

**UNIVERSIDADE DO PORTO**  
**FACULDADE DE DIREITO**

**A ERA DIGITAL E O ESTADO DE DIREITO  
DEMOCRÁTICO NA UNIÃO EUROPEIA**

Tiago Filipe Morais da Rocha

Orientação pela Professora Doutora Maria da Graça Jerónimo Enes Ferreira

Dissertação de Mestrado apresentada para efeitos  
de obtenção do grau de Mestre em Ciências  
Jurídico-Políticas pela Faculdade de Direito da  
Universidade do Porto.

Porto e FDUP, outubro de 2020

## RESUMO \ ABSTRACT

A revolução digital, que transformou o mundo numa imensa rede hiperconectada, fez emergir novos perigos mundiais: campanhas de desinformação e manipulação *online* amplificadas com recurso a processos automatizados; um novo ambiente digital dominado pela personalização de conteúdos decorrente de inferências algorítmicas sobre a personalidade dos indivíduos; recolha e uso dos dados pessoais em violação dos direitos de privacidade dos utilizadores; cibercrimes e ciberataques à escala global que erodem a confiança nas instituições e nos processos democráticos. Estes perigos acarretam riscos para o Estado de Direito democrático, que podem ser analisados sob vetores como a liberdade de expressão, a destabilização da esfera pública, a redução do pluralismo, a disrupção dos processos democráticos e a interferência em processos eleitorais. Em última análise, o grande risco que os perigos da Era Digital colocam ao Estado de Direito democrático é a sua captura, ainda que através de processos legítimos, por forças antidemocráticas, o que pode conduzir ao enfraquecimento dos seus princípios básicos, à violação dos direitos fundamentais e/ou a um afastamento do modelo da democracia liberal. Por outro lado, os riscos podem constituir oportunidades de mudança e de transformação do tecido social e político. A Era Digital constitui, num quadro de efetiva gestão do risco digital, uma oportunidade (que não deve ser desperdiçada) para apoiar a democratização e o progresso da sociedade europeia. A este propósito, a União Europeia deve ser encarada como um exemplo de gestão multinível e em rede do risco digital, podendo as suas capacidades de ação servir de inspiração para sistemas globais de governança, únicos capazes de dar resposta à natureza transnacional destes riscos.

/// \\

*The digital revolution, which has transformed the world into an immense hyperconnected network, has brought out new global dangers: online disinformation and manipulation campaigns amplified using automated processes; a new digital environment dominated by the personalization of content resulting from algorithmic inferences about the personality of individuals; collection and use of personal data in violation of users' privacy rights; cybercrimes and cyber-attacks on a global scale that erode trust in democratic institutions and processes. These dangers pose risks to the rule of law and democracy, which can be analyzed under such vectors as freedom of expression, destabilization of the public sphere, reduction of pluralism, disruption of democratic processes and interference in electoral processes. Ultimately, the great risk that the dangers of the Digital Age pose to the democratic rule of law is its capture, even through legitimate processes, by anti-democratic forces, which can lead to the weakening of its basic principles, the violation of fundamental rights and/or a departure from the model of liberal democracy. On the other hand, the risks may constitute opportunities for change and transformation of the social and political fabric. The Digital Age constitutes, within a framework of effective digital risk management, an opportunity (which should not be wasted) to support democratization and progress in European society. In this respect, the EU should be seen as an example of multilevel, networked management of digital risk, and its capacities for action could serve as an inspiration for global systems of governance, the only ones capable of responding to the transnational nature of these risks.*

