Revista JURÍDICA PORTUCALENSE

www.upt.pt

IJP PORTUCALENSE INSTITUTE FOR LEGAL RESEARCH

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

N.º 29 | Universidade Portucalense | Porto | 2021

https://doi.org/10.34625/issn.2183-2705(29)2021

Jorge Bacelar Gouveia

Direito do Ciberespaço e Segurança Cibernética

DOI: https://doi.org/10.34625/issn.2183-2705(29)2021.ic-04

Secção I

Investigação Científica*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review*.

Direito do Ciberespaço e Segurança Cibernética

CyberLaw and CyberSecurity

Jorge Bacelar GOUVEIA[1]

RESUMO: A nova realidade do Ciberespaço, por definição global e a-territorial, não é apenas um novo ambiente da atividade humana, mas requer sobretudo uma adaptação do Direito que se lhe aplica – o Direito do Ciberespaço – com a especiosa preocupação de disciplinar as atividades nele exercidas, avultando a segurança tanto das pessoas que o usam como das instituições que, por sua causa, podem tornar-se mais vulneráveis em relação às novas ameaças e riscos que o mesmo potencia.
PALAVRAS-CHAVE: Ciberespaço; Segurança; Riscos; Direito.

ABSTRACT: Cyberspace, with global and non-territorial dimensions, is not only a recente arena for human activities, but, above all, requires the development of a new branch of Law – Cyberlaw – with the special purpose to protect citizens and organisations against more powerfull threats, obliging the improve of legislation in order to better face them.
KEYWORD: Cyberspace; Protection; Treats; Cyberlaw.

1. CiberEspaço, CiberDireito e CiberSegurança

I. A *segurança cibernética* – ou a *cibersegurança* – *significa a proteção que se realiza no ciberespaço contra as ameaças a valores ou direitos da comunidade política, assim perpetrados neste novo ambiente digital.*

Não é inequívoca a localização da segurança cibernética no quadro da segurança nacional, com a confluência de múltiplas dimensões, quer nos intervenientes públicos e privados, quer na intensidade e proveniência das ameaças em causa[2].

---

[1] Advogado, Jurisconsulto e Professor Catedrático da Faculdade de Direito da Universidade NOVA de Lisboa/NOVA School of Law e da Universidade Autónoma de Lisboa. Presidente do Instituto de Direito e Segurança e Diretor da *Revista de Direito e Segurança*. Investigador do CEDIS – Centro de Investigação & Desenvolvimento sobre Direito e Sociedade e do CIDES – Centro de Investigação & Desenvolvimento sobre Direito e Segurança. Orcid ID: Orcid.org/0000-0003-1377-3179; Ciência ID – 801F-90C2-EFD9. www.jorgebacelargouveia.com. E-mail: jorgebacelargouveia@live.com.

[2] Sobre estes conceitos e a cibersegurança em geral, bem como as suas complexidades e contradições, v. LOUIS COUFFIGNAL, *La Cybernétique*, Paris, 1963, pp. 5 e ss.; MARIA EDUARDA GONÇALVES, *Direito da Informação*, Coimbra, 1994, pp. 137 e ss.; SOLANGE GHERNAOUTI-HÉLIE, *Cybercriminalité et sécurité intérieure: état des lieux et éléments de*

Segundo LINO SANTOS, "…a cibersegurança pode ser vista a partir de duas perspetivas, independentemente de o objeto da cibersegurança ser o Estado, as organizações ou os indivíduos: a segurança do ciberespaço (na aceção física deste como entidade autónoma) e a segurança da componente "ciber" de um qualquer sistema (segurança do ciberespaço desse sistema)"[3].

II. O ponto de partida é a nova realidade do *Ciberespaço*, *no qual se cruzam, graças às tecnologias digitais, intervenções públicas e privadas, novo espaço de aproximação, mas também novo espaço de conflito.*

Como refere LINO SANTOS, "O ciberespaço apresenta algumas características distintivas. Desde logo, aumenta radicalmente a velocidade e a quantidade das comunicações, ao mesmo tempo que reduz ou elimina a distância entre instituições, entre indivíduos ou mesmo entre nações. Por outro lado, o ciberespaço é aterritorial. (…) Outra característica deste espaço virtual diz respeito à possibilidade de realização de ações de forma praticamente

prévention, in AAVV, *Traité de Sécurité Intérieure* (sob a direção de MAURICE CUSSON, BENOÎT DUPONT e FRÉDÉRIC LEMIEUX), Lausanne, 2008, pp. 246 e ss.; PAULO VIEGAS NUNES, *O Vetor Estratégico "Informação e Segurança do Ciberespaço"*, in AAVV, *Contributos para um Conceito Estratégico de Defesa Nacional* (coordenação de ANTÓNIO FIGUEIREDO LOPES, NUNO SEVERIANO TEIXEIRA e VÍTOR RODRIGUES VIANA), Lisboa, 2012, pp. 165 e ss.; JULIAN ASSANGE, *Liberdade e o futuro da Internet – Cypherpunks*, São Paulo, 2012, pp. 25 e ss.; JOÃO MANUEL DIAS MOREIRA, *O impacto do Ciberespaço como nova dimensão nos conflitos*, in *Boletim do IESM – Instituto de Estudos Superiores Militares*, nº 13, novembro de 2012, pp. 27 e ss.; VICENTE FREIRE e ALEXANDRE CALDAS, *O Ciberespaço: desafios à Segurança e à Estratégia*, in AAVV, *Segurança Internacional – perspetivas analíticas* (coordenação de ISABEL FERREIRA NUNES), Lisboa, 2013, pp. 81 e ss.; LINO SANTOS, *Contributos para uma melhor Governação da Cibersegurança em Portugal,* in AAVV, *Estudos de Direito e Segurança* (coordenação de JORGE BACELAR GOUVEIA), II, Coimbra, 2012, pp. 217 e ss., *Ciberespaço*, in AAVV, *Enciclopédia de Direito e Segurança* (coordenação de JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra, 2015, pp. 60 e ss., e *Cibersegurança*, in AAVV, *Enciclopédia de Direito e Segurança* (coordenação de JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra, 2015, pp. 63 e ss.; ALEXANDRE SOUSA PINHEIRO, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, 2015, pp. 64 e ss.; EMMANUEL DUPIC, *Droit de la Sécurité Intérieure*, Paris, 2014, pp. 246 e ss.; JOSÉ PEDRO TEIXEIRA FERNANDES, *Ciberguerra: quando a utopia se transforma em realidade,* Editor Quidnovi, 2014, pp. 67 e ss.; MARIA LUÍS BARBOSA, *As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal,* in *Revista de Direito e Segurança*, ano, IV, nº 8, Lisboa, julho-dezembro de 2016, pp. 163 e ss.; ANDRÉ BARRINHA e HELENA CARRAPIÇO, *Cibersegurança*, in AAVV, *Segurança Contemporânea* (coordenação de RAQUEL DUQUE, DIOGO NOIVO e TERESA DE ALMEIDA E SILVA), Lisboa, 2016, pp. 245 e ss.; AAVV, *Ciberseguridad – la protección de la información en un mundo digital*, Madrid/Barcelona, 2016, pp. 1 e ss.; JORGE BACELAR GOUVEIA, *Direito da Segurança*, 2ª ed., Coimbra, 2020, pp. 951 e ss.

[3] LINO SANTOS, *Cibersegurança*, p. 63.

anónima, o que levanta, novamente, dificuldades quanto à atribuição dos atos praticados ou à identificação dos seus autores"[4].

Assim se justifica falar de um *Direito do Ciberespaço*, representando o setor da Ordem Jurídica que disciplina a utilização das tecnologias digitais em vista da necessidade de adaptar ou estabelecer um dever-ser específico a essa realidade.

O Direito do Ciberespaço é um subsistema jurídico, com dimensões pública e privada, que visa não apenas regular o uso das novas tecnologias digitais, atendendo à sua novidade e aos novos desafios que elas corporizam, mas também regular as atividades que ocorrem no ciberespaço, considerando a mutação a que as mesmas se sujeitam por força desse ambiente virtual, simultaneamente na defesa das pessoas e das instituições.

III. O Direito do Ciberespaço já é uma realidade complexa, multiplicando-se os capítulos por que o mesmo se vai densificando, à medida que crescem as matérias tratadas em razão da necessidade de atender aos desafios impostos pelo mundo digital[5].

Eis algumas dessas matérias:

- o regime das comunicações eletrónicas;

- o regime do comércio eletrónico;

- a proteção dos direitos fundamentais no mundo digital;

- a punição dos comportamentos que surjam no mundo digital.

IV. O Direito do Ciberespaço está longe de ser uma realidade nacional, só sendo útil numa dimensão transnacional, com a importância de a União Europeia ter recentemente promanado três relevantes diplomas legislativos:

- *o Regulamento Geral sobre Proteção de Dados* (RGPD), aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016;

- *a Diretiva sobre o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de*

[4] LINO SANTOS, *Ciberespaço*, p. 63.

[5] Quanto às questões que se suscitam no Direito do Ciberespaço, v. DÁRIO MOURA VICENTE, *Problemática Internacional da Sociedade da Informação*, Coimbra, 2005, pp. 83 e ss.

infrações penais ou execução de sanções penais, aprovada pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016; e

- *a Diretiva relativa à utilização dos dados pessoais dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave*, aprovada pela Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho.

V. Em termos nacionais, a legislação é dispersa, sendo essencialmente de mencionar a nova *Lei de Proteção de Dados Pessoais*, editada na sequência daquele novo regulamento comunitário, em conjunto com dois outros diplomas:

- *a Lei da Execução do Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no tocante ao tratamento de dados pessoais, bem como à livre circulação desses dados* (Lei nº 58/2019, de 8 de agosto);

- *o Regime da Transferência dos Dados dos Registos de Identificação dos Passageiros* (Lei nº 21/2019, de 25 de fevereiro);

- *o Regime do Tratamento de Dados Pessoais para efeitos de Prevenção, Deteção, Investigação ou Repressão de Infrações Penais ou de Execução de Sanções Penais* (Lei nº 59/2019, de 8 de agosto);

- *o Regime Jurídico da Segurança do Ciberespaço* (Lei nº 46/2018, de 13 de agosto).

VI. Mais recentemente, é de frisar a importância da *Carta Portuguesa de Direitos Humanos na Era Digital*, aprovada pela Lei nº 27/2021, de 17 de maio, um conjunto de 23 artigos que inclui tanto normas de intensidade diversa – oscilando entre o precetivo e o programático – como disposições que se aplicam às dimensões individuais e coletivas da comunidade política, sem excluir a atividade jurídico-privada, nos seguintes termos:

- Artigo 1º - *Objeto*
- Artigo 2º - *Direitos em ambiente digital*
- Artigo 3º - *Direito de acesso ao ambiente digital*
- Artigo 4º - *Liberdade de expressão e criação em ambiente digital*
- Artigo 5º - *Garantia de acesso e uso*
- Artigo 6º - *Direito à proteção contra a desinformação*

- Artigo 7º - *Direitos de reunião, manifestação, associação e participação em ambiente digital*

- Artigo 8º - *Direito à privacidade em ambiente digital*

- Artigo 9º - *Uso da inteligência artificial e de robôs*

- Artigo 10º - *Direito à neutralidade da Internet*

- Artigo 11º - *Direito ao desenvolvimento de competências digitais*

- Artigo 12º - *Direito à identidade e outros direitos pessoais*

- Artigo 13º - *Direito ao esquecimento*

- Artigo 14º - *Direitos em plataformas digitais*

- Artigo 15º - *Direito à cibersegurança*

- Artigo 16º - *Direito à liberdade de criação e à proteção dos conteúdos*

- Artigo 17º - *Direito à proteção contra a geolocalização abusiva*

- Artigo 18º - *Direito ao testamento digital*

- Artigo 19º - *Direitos digitais face à Administração Pública*

- Artigo 20º - *Direito das crianças*

- Artigo 21º - *Ação popular digital e outras garantias*

- Artigo 22º - *Direito transitório*

- Artigo 23º - *Entrada em vigor*

VII. Focando estas linhas naquilo que diz respeito ao Direito da Cibersegurança, salientando-se neste escrito sobretudo a segurança comunitária, são dois os tópicos fundamentais a considerar:

- por um lado, *a proteção dos direitos fundamentais das pessoas frente ao uso da informática*, proverbialmente antecipado pela CRP logo em 1976, assunto que se reforçou com a nova legislação europeia e interna aprovada;

- por outro lado, *a proteção da comunidade política que seja empreendida através de estruturas de segurança nacional dedicadas a combater a ciberameaças*, as quais podem assumir uma variedade apreciável.

2. A proteção dos dados pessoais informatizados pelos direitos fundamentais em geral

I. *A primeira vertente é a da proteção dos dados pessoais informatizados, assunto que mereceria uma extrema relevância constitucional,*

numa altura em que a utilização das tecnologias digitais dava os seus primeiros passos[6].

Beneficiando de algumas revisões constitucionais, o texto que a atual versão da CRP tem sobre a matéria continua a ser, a vários títulos, modelar, prescrevendo-se o seguinte:

Artigo 35° – **Utilização da informática**

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

[6] Quanto ao regime da proteção de dados, em especial a partir do art. 35º da CRP, v. MARIA EDUARDA GONÇALVES, *Direito*…, pp. 82 e ss.; ALEXANDRE SOUSA PINHEIRO, *Privacy e proteção*…, pp. 665 e ss.; MARIA PAULA RIBEIRO DE FARIA, *Anotação ao Artigo 35º*, in AAVV, *Constituição Portuguesa anotada* (organização de JORGE MIRANDA e RUI MEDEIROS), I, 2ª ed., Lisboa, 2017, pp. 565 e ss.

7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

II. O que de essencial se retira destas disposições constitucionais é a afirmação de um *feixe de direitos fundamentais perante o uso da informática*, os quais podem beneficiar de uma dogmática geral, em que se deve frisar:

- os titulares[7]*;*

- o objeto; e

- o regime.

III. Em matéria de *titularidade dos direitos*, são duas as questões que se suscitam, a partir da referência direta que o texto da CRP faz aos "cidadãos", na dúvida relativa à sua pertinência exclusiva a pessoas físicas de cidadania portuguesa e a titularidade por parte de pessoas coletivas.

No que toca à primeira questão, vigora o princípio constitucional da equiparação, pelo qual os estrangeiros e os apátridas beneficiam dos mesmos direitos – inclusive direitos fundamentais – atribuídos aos portugueses (cfr. o art. 15.º, n.º 1, da CRP), concluindo-se pela sua atribuição a essas categorias de pessoas, não se estando perante nenhuma das exceções relacionadas com direitos políticos, funções públicas que não tenham caráter predominantemente técnico ou direitos reservados a portugueses (cfr. o art. 15.º, n.º 2, da CRP)

Quanto à outra interrogação, a resposta é mais difícil, *prima facie* vista seria pouco compatível com o fundamento destes direitos fundamentais, virados para a proteção da privacidade, a sua atribuição a pessoas coletivas.

Contudo, já se tem reconhecido às pessoas coletivas direitos fundamentais desta índole, como os relacionados com a inviolabilidade do sigilo da correspondência e do domicílio, e neste caso parecendo que há interesses dignos de tutela que justificam a sua titularidade por parte destas pessoas jurídicas, em aplicação da outra vertente do princípio constitucional da universalidade (cfr. o art. 12.º, n.º 2, da CRP).

[7] Em relação com este tema, também se poderia apreciar em que termos as pessoas jurídicas em geral se encontram vinculadas a estes direitos. A resposta deve ser a de considerar a sua vinculatividade geral.

IV. A dilucidação do sentido dos "dados pessoais informatizados" objeto destes direitos decorre, na sua quase totalidade, do próprio texto constitucional.

Pode assim decompor-se em três elementos constitutivos[8]:

- por um lado, trata-se de um conjunto de informações ou de conhecimentos que retratam certo facto ou situação;
- por outro lado, essas informações – ou dados – são referidas a pessoas, não a realidades não humanas, mas têm de ser identificadas ou identificáveis por relação com essas pessoas;
- por fim, estes direitos só fazem sentido enquanto dirigidos a dados pessoais alvo de um tratamento informatizado, por recurso à técnica informática, não através de outros instrumentos de trabalho ou processamento[9].

V. A inserção destes direitos fundamentais no capítulo I do título II da parte I da CRP, dedicado aos "Direitos, liberdades e garantias pessoais", bem como o caráter precetivo das normas que os atribuem, determinam a aplicação do regime específico dos direitos, liberdades e garantias.

3. Os direitos fundamentais à proteção dos dados pessoais informatizados em especial e o seu elevado mérito

I. A observação dos direitos fundamentais à proteção dos dados pessoais informatizados em especial faz realçar a existência de *quatro tipos de direitos*, todos eles distintos a partir do respetivo conteúdo, ou seja, tomando por base a utilidade que conferem ao titular relativamente ao objeto sobre que incidem.

São eles[10]:

- *o direito ao controlo dos dados pessoais informatizados;*
- *o direito à não difusão dos dados pessoais informatizados;*

[8] JORGE BACELAR GOUVEIA, *Os direitos fundamentais à proteção dos dados pessoais informatizados,* in *Revista da Ordem dos Advogados*, III, Lisboa, dezembro de 1991, pp. 714 e 715.

[9] Pode pensar-se, porém, por via de um raciocínio analógico, na necessidade de alargar esta proteção também aos ficheiros manuais, na medida em que possam pôr em causa as liberdades fundamentais da pessoa.

[10] Cfr. JORGE BACELAR GOUVEIA, *Os direitos fundamentais à proteção…,* pp. 717 e ss.

- *o direito à proibição do tratamento informatizado dos dados pessoalíssimos;* e
- *a garantia da não atribuição de um número nacional único.*

II. O primeiro (cfr. o art. 35º, nº 1, da CRP) desdobra-se em quatro faculdades de intervenção sobre os dados pessoais informatizados:

- o poder de conhecer o seu teor;

- o poder de conhecer a finalidade do seu armazenamento;

- o poder de exigir a sua retificação; e

- o poder de exigir a sua atualização.

III. O segundo (cfr. o art. 35º, nº 4, da CRP) reparte-se por duas vertentes distintas:

- *a vertente subjetiva visa impedir a divulgação do teor dos dados pessoais informatizados a terceiros*, garantindo-se assim a confidencialidade dos mesmos;

- *a vertente objetiva destina-se a evitar o cruzamento da informação entre diferentes ficheiros*, por forma a não permitir a formação de um retrato informatizado global acerca da pessoa.

IV. O terceiro (cfr. o art. 35º, nº 3, da CRP) tem por conteúdo a proibição, pura e simples, de se realizar o tratamento informatizado de certas categorias de dados – dados que se apelida de "pessoalíssimos".

A tipologia que é apresentada, pela delicadeza do assunto, só pode considerar-se taxativa[11].

V. O quarto, que é uma garantia (cfr. o art. 35º, nº 5, da CRP), destina-se a impedir a adoção de uma chave identificadora comum, o que tornaria mais fácil o acesso à informação[12].

[11] Neste sentido, JORGE BACELAR GOUVEIA, *Os direitos fundamentais à proteção...,* pp. 725 e 726.

[12] A atribuição de um número nacional único poderia acarretar não só um perigo de ordem política como um risco de perda de individualidade. Salienta, a este propósito, PEDRO SOARES MARTÍNEZ *(Comentários à Constituição Portuguesa de 1976,* Lisboa, 1978, p. 52): "Entende-se bem que, *brevitatis causa,* no plano escolar, na vida militar, para efeitos fiscais, para muitos outros, a cada indivíduo correspondam números. Mas estes, embora plurais,

O número nacional único entende-se como um código informático, que possa refletir as várias facetas da pessoa em termos de tratamento informatizado dos seus dados pessoais.

VI. A avaliação a fazer da proteção que a CRP preconiza quanto à utilização da informática é bastante positiva, sublinhando-se quatro notas mais significativas[13].

Em primeiro lugar, *é de salientar a própria tipificação de vários direitos fundamentais no tratamento informatizado dos dados pessoais informatizados*. O texto constitucional podia ter ficado apenas numa regulação vaga, de orientação geral do legislador ordinário. Não foi, contudo, o que sucedeu; quis-se ir mais além e apresentar uma panóplia de direitos a cobrir, com a eficácia que é reconhecida à técnica dos direitos fundamentais dentro do ordenamento jurídico, todo um vasto leque de situações[14].

Não deixa de ser louvável também a precisão e pormenorização alcançada na positivação desses direitos. Os conceitos constitucionais utilizados, longe de indeterminados, têm um elevado grau de concisão, o que só reforça a garantia oferecida aos respetivos titulares, não dependentes assim de valorações legislativas ou jurisdicionais.

De referir ainda que a existência de remissões constitucionais para a lei foi reduzida ao mínimo e note-se que, em grande medida, a liberdade de conformação do legislador é meramente aparente.

Por fim, *o estatuto constitucional destes direitos fundamentais sai reforçado ao ser-lhes aplicável o regime particularmente sólido privativo dos direitos, liberdades e garantias.*

---

sectoriais, não devem utilizar-se em termos de contribuírem para qualquer apagamento da personalidade. Importa que, a todo o momento, a cada número se possa fazer corresponder elementos de personalização – um nome, uma filiação, uma naturalidade, um estado civil".

[13] Pode mesmo dizer-se – sem qualquer laivo nacionalista – que a CRP é o documento constitucional mais aperfeiçoado na proteção conferida à pessoa relativamente à utilização da informática.

[14] Como se pôde observar a propósito da referência a cada uma dessas posições subjetivas existentes neste domínio.

4. A proteção dos dados pessoais no Direito Legal e no Direito da União Europeia

I. A regulação constitucional do uso da informática não se queda por aqui: *aponta para uma dimensão institucional, ao fixar orientações para que organismos dotados de poder público possam fazer a regulação da atividade que implica a compressão de direitos fundamentais através do uso da informática.*

É assim que se estabelece a Comissão Nacional de Proteção de Dados (CNPD), que ao abrigo da sua lei estatutária, tem as competências para intervir como autoridade independente, disciplinando a atividade neste setor, mas também fiscalizando e impondo sanções contra a violação das regras aplicáveis[15].

Há bem pouco tempo, estas matérias passaram a beneficiar de um amplo desenvolvimento trazido pela *Carta Portuguesa de Direitos Humanos na Era Digital*, a qual, embora não tivesse inovado substancialmente e se assuma com uma feição essencialmente programática, tem um notável alcance de acrescentar novos direitos e colocar na agenda legislativa o tratamento de certos assuntos, como é o caso das "fake news".

II. O Direito da União Europeia tem dado significativos passos nesta matéria, confirmando tudo o que a CRP conseguiu antecipar 40 anos antes e numa altura em que nem sequer havia o uso generalizado das tecnologias digitais.

É desde logo de mencionar na Carta de Direitos Fundamentais da União Europeia o reconhecimento do *direito fundamental à proteção de dados pessoais*: "Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito" (art. 8º, nº 1, da CDFUE e também art. 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia).

[15] Além de se poder perspetivar a relação da proteção de dados pessoais com a segurança nacional, como se analisa na obra coletiva AAVV, *Protection des donnés personnelles et Sécurité nationale – quelles garanties juridiques dans l'utilisation du numérique?* (sob a coordenação de ODILE DE DAVID BEAUREGARD-BERTHIER e AKILA TALEB-KARLSSON), Bruxelles, 2017, pp. 15 e ss.

Depois também se deve referir *o fortalecimento da proteção do uso de tais dados pessoais que se obteve com o Regulamento Geral sobre Proteção de Dados*, especialmente o direito ao apagamento dos dados (cfr. os arts. 12º e seguinte do RGPD), o que configura um novo direito fundamental atípico, constitucionalmente relevante para efeito do art 16º, nº 1, da CRP[16].

5. O combate às ciberameaças: a Estratégia Nacional de Segurança do Ciberespaço e a Orientação Política para a Ciberdefesa

I. *Se a cibersegurança tem uma indiscutível dimensão individual, não deixa de ostentar uma proteção institucional contra as ameaças aos valores da comunidade política que sejam perpetrados no ciberespaço, as quais tomam o nome de ciberameaças.*

O desenvolvimento das tecnologias do mundo digital tem vindo a multiplicar a variedade dessas ciberameaças, as quais atingem vários alvos e obrigando a paralelas respostas por parte das estruturas de segurança nacional.

II. É viável elaborar uma taxonomia que considere esses tipos de ciberameaça à segurança nacional, que pode assumir a veste de uma cibersegurança nacional:

- *a ciberguerra*, que se traduz na realização de ataques armados contra alvos digitais, ou que se socorre das tecnologias digitais para a realizar, como o uso de veículos não tripulados;

- *o ciberterrorismo*, que se materializa na realização de ataques terroristas contra alvos civis com a utilização de tecnologias digitais;

- *a ciberespionagem*, que se consuma em ações de espionagem que utilizam a infiltração nos meios digitais, acedendo a informação de Estado;

[16] Quanto às questões que neste âmbito se têm suscitado, v. MARIA EDUARDA GONÇALVES, *The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward*, in *Information & Communications Technology Law*, 2017, pp. 1 e ss.

- *o cibercrime*, em que se comete crimes no contexto das tecnologias digitais, contra o qual se aprovou a *Lei do Cibercrime*, constante da Lei nº 109/2009[17], de 15 de setembro[18].

III. Portugal tem vindo a despertar para a importância da proteção do ciberespaço, tomando medidas que permitem enfrentar as ameaças que sobre o mesmo impendem, reduzindo as suas vulnerabilidades.

Foi pela primeira vez definida a *Estratégia Nacional de Segurança do Ciberespaço* (ENSC-2015)[19] pela Resolução do Conselho de Ministros nº 36/2015, de 12 de junho, a qual "…funda-se no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (nº 1 da ENSC-2015).

A preocupação que se traduziu na elaboração da ENSC-2015 era sublinhada no seu preâmbulo, ao dizer-se que "…é fundamental que o País disponha de uma Estratégia Nacional de Segurança do Ciberespaço, que estabeleça 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" (parágrafo 10 do preâmbulo da ENSC-2015).

Os objetivos da ENSC-2015 eram bem o exemplo da ambivalência da cibersegurança *na proteção das pessoas e das instituições*:

"a) Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;

---

[17] Sobre a Lei do Cibercrime, v. PEDRO VERDELHO, *Lei do Cibercrime*, in AAVV, *Enciclopédia de Direito e Segurança* (coordenação de JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra, 2015, pp. 255 e ss.; PEDRO LEDO, *O cibercrime – o fenómeno e meios de obtenção de prova*, in AAVV, *Segurança e Defesa* (coordenação de JOSÉ MANUEL ANES), Lisboa, 2020, pp. 123 e ss.

[18] De frisar também a criação, na Polícia Judiciária, da Unidade Nacional de Investigação da Criminalidade Informática, nos termos da Lei nº 103/2015, de 24 de agosto, objeto de explicitação pelo Decreto-Lei nº 81/2016, de 28 de novembro, que a rebatizou com o nome Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

[19] Sobre a Estratégia Nacional para a Segurança do Ciberespaço, v. MARIA LUÍS BARBOSA, *As ameaças ao ciberespaço*…, pp. 180 e ss.

b) Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;

c) Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;

d) Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação" (nº 3 da ENSC-2015).

IV. Entretanto, a ENSC-2015 – mercê do amadurecimento dos conhecimentos alcançados e da prática obtida, por junto com o *Regime Jurídico da Segurança do Ciberespaço* aprovado em 2018 – foi substituída pela *Estratégia Nacional de Segurança do Ciberespaço para o quadriénio 2019-2023* (ENSC/2019-2023), aprovada pela Resolução do Conselho de Ministros nº 92/2019, de 5 de junho, esta orientando-se agora por *três princípios*:

a) *Princípio da subsidiariedade*: "Portugal afirma o seu forte compromisso com a segurança do ciberespaço. Considerando que grande parte das infraestruturas tecnológicas que compõem o ciberespaço é detida por entidades do setor privado, cabe a estas a responsabilidade primária pela sua proteção. Esta responsabilidade inicia-se no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais";

b) *Princípio da complementaridade*: "A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, coletivos ou individuais. Uma abordagem inclusiva, alargada e integradora da segurança do ciberespaço exige diferentes responsabilidades e capacidades, para benefício do interesse comum", sendo certo que "A interdependência das infraestruturas tecnológicas, e a consequente probabilidade de propagação dos impactos resultantes de incidentes, requer uma atuação complementar e confiável, assente na consciência do dever de cooperação reforçado entre as estruturas e entidades nacionais, atentas às referidas dependências por forma a maximizar a proteção e a resiliência digital.";

c) *Princípio da proporcionalidade*: "A segurança do ciberespaço resulta também de um exercício complexo, verificável e contínuo, de avaliação dos riscos associados ao ecossistema digital. Em consequência, a adequação e a alocação de recursos deve ser proporcional aos riscos identificados e à

execução das linhas de ação constantes da presente Estratégia" (nº 1 da ENSC/2019-2023).

V. A concretização da ENSC-2019/2023 assenta em *seis eixos fundamentais*, a saber:

- *Eixo 1 – Estrutura de segurança do ciberespaço*: "A complexidade e a abrangência dos desafios da segurança do ciberespaço requerem uma liderança e governação forte e transversal, uma coordenação operacional ágil, célere e eficaz, uma capacidade de resposta e salvaguarda dos interesses nacionais e, acima de tudo, uma envolvência de recursos, conhecimentos e competências";

- *Eixo 2 – Prevenção, educação e sensibilização*: "No âmbito da prevenção, importa salvaguardar o papel fundamental da partilha de informação na avaliação precoce da ameaça";

- *Eixo 3 – Proteção do ciberespaço*: "A segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o regular funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço";

- *Eixo 4 – Resposta às ameaças e combate ao cibercrime*: "A segurança nacional do ciberespaço alicerça-se igualmente na sua capacidade de edificação de mecanismos de dissuasão" e a "A realização de tal desiderato passa pela capacitação das entidades responsáveis pela segurança do ciberespaço de mecanismos defensivos e de resposta de modo que qualquer atuação ilícita contra o ciberespaço de interesse nacional seja merecedora de uma ação apropriada";

- *Eixo 5 – Investigação, desenvolvimento e inovação*: "A criação de capacidades tecnológicas no âmbito da segurança no ciberespaço assume-se como fundamental na presente Estratégia para um desenvolvimento sustentado e para a observação pertinente do futuro", pelo que "…pretende-se fortalecer, apoiar e promover o potencial nacional de investigação, desenvolvimento e inovação de processos e tecnologias de vanguarda para a cibersegurança, com base nas capacidades individuais e coletivas do setor público e privado, da academia e da indústria";

- *Eixo 6 – Cooperação nacional e internacional*: "Num mundo altamente interligado e interdependente, a segurança do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais, alicerçada no desenvolvimento de confiança mútua" (nº 5 da ENSC/2019-2023).

6. O Regime Jurídico da Segurança do Ciberespaço

I. Até um certo momento, a efetivação da ENSC de 2015 pouco frutificaria, embora se salientasse, no plano institucional, os seguintes organismos:

- *o Conselho Superior de Segurança do Ciberespaço (CSSC);*
- *o Centro Nacional de CiberSegurança (CNCS);*
- *Organismos específicos nas várias dimensões da segurança nacional*, como é o caso da ciberdefesa e da cibercriminalidade.

II. O CSSC foi criado pela Resolução do Conselho de Ministros nº 115/2017, de 24 de agosto, e consistia, nesse diploma, num "…grupo de projeto (…), que funciona na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar", tendo por missão "…assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional de Segurança do Ciberespaço (ENSC) e da respetiva revisão" (respetivamente, nºs 1 e 2, da Resolução do Conselho de Ministros nº 115/2017).

A sua instituição apoiava-se na necessidade de uma resposta transversal: "A responsabilidade pela segurança do ciberespaço nacional encontra-se distribuída por diferentes entidades com missões e objetivos diversos, sendo, por essa razão, imperioso assegurar a existência de uma abordagem transversal e integradora das variadas sensibilidades, necessidades e capacidades dos diversos setores com intervenção neste âmbito" (parágrafo nº 2 da Resolução do Conselho de Ministros nº 115/2017, de 24 de agosto).

III. Entretanto, ocorreu a aprovação do *Regime Jurídico da Segurança do Ciberespaço* (RJSC) (Lei nº 46/2018, de 13 de agosto), central diploma com 33 artigos e a seguinte sistematização, fixando em *hard law* todo o caminho preparado por aquela resolução governamental:

- Capítulo I – *Disposições gerais*
- Capítulo II – *Estrutura de segurança do ciberespaço*
- Capítulo III – *Segurança das redes e dos sistemas de informação*
- Capítulo IV – *Fiscalização e sanções*
- Capítulo V – *Disposições finais*

Coube a esta lei parlamentar a transposição da Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

7. A estrutura de governo do Ciberespaço em Portugal

I. *A estrutura do governo da Segurança do Ciberespaço passou a assentar na existência de três entidades* (cfr. os art. 5º e ss. do RJSC):

- o Conselho Superior de Segurança do Ciberespaço;

- o Centro Nacional de Cibersegurança, também a Autoridade Nacional de Cibersegurança; e

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

II. O *Conselho Superior de Segurança do Ciberespaço* é o "…órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço" (art. 5º, nº 1, do RJSC), tendo competências consultivas e de acompanhamento na garantia da Segurança do Ciberespaço:

"a) Assegurar a coordenação político-estratégica para a segurança do ciberespaço;

b) Verificar a implementação da Estratégia Nacional de Segurança do Ciberespaço;

c) Pronunciar-se sobre a Estratégia Nacional de Segurança do Ciberespaço previamente à sua submissão para aprovação;

d) Elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da Estratégia Nacional de Segurança do Ciberespaço;

e) Propor ao Primeiro-Ministro, ou ao membro do Governo em quem aquele delegar, a aprovação de decisões de caráter programático relacionadas com a definição e execução da Estratégia Nacional de Segurança do Ciberespaço;

f) Emitir parecer sobre matérias relativas à segurança do ciberespaço;

g) Responder a solicitações por parte do Primeiro-Ministro, ou do membro do Governo em quem aquele delegar, no âmbito das suas competências" [art. 6º, nº 1, als. a) a g), do RJSC].

III. O *Centro Nacional de Cibersegurança* "…tem por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais" (art. 7º, nº 2, do RJSC).

Quanto a este organismo, é de ressaltar o seu lugar de charneira na Segurança do Ciberespaço, uma vez que "…atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à autoridade competente, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes" (art. 7º, nº 7, do RJSC).

IV. Ao nível da Defesa Nacional, é de assinalar a *Orientação Política para a Ciberdefesa*, aprovada pelo Despacho nº 13692/2013, de 11 de outubro de 2013, do Ministro da Defesa Nacional, que "…tem por finalidade determinar os princípios essenciais, definir objetivos e estabelecer as correspondentes linhas orientadoras dos esforços a desenvolver, no âmbito da Defesa Nacional,

visando, nomeadamente, o levantamento da capacidade nacional de Ciberdefesa" (ponto I – 2 da *Orientação Política para a Ciberdefesa*).

Os *objetivos* desta Política de Ciberdefesa ficam claros:

"1) Garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques;

2) Assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional;

3) Contribuir de forma cooperativa para a cibersegurança nacional" (ponto III da *Orientação Política para a Defesa*).

REFERÊNCIAS BIBLIOGRÁFICAS

AAVV, Estudos de Direito e Segurança (coordenação de JORGE BACELAR GOUVEIA), II, Coimbra, 2012.

AAVV, Enciclopédia de Direito e Segurança (coordenação de JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra, 2015.

ALEXANDRE SOUSA PINHEIRO, Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional, Lisboa, 2015

EMMANUEL DUPIC, Droit de la Sécurité Intérieure, Paris, 2014.

JORGE BACELAR GOUVEIA, Direito da Segurança, 2ª ed., Coimbra, 2020.

JOSÉ PEDRO TEIXEIRA FERNANDES, Ciberguerra: quando a utopia se transforma em realidade, Editor Quidnovi, 2014.

MARIA LUÍS BARBOSA, As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal, in Revista de Direito e Segurança, ano, IV, nº 8, Lisboa, julho-dezembro de 2016, pp. 163 e ss.

Data de submissão do artigo: 27/06/2021

Data de aprovação do artigo: 31/07/2021

Edição e propriedade:

Universidade Portucalense Cooperativa de Ensino Superior, CRL

Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto

Email: upt@upt.pt