto de ainda não ter sido adotada a legislação que há de definir os requisitos de segurança e os requisitos de notificação de incidentes cujo incumprimento importará responsabilidade contraordenacional.

A CNPD tem competências de fiscalização e sanção ao abrigo do RGPD e exerceu-as, pela primeira vez em 2018 (Deliberação n.º 984/2018[37]), quando ainda não tinha sido adotada a Lei n.º 58/2019 que veio assegurar a execução do RGPD na ordem jurídica portuguesa. Perante a alegação de que estaria a arrogar-se uma condição que ainda não lhe pertencia, violando o princípio da legalidade, a CNPD invocou o estatuto de autoridade nacional com a atribuição de controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais que lhe advinha do artigo 22.º, n.º 1, da Lei n.º 67/98, de 26 de outubro, notando que o RGPD não trouxera novidades relevantes para os seus poderes. O caso versava, no essencial, sobre a existência, num centro hospitalar, de uma política de atribuição de credenciais de acesso que permitira a funcionários do grupo funcional "técnico/a" usufruir do nível de acesso reservado ao grupo funcional "médico", o que se traduzira "na possibilidade indiscriminada de consulta de processos clínicos de todos os utentes do hospital". A CNPD considerou terem sido praticadas três contraordenações – violação do princípio da minimização dos dados, violação do princípio da integridade e confidencialidade, incapacidade do responsável pelo tratamento em assegurar a confidencialidade, integridade, disponibilidade e resiliência permanente dos sistemas e serviços de tratamento – a que fez corresponder três coimas, num valor global de quatrocentos mil euros.

Em 2019, a CNPD concluiu quatro processos contraordenacionais. Os textos das deliberações disponíveis no *site* da CNPD estão anonimizados, o que não permite determinar o perfil dos arguidos. A Deliberação n.º 21/2019 aplicou uma coima no valor de vinte mil euros, em razão da violação do direito de acesso do titular aos respetivos dados, nos termos do artigo 83.º, n.º 3, do RGDP[38]. A Deliberação n.º 207/2019 aplicou uma coima no valor de dois mil euros, por violação do direito de informação, resultante de a arguida ter realizado um tratamento de dados não assegurando a informação sobre este aos titulares, e por violação de direito dos titulares no quadro do RGPD[39]. A Deliberação n.º 222/2019 aplicou uma coima no valor de dois mil euros, em razão da violação do direito de informação aos titulares acerca do tratamento de dados pessoais[40]. A Deliberação n.º 297/2019 aplicou oitenta e seis coimas, num valor global de cento e sete mil euros, pela prática de contraordenações resultantes do envio de comunicações não solicitadas, com fins de marketing direto e publicidade, sem prévio consentimento do destinatário[41].

Como referido no capítulo anterior, em 2017, a CNPD deliberou desaplicar a Lei n.º 32/2008 nas situações de

37 Deliberação n.º 984/2018, de 9 de outubro, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].
38 Deliberação n.º 21/2019, de 5 de fevereiro, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].
39 Deliberação n.º 207/2019, de 19 de março, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].
40 Deliberação n.º 222/2019, de 25 de março, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].
41 Deliberação n.º 297/2019, de 6 de maio, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].

tratamento de dados pessoais a apreciar daí em diante, por considerá-la incompatível com a CDFUE e com a CRP (Deliberação n.º 1008/2017). Em 2019, a CNPD adotou uma deliberação de sentido semelhante, desta feita a respeito de algumas disposições da Lei n.º 58/2019, diploma que, como vimos, veio assegurar a execução do RGPD na ordem jurídica portuguesa. Recordando o seu Parecer n.º 20/2018, de 2 de maio, sobre a então Proposta de Lei n.º 120/XIII/3.ª, a CNPD notou que o legislador português havia decidido manter algumas das normas aí assinaladas como violadoras do Direito da União e disse não ser possível salvá-las através de uma interpretação corretiva, por ser insuprível a antinomia com as normas do RGPD e da CDFUE[42].

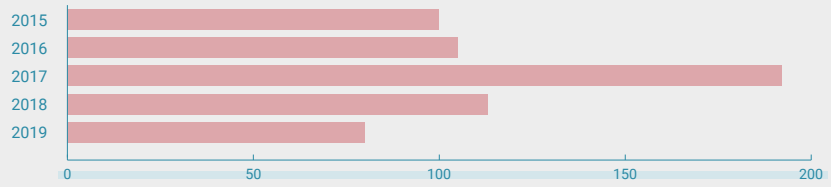
Também em 2019, a CNPD recebeu de várias entidades públicas o pedido de dispensa de aplicação de coimas durante três anos, ao abrigo do disposto nos artigos 44.º, n.º 2, e 59.º da Lei n.º 58/2019, sem que contra elas estivesse a decorrer um processo de natureza contraordenacional. Com a Deliberação n.º 495/2019, a CNPD esclareceu que a dispensa prevista na lei só pode ser requerida pelas entidades públicas e decidida após a notificação da acusação da prática de um ilícito contraordenacional, no âmbito de um processo concreto, pelo que todos os requerimentos de dispensa apresentados fora deste contexto não justificam a abertura de um procedimento decisório[43].

3.2.2. Reporte de incidentes de segurança

Apesar de, como referimos na secção anterior, ainda não ter sido adotada a legislação que há de definir os requisitos de notificação de incidentes de segurança, nos termos do artigo 13.º da Lei n.º 46/2018, o CERT.PT tem vindo a registar incidentes. Segundo o *Relatório Riscos & Conflitos* (CNCS, 2020: 40), o CERT.PT registou 754 incidentes em 2019, o que representou um aumento de 26% em relação ao ano anterior e confirma a tendência de crescimento constante verificada desde 2015. Os incidentes mais comuns em 2019 foram o *phishing*, a infeção por *malware* e o compromisso de conta, 31%, 16% e 13% do total, respetivamente (CNCS, 2020: 38).

A ANACOM, por seu turno, recebeu, em 2019, notificações de 80 incidentes de segurança por parte das empresas que oferecem redes públicas ou serviços de comunicações eletrónicas acessíveis ao público, um valor inferior ao de 2018 (113 incidentes) e o mais baixo desde 2015 (ANACOM, 2020: 5).

FIG. 2 - NÚMERO ANUAL DE NOTIFICAÇÕES



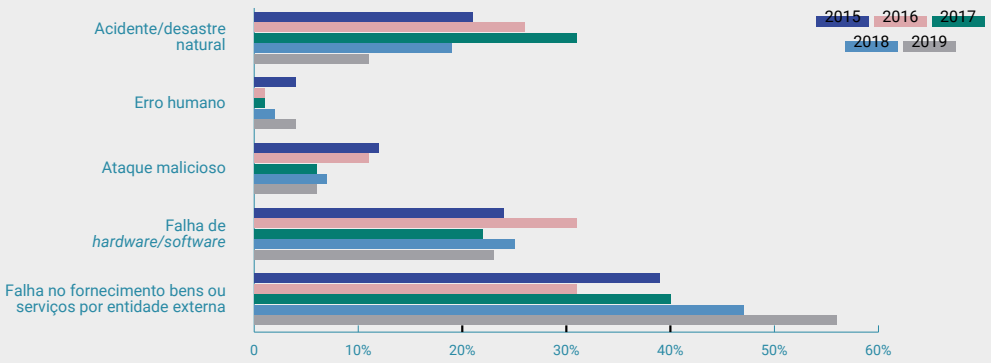
Fonte: ANACOM (2020)

42 Deliberação n.º 494/2019, de 3 de setembro, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].

43 Deliberação n.º 495/2019, de 3 de setembro, disponível em https://www.cnpd.pt/home/decisoes/ [12.12.2020].

A principal "causa raiz" na base dos incidentes de segurança notificados à ANACOM continua a ser a falha no fornecimento de bens ou serviços por entidade externa (56%), sendo que a falha de *hardware/software* se cifrou nos 23%, o ataque malicioso em 6%, o erro humano em 4% e o acidente/desastre natural em 11%.

FIG. 3 - INCIDENTES DE SEGURANÇA NOTIFICADOS POR CAUSA RAIZ



Fonte: ANACOM (2020)

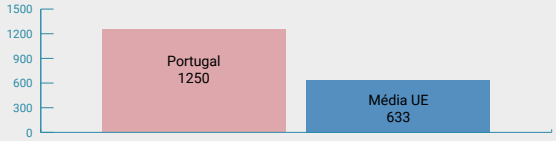
Entre os aspetos mais relevantes apontados pela ANACOM no seu relatório sobre 2019, refira-se o facto de esta ter reportado à ENISA oito incidentes de segurança, "os quais excederam o limiar à escala da UE, com base na duração de um incidente e no número relativo de assinantes/acessos afetados", número este mais elevado do que o verificado em 2018 (cinco).

3.2.3. Caracterização de operadores de serviços essenciais

Em cumprimento do disposto no artigo 29.º, n.º 1, da Lei n.º 46/2018, o CNCS procedeu à identificação dos operadores de serviços essenciais. Os dados disponíveis indicam que foram identificados 26 serviços essenciais e 1250 operadores de serviços essenciais, segundo informações comunicadas à Comissão Europeia e apresentadas no relatório de 28 de outubro de 2019, em que esta fez a avaliação da coerência das abordagens adotadas pelos Estados Membros na identificação dos operadores de serviços essenciais de acordo com o artigo 23.º, n.º 1, da Diretiva SRI [COM(2019) 546]. Segundo o relatório, Portugal está abaixo da média da UE no que respeita à identificação de serviços essenciais (35 serviços) e acima da média da UE no que respeita à identificação de operadores de serviços essenciais (633 operadores).

FIG. 4 - SERVIÇOS ESSENCIAIS IDENTIFICADOS

FIG. 5 - OPERADORES DE SERVIÇOS ESSENCIAIS IDENTIFICADOS



Na análise que fez dos resultados, a Comissão Europeia notou que o facto de as autoridades nacionais não serem obrigadas a apresentar o nome dos operadores identificados torna difícil a comparação dos resultados do processo de identificação em termos da exaustividade da lista e do impacto em empresas da mesma dimensão e pertencentes ao mesmo setor. Portugal é referido como tendo optado por adotar uma abordagem mais granular do que a Estónia, que optou por um título muito geral que permite identificar basicamente qualquer operador que considerem essencial no subsector da eletricidade, e menos granular do que a Bulgária, que elaborou uma lista extremamente pormenorizada de serviços e incluiu mesmo um serviço não abrangido pelo Anexo II da Diretiva SRI. Tal como a Dinamarca, Portugal optou por não incluir alguns serviços que outros Estados Membros incluíram. A Comissão concluiu que os Estados Membros têm interpretações divergentes quanto ao que constitui um serviço essencial nos termos da Diretiva SRI, observando que estas "lacunas de coerência" podem dar origem a condições de concorrência diferentes entre os operadores de serviços essenciais no mercado interno.

O relatório da Comissão apenas disponibiliza dados quanto aos serviços essenciais identificados pelos Estados Membros nos subsetores da eletricidade e do transporte ferroviário. Portugal identificou dois serviços essenciais em cada subsetor:

TABELA 2

Subsetor	Serviços identificados
Eletricidade	Operadores de redes de distribuição Operadores da rede de transporte
Transporte ferroviário	Gestores de infraestruturas na aceção do artigo 3.º, n.º 2, da Diretiva 2012/34/UE Empresas ferroviárias na aceção do artigo 3.º, n.º 1, da Diretiva 2012/34/UE, incluindo os operadores de instalações de serviço na aceção do artigo 3.º, n.º 12, da Diretiva 2012/34/UE

DESTAQUES

A aplicação do quadro legal de Direito da União Europeia e de Direito português tem suscitado dúvidas por parte dos tribunais e das entidades administrativas com poderes de fiscalização e sanção.

A declaração de invalidade da Diretiva 2006/24/CE, pelo TJUE, no acórdão *Digital Rights Ireland*, de 2014, suscitou, em Portugal, a questão de saber qual a validade jurídica da Lei n.º 32/2008, sobre conservação de dados, que transpôs a Diretiva para a ordem jurídica portuguesa. A CNPD considera-a inválida e, em deliberação de 2017, decidiu deixar de a aplicar, ao passo que o Ministério da Justiça e o Gabinete Cibercrime da Procuradoria-Geral da República entendem que a Lei permanece válida.

Num acórdão de 2019, o Tribunal reconheceu que, apesar de a declaração da invalidade da Diretiva 2006/24/CE não pôr imediatamente em causa a Lei n.º 32/2008, isso não obsta a que se considere imperativo avaliar a conformidade desta com o Direito da União Europeia, em especial com a Carta dos Direitos Fundamentais da União Europeia. Encontra-se pendente no Tribunal Constitucional um processo de fiscalização abstrata da constitucionalidade da Lei n.º 32/2008, requerido pela Provedora de Justiça, em 2019.

Os tribunais portugueses também se têm debatido com dúvidas quanto à articulação entre a Lei do Cibercrime e o Código de Processo Penal, em virtude da área de sobreposição existente entre o artigo 189.º do Código e os artigos 17.º (apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 19.º (interceção de comunicações) da Lei do Cibercrime. A orientação dos tribunais tem sido no sentido de sustentar uma revogação implícita ou tácita, pelo menos parcial, do artigo 189.º do Código de Processo Penal.

Dados da Direção-Geral de Política da Justiça indicam que os cibercrimes registados sofreram um crescimento acentuado desde a entrada em vigor da Lei do Cibercrime, na ordem dos 600%, sendo que o número total de cibercrimes registados pelas autoridades policiais em 2019 (18.158) corresponda a 5.41% do total de crimes registados no território nacional nesse ano.

Ainda não existem registos de processos contraordenacionais instruídos ao abrigo da Lei n.º 46/2018, por não ter sido adotada a legislação que há de definir os requisitos de segurança e os requisitos de notificação de incidentes cujo incumprimento importará responsabilidade contraordenacional.

A CNPD já exerce as suas competências de fiscalização e sanção ao abrigo do RGPD desde 2018, tendo produzido, até ao momento, cinco deliberações condenatórias (uma em 2018 e quatro em 2019). Os valores globais das coimas aplicadas oscilam entre dois mil euros e quatrocentos mil euros.

Em cumprimento do disposto no artigo 29.º, n.º 1, da Lei n.º 46/2018, o CNCS procedeu à identificação dos operadores de serviços essenciais. Os dados disponíveis indicam que foram identificados 26 serviços essenciais e 1250 operadores de serviços essenciais. Segundo relatório da Comissão Europeia, Portugal está abaixo da média da UE no que respeita à identificação de serviços essenciais (35 serviços) e acima da média da UE no que respeita à identificação de operadores de serviços essenciais (633 operadores).

4. NOTAS CONCLUSIVAS

O quadro normativo aplicável à segurança do ciberespaço está em constante evolução, pelo que o levantamento feito neste Relatório tornar-se-á, rápida e inexoravelmente, desatualizado. Foi possível identificar, em todo o caso, algumas necessidades de intervenção legislativa no plano nacional, como são a adoção de legislação que fixe os requisitos de segurança e os requisitos de notificação de incidentes, nos termos dos artigos 12.º e 13.º da Lei n.º 46/2018, a transposição da Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas e a introdução de alterações à Lei n.º 58/2019, para assegurar a sua conformidade com o Direito da União. A agenda legislativa ao nível da União Europeia também está em intenso desenvolvimento, com propostas para um regulamento relativo a ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal e para um regulamento sobre o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação.

No que respeita ao mapeamento dos problemas ético-morais associados à cibersegurança, este Relatório procurou sobretudo identificar as questões com que se debatem decisores políticos, reguladores, empresas de tecnologia e académicos quando refletem e traçam planos de ação para promover a segurança no ciberespaço, com a consciência dos valores fundamentais que estão em jogo e das responsabilidades que impendem sobre todos os participantes no ciberespaço, desde os profissionais de cibersegurança até aos cidadãos comuns, passando pelos Estados, as empresas e as organizações. Também aqui o mapeamento é aproximativo e provisório, como provisórias são as soluções jurídicas ensaiadas para tentar domar os avanços tecnológicos de modo a colher os benefícios e a minimizar os riscos.

5. NOTAS METODOLÓGICAS

O *Relatório Cibersegurança em Portugal – Linha de Observação Ética & Direito* utiliza fontes de diversa natureza, ainda que com clara prevalência das fontes documentais de acesso aberto, como são as bases jurídico-documentais da Organização das Nações Unidas, do Conselho da Europa, da União Europeia, do Instituto de Gestão Financeira e Equipamentos da Justiça, da Procuradoria-Geral da República de Lisboa e da Direção-Geral de Políticas de Justiça. Recorreu-se também a relatórios elaborados pelo CNCS, pelo CERT.PT, pelo Ministério da Administração Interna, pelo Ministério Público e pelo Sistema de Segurança Interna, bem como a dados disponibilizados diretamente por algumas organizações, como os relativos ao cibercrime, da DGPJ.

O Relatório privilegia o uso de fontes primárias – legislação, jurisprudência, instrumentos de política –, mas não deixa de convocar alguns trabalhos académicos relevantes para o tratamento dos temas analisados, sobretudo no capítulo dedicado ao mapeamento dos problemas ético-morais.

A análise do quadro normativo de Direito da União Europeia e de Direito português em matéria de segurança das redes e da informação e das questões suscitadas a propósito da aplicação da Lei de Cibercrime e da proteção de dados na investigação penal beneficiou da colaboração prestada pelos parceiros deste Relatório, nomeadamente, a Polícia Judiciária e Gabinete Cibercrime da Procuradoria-Geral da República..

ENTIDADES PARCEIRAS

Agência da União Europeia para a Cibersegurança (ENISA)

Agência para a Modernização Administrativa (AMA)

Autoridade Nacional de Comunicações (ANACOM)

Assembleia da República

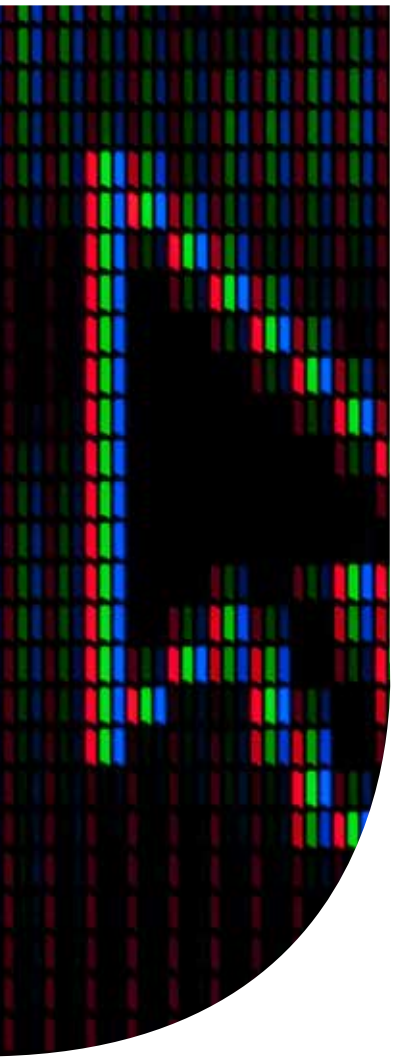
Comissão Nacional de Proteção de Dados (CNPD)

Direção-Geral da Política de Justiça (DGPJ)

Instituto Português de Acreditação (IPAC)

Polícia Judiciária

Procuradoria-Geral da República



CONSELHO CONSULTIVO

Alexandre Sousa Pinheiro
(Professor Universitário em Direito)

António Brandão Moniz
(Faculdade de Ciências e Tecnologia – Universidade Nova de Lisboa)

José Luís Garcia
(Instituto de Ciências Sociais – Universidade de Lisboa)

Luís Antunes
(Faculdade de Ciências – Universidade do Porto)

Manuel Mira Godinho
(Instituto Superior de Economia e Gestão – Universidade de Lisboa)

Maria Eduarda Gonçalves
(ISCTE – Instituto Universitário de Lisboa)

Paulo Esteves-Veríssimo
(KAUST – King Abdullah University of Science and Technology)

Pedro Miguel Alves Ribeiro Correia
(Instituto Superior de Ciências Sociais e Políticas – Universidade de Lisboa)

Sandro Miguel Ferreira Mendonça
(ISCTE – Instituto Universitário de Lisboa)


Workflow
abandons
1 hr.
1 day

REFERÊNCIAS PRINCIPAIS

Relatórios

ANACOM (2020), *Relatório de Violações de Segurança ou Perdas de Integridade 2019*.

CANVAS (2017a), *White Paper 1 Cybersecurity and Ethics*.

CANVAS (2017b), *White Paper 4 Technological Challenges in Cybersecurity*.

CNCS (2020), *Relatório Cibersegurança em Portugal: Riscos & Conflitos 2020*. Lisboa: Centro Nacional de Cibersegurança.

C-PROC (2020), *The global state of cybercrime legislation 2013 – 2020: A cursory overview*. Estrasburgo: Conselho da Europa.

EC (2019), *Relatório da Comissão ao Parlamento Europeu e ao Conselho que avalia a coerência das abordagens adotadas pelos Estados-Membros na identificação dos operadores de serviços essenciais de acordo com o artigo 23.º, n.º 1, da Diretiva 2016/1148/UE relativa à segurança das redes e sistemas de informação*, COM(2019) 546 final, 28.10.2019.

EC (2020), *Índice de Digitalidade da Economia e da Sociedade (IDES) de 2020*: Portugal.

ENISA (2016), *Definition of Cybersecurity: Gaps and Overlaps in Standardisation*, European Agency for Network and Information Security.

ERC (2019), *A Desinformação – Contexto Europeu e Nacional (Contributo da ERC para o debate na Assembleia da República)*. Lisboa: ERC.

GGE (2013), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98.

Sistema de Segurança Interna (2019), *Relatório Anual de Segurança Interna 2018*.

Sistema de Segurança Interna (2020), *Relatório Anual de Segurança Interna 2019*.

Publicações académicas

Brey, P. (2007), "Ethical Aspects of Information Security and Privacy", *in* M. Petković e W. Jonker (eds.), *Security, Privacy, and Trust in Modern Data Management*, Berlin/Heidelberg, Springer, pp. 21-36.

Claps, M., e Alexa, J. (2020), "The new Ethic of the Citizen-Centric Public Services", *INNOVATION: Analyze the Future*, disponível em https://blog-idcuk.com/the-new-ethic-of-the-citizen-centric-public-services/ [27.10.2020].

Covelo de Abreu, J. (2020), "Os princípios gerais da Administração Pública em linha na União Europeia e a análise do artigo

14.º do CPA – revisitando as necessidades de literacia digital", *in* C. Amado Gomes *et al.* (eds.) *Comentários ao Código do Procedimento Administrativo*, vol. I, 5.ª ed., Lisboa, AAFDL, pp. 387-411.

Eggenschwiler, J. (2019), *International Cybersecurity Norm Development: The Roles of States Post-2017*, EU Cyber Direct.

Freitas, P. e Novais, P. (2018), *Inteligência Artificial e Regulação de Algoritmos*, Ministério da Ciência, Tecnologia, Inovações e Comunicações, Brasil.

Gerard, G. (2019), "Botnet mitigation and international law", *Columbia Journal of Transnational Law*, vol. 58, n.º 1.

Mačák, K. (2016), "Is the international law of cybersecurity in crisis?", *in* N. Pissanidis *et al.* (eds.), *Cyber Power: 2016 8th International Conference on Cyber Conflict*, Tallinn, NATO Publications, pp. 127-139.

Osula, A-M & Rõigas, H. (eds.) (2016), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, NATO Publications.

Persing, C. (2018), "Ethics in Cyber Security: WWW in Reference to Cyber Security Does Not Mean What You Think!", *Association News*, disponível em https://www.nacva.com/content.asp?admin=Y&contentid=624 [27.10.2020].

Schmitt, M. (ed.) (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press.

Schmitt, M. (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press.

Vallor, S. (2018), *An Introduction to Cybersecurity Ethics*, disponível em https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf [27.10.2020].

Outros documentos

ACM, *ACM Code of Ethics and Professional Conduct*, disponível em https://www.acm.org/code-of-ethics [27.10.2020].

ISSA, *Information Systems Security Association Code of Ethics*, disponível em https://www.issa.org/issa-code-of-ethics/ [27.10.2020].

Microsoft (2014), *International Cybersecurity Norms: Reducing conflict in an Internet-dependent world*, disponível em https://www.microsoft.com/en-us/cybersecurity/content-hub/reducing-conflict-in-Internet-dependent-world [27.10.2020].

Microsoft (2016), *From Articulation to Implementation: Enabling progress on cybersecurity norms*, disponível em https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8 [27.10.2020].

Websites

http://curia.europa.eu

http://www.dgsi.pt/

http://www.tribunalconstitucional.pt

https://dre.pt/

https://eur-lex.europa.eu

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt
(+351) 210 497 400

Observatório
de **Cibersegurança**