## SUMÁRIO

|                                                                                                                   |           |
|-------------------------------------------------------------------------------------------------------------------|-----------|
| <b>RESUMO \ ABSTRACT</b>                                                                                          | <b>2</b>  |
| <b>LISTA DE ABREVIATURAS</b>                                                                                      | <b>5</b>  |
| <b>INTRODUÇÃO</b>                                                                                                 | <b>6</b>  |
| <b>PARTE I – A ERA DIGITAL E OS PERIGOS PARA O ESTADO DE DIREITO DEMOCRÁTICO NA UNIÃO EUROPEIA.</b>               | <b>7</b>  |
| CAPÍTULO I – CONSIDERAÇÕES PRELIMINARES. ....                                                                     | 7         |
| Secção I – A Era Digital na Europa e no Mundo.                                                                    | 7         |
| Secção II – Por uma compreensão atualista da teoria do risco: os (novos) riscos (tecnológicos) mundiais.          | 14        |
| Secção III – A União Europeia e o Estado de Direito democrático.                                                  | 16        |
| CAPÍTULO II – QUE PERIGOS? .....                                                                                  | 23        |
| Secção I – Verdade e desinformação.                                                                               | 24        |
| Secção II – Algoritmos, automação, personalização e datificação.                                                  | 37        |
| Secção III – Cibercrime e conteúdos digitais ilegais.                                                             | 50        |
| Secção IV – Novas tecnologias disruptivas.                                                                        | 55        |
| CAPÍTULO III: O ESTADO DE DIREITO DEMOCRÁTICO EM RISCO. ....                                                      | 57        |
| <b>PARTE II – AS OPORTUNIDADES DA «CONSTELAÇÃO DIGITAL» PARA A CONSTITUCIONALIZAÇÃO DA UNIÃO EUROPEIA.</b>        | <b>64</b> |
| CAPÍTULO I – DOS RISCOS ÀS OPORTUNIDADES: OS RISCOS COMO IMPULSIONADORES DO «MOMENTO COSMOPOLITA» PARA AGIR. .... | 64        |
| Secção I – Conceptualizar a «constelação digital».                                                                | 64        |
| Secção II – O mundo em rede necessita de respostas em rede: a gestão do risco digital na União Europeia.          | 70        |
| CAPÍTULO II – O CONSTITUCIONALISMO MULTINÍVEL NA UNIÃO E O PAPEL (POSSÍVEL) DA DEMOCRACIA DIGITAL. ....           | 79        |
| <b>CONCLUSÃO</b>                                                                                                  | <b>93</b> |
| <b>BIBLIOGRAFIA</b>                                                                                               | <b>95</b> |

**Vinte e Três<sup>1</sup>**

*«Abrir a janela, vozes a gritar,  
quero acordar alguém.  
Ter a memória a correr atrás de mim,  
o mundo ainda não parou.*

*Olhar para trás sem medo de morrer,  
não perder o que quero lembrar.  
Deixar cair, para onde vais,  
coisas simples e reais.»*

Esta dissertação, elaborada num período de convulsões, é o resultado direto do tempo (e sobretudo da falta dele), da idade e das pessoas que nos acompanharam. Fosse o tempo (o real e o histórico), a idade e as pessoas outras, certamente que o resultado seria, também ele, muito diverso. Mas o mundo teima em não parar.

Evidentemente, todos os defeitos são da exclusiva responsabilidade do Autor, que, capitalizando o seu nome, pouco sabe e muito mais desconhece.

Quando concluímos este trabalho tínhamos abandonado há pouco a casa dos vinte e três, realmente sentindo que temos a memória a correr atrás de nós, atleta cada vez mais lenta... E porque, muito pleonasticamente, não queremos perder o que precisamos lembrar, deixamos aqui, por palavras, o nosso agradecimento a todos os que povoaram a nossa existência durante este período, certos, todavia, de que muito mais lhes devemos do que estas lacónicas linhas.

Em especial:

*À minha Mãe, por suportar a ausência.*

*Aos meus mais leais amigos, pela maçada de me terem.*

*À Prof. Doutora Graça Enes, pela orientação, e, talvez mais, pela confiança.*

---

<sup>1</sup> NOISERV – *Vinte e Três* [Registo sonoro]; 00:00:00. [S.l.]: [S.n.], 2016. 1 disco (CD).

## LISTA DE ABREVIATURAS

|       |                                                   |
|-------|---------------------------------------------------|
| Art.º | Artigo                                            |
| CDFUE | Carta dos Direitos Fundamentais da União Europeia |
| CE    | Comissão Europeia                                 |
| CEDH  | Convenção Europeia dos Direitos Humanos           |
| CEE   | Comunidade Económica Europeia                     |
| CERN  | Organização Europeia para a Pesquisa Nuclear      |
| d.C.  | Depois de Cristo                                  |
| DUDH  | Declaração Universal dos Direitos Humanos         |
| EEAS  | <i>European Union External Action Service</i>     |
| EFTA  | Associação Europeia de Comércio Livre             |
| ELSJ  | Espaço de liberdade, segurança e justiça          |
| EM    | Estado-membro                                     |
| ENISA | Agência Europeia para a Cibersegurança            |
| EUA   | Estados Unidos da América                         |
| FAQS  | <i>Frequently Asked Questions</i>                 |
| IA    | Inteligência artificial                           |
| IoE   | <i>Internet of Everything</i>                     |
| IoP   | Internet das pessoas                              |
| IoT   | Internet das Coisas                               |
| IRA   | <i>Internet Research Agency</i>                   |
| MUD   | Mercado Único Digital                             |
| NATO  | Organização do Tratado do Atlântico Norte         |
| ONU   | Organização das Nações Unidas                     |
| PC    | Computador pessoal                                |
| PE    | Parlamento Europeu                                |
| PESC  | Política Externa e de Segurança Comum             |
| PME   | Pequenas e médias empresas                        |
| Séc.  | Século                                            |
| SMS   | <i>Short Message Service</i>                      |
| TEDH  | Tribunal Europeu dos Direitos do Homem            |
| TFUE  | Tratado sobre o Funcionamento da União Europeia   |
| TIC   | Tecnologias de informação e comunicação           |
| TJUE  | Tribunal de Justiça da União Europeia             |
| TPI   | Tribunal Penal Internacional                      |
| TUE   | Tratado da União Europeia                         |
| UE    | União Europeia                                    |
| UIT   | União Internacional das Telecomunicações          |
| URSS  | União das Repúblicas Socialistas Soviéticas       |

## INTRODUÇÃO

Quando PLÍNIO, O VELHO, termina a sua *História Natural*, descreve o ferro, cuja fundição se revelou um avanço crucial para as Civilizações Antigas<sup>2</sup>, de forma semelhante àquela que hoje podemos usar para descrever a Era Digital. Diz o naturalista que o ferro é, simultaneamente, «*a ferramenta mais útil e mais fatal nas mãos da Humanidade*»<sup>3</sup>. Este exemplo remoto tem a virtualidade de nos lembrar que quase sempre a evolução tecnológica apresenta-se multifacetada, ora potenciando o que de melhor tem uma sociedade, ora despoletando, amplificando ou acelerando processos danosos. De facto, e conforme afirma a primeira Lei de Kranzberg, «*a tecnologia não é [em si mesma] nem boa, nem má; mas também não é neutra*»<sup>4</sup>, o que remete para a imprevisibilidade das consequências sociais, políticas e económicas dos avanços tecnológicos. Sem prejuízo, é de evitar uma visão excessivamente determinista que sustenta que só a tecnologia, que já se encontra para lá do controlo humano, orienta as nossas vivências comuns<sup>5</sup>. Antes, os fatores sociais, culturais e económicos influenciam a direção, a velocidade e as consequências da inovação tecnológica<sup>6</sup>, pelo que, mais corretamente, podemos dizer que a tecnologia molda os processos sociais e, vice-versa, a sociedade define os usos e aplicações das ferramentas e inovações tecnológicas.

Bebendo da ideia de que a tecnologia nunca é neutra, este trabalho procura explorar os *riscos*, decompostos em *perigos* e *oportunidades* (senão *possibilidades*) que os últimos desenvolvimentos da Era Digital representam para dois valores fundacionais da UE: a democracia e o Estado de Direito (art.º 2.º TUE). Assumimos, desde já, a impossibilidade de cobrir sequer uma parte significativa desses desenvolvimentos, quer por limitações de espaço e tempo, quer graças à imensidão e constante evolução do objeto de estudo. Assim, focar-nos-emos em perigos como a desinformação, a personalização de conteúdos por via dos algoritmos, a datificação, o cibercrime e os conteúdos digitais ilegais, procurando daí extrair os riscos que se colocam ao Estado de Direito e à democracia, concluindo, depois, pelas oportunidades que esses mesmos riscos representam para a arquitetura da União e da democracia global.

<sup>2</sup> Para mais desenvolvimentos vide DANIEL R. HEADRICK - *Technology: A World History*. New York: Oxford University Press, Inc., 2009. p. 35 e ss.

<sup>3</sup> PLÍNIO, O VELHO; BOSTOCK, John; RILEY, Henry T; MAYHOFF, Karl Friedrich Theodor - *Pliny the Elder, The Natural History*, Livro XXXIV, Cap. 39.

<sup>4</sup> KRANZBERG, Melvin - *Technology and History: "Kranzberg's Laws"*. Technology and Culture. Vol. 27. n.º 3 (1986). p. 545.

<sup>5</sup> Cfr., entre outros, WINNER, Langdon - *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Massachusetts: The MIT Press, 1977.

<sup>6</sup> WILLIAMS, Robin; EDGE, David - *The Social Shaping of Technology*. Research Policy. Vol. 25. (1996). p. 856-899.

## PARTE I – A ERA DIGITAL E OS PERIGOS PARA O ESTADO DE DIREITO DEMOCRÁTICO NA UNIÃO EUROPEIA.

### CAPÍTULO I – CONSIDERAÇÕES PRELIMINARES.

#### Secção I – A Era Digital na Europa e no Mundo.

Antes de iniciarmos a análise dos perigos da Era Digital em que vivemos, convém, em leves traços, responder à questão de saber como é que chegamos até aqui. A esse respeito, a maioria dos académicos concorda que a inovação tecnológica<sup>7</sup> nunca *surge* isolada, estando sempre interconectada com vários processos evolutivos que se autoalimentam. Assim, as inovações estão «*historicamente relacionadas com os longos ciclos de desenvolvimento económico*»<sup>8</sup>. No início dos anos 90 a computação, as telecomunicações e a Era da Informação já podiam reclamar, devido, essencialmente, «à sua capacidade de penetrabilidade em todas as esferas da atividade humana»<sup>9</sup>, um potencial transformativo imenso. Note-se que, terminologicamente, não adotamos nenhuma posição fundamentalista, pelo que as expressões *Era Digital*, *Era da Informação*, *revolução digital*, *sociedade digital* e *sociedade informacional* vão aqui usadas como tradutoras do mesmo paradigma fundamental<sup>10</sup>. Quando falamos da Era Digital falamos, também, senão sobretudo, da revolução da comunicação humana ocorrida no último século e meio. Apesar dos avanços que representaram, a imprensa escrita, o telégrafo, o telefone, o rádio e a televisão, todos sofriam de uma limitação ou outra, ora porque permitiam que entre dois utilizadores se estabelecesse uma ligação direta (telégrafo e telefone), ora porque possibilitavam que um emissor conseguisse, ao mesmo tempo, chegar a vários milhares ou milhões de recetores (rádio e televisão). Nenhuma tecnologia, contudo, permitia as duas coisas de uma só vez: até que a *internet* nasceu. Para a invenção da *internet* foi crucial, antes de mais, o desenvolvimento da ciência da computação e do seu melhor invento: o computador<sup>11</sup>. Os

<sup>7</sup> Não sendo este o espaço indicado para uma discussão em torno da definição de *tecnologia*, que funciona, tantas vezes, como um termo *catch-all*, aderimos à noção ampla de quem a entende como o desenvolvimento e aplicação de ferramentas, máquinas, materiais e processos que auxiliam a resolução de problemas humanos.

<sup>8</sup> EVANGELIDIS, Basil - *Landmarks in the History of Science: Great Scientific Discoveries from a Global-Historical Perspective*. Delaware: Vernon Press, 2019. cap. 6.4.

<sup>9</sup> CASTELLS, Manuel - *A Era da Informação: Economia, Sociedade e Cultura*. 3.<sup>a</sup> ed. Lisboa: Fundação Calouste Gulbenkian, 2007. Vol. I – A Sociedade em Rede. p. 5.

<sup>10</sup> Aliás na esteira do que faz o Dicionário de Cambridge ([vide https://dictionary.cambridge.org/dictionary/english/digital-age](https://dictionary.cambridge.org/dictionary/english/digital-age)). Reconhecemos, não obstante, que os termos não contêm entre si uma sinonímia completa. Por exemplo, existem diferenças analíticas entre “sociedade de informação” e “sociedade informacional” ou “Era da informação” e “Era informacional”, uma vez que as primeiras designações apontam mais para o papel da informação na sociedade, ao passo que as segundas são referentes a um atributo específico da organização social presente, em que a informação e o digital (na ótica da sua aquisição, processamento e transmissão) se tornaram nas fontes principais de riqueza e crescimento económico, atentas as possibilidades tecnológicas existentes neste período histórico.

<sup>11</sup> Ao contrário de outras tecnologias, o computador não se destina a desenvolver nenhuma tarefa específica, mas, antes, é capaz de processar qualquer tipo de informação. Segundo a periodização apresentada por EVANGELIDIS

dispositivos (ou *hardware*) apresentam extraordinários níveis de desenvolvimento desde os anos 60. A cada ciclo tecnológico, a capacidade de processamento de informação das máquinas multiplica-se várias vezes. Nesta senda, um apontamento se faça a um outro marco relevante: a invenção do telemóvel<sup>12</sup>. Por volta de 1969, primeiro na Europa e depois nos EUA, começam a desenvolver-se as infraestruturas para a criação de uma rede que permitisse a operação da tecnologia móvel sem fios. O primeiro telemóvel a estar disponível para comercialização é apresentado pela NOKIA, uma empresa finlandesa, e constituiu a primeira geração (1G) da tecnologia sem fios. Em 1992, surge um novo telemóvel, novamente pelas mãos da NOKIA, capaz de fazer chamadas a partir de todo o mundo, uma vez que podia aceder ao *Global System for Mobile Communication Network* (GSM), constituindo assim a segunda geração tecnológica (2G). No mesmo ano é enviado o primeiro SMS. Em 2000, inventam-se os “emojis”, no Japão, e, em 2003, depois de milhões de unidades vendidas, a *internet* chega ao telemóvel (3G). O 5G, de acordo com os objetivos da Comissão<sup>13</sup>, chegará em força à UE a partir de 2020, permitindo assinaláveis transformações, levando à expansão da IoT (*Internet of Things*), da IoP (*Internet of People*) e da IoE (*Internet of Everything*). Em 2019, 97% da população mundial vivia ao alcance de uma rede móvel e 93% ao alcance de uma rede 3G ou superior<sup>14</sup>.

Em 1989, nova revolução acontece quando Tim Berners-Lee, investigador do CERN, inventa a *World Wide Web*, um sistema de indexação que utiliza hipertexto. A *web* representa, na essência, o aspeto atual da *internet* quando pensamos em páginas com conteúdos<sup>15</sup>. Na reinventada *internet*, «qualquer pessoa com capacidades informáticas mínimas pode aceder a

---

– *Landmarks in the History...*, cap. 6, a primeira geração de computadores (~1943 a ~1959) era baseada em válvulas termiônicas. A segunda geração de computadores é inaugurada, em 1947, com a invenção do transístor, mas o seu uso em grande escala só se inicia com a invenção dos circuitos integrados, em 1959. A terceira geração de computadores, entre 1971 e 1980, abre com a invenção do microprocessador, que é o «*computador num único chip*». A quarta geração de computadores, a partir de 1980, é dada pela tecnologia de integração em larga escala, por via da qual se incluíam dez ou vinte mil componentes num só *chip* de silício. A quinta geração, iniciada neste século, vai apontada à realização de cálculos e operações a grande velocidade e ao armazenamento de informação em larga escala. Os grandes desafios desta nova geração são a inteligência artificial e a construção de computadores quânticos, capazes de processar inimagináveis quantidades de informação no espaço de segundos.

<sup>12</sup> A história desta invenção remonta a 1908 quando nos EUA é registada uma patente para um “telefone sem fios”. Porém, o mundo havia de esperar até 1973, quando, na Motorola, se fez a primeira chamada a partir de um telefone celular: era a tecnologia 0G.

<sup>13</sup> Segundo as metas definidas pela Comissão, cada Estado-membro deverá assegurar que pelo menos uma grande cidade esteja «preparada para a 5G» até ao final de 2020 e que todas as zonas urbanas e as principais vias de transporte terrestre tenham cobertura 5G ininterrupta até 2025. Cfr. COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. 5G para a Europa: um Plano de Ação*. COM(2016) 588 final. Bruxelas, 14.9.2016. p. 5.

<sup>14</sup> INTERNATIONAL TELECOMMUNICATION UNION - *Measuring digital development: Facts and figures*. Geneva: ITU Publications, 2019.

<sup>15</sup> A *World Wide Web* tem na sua base três protocolos: o URL (*uniform resource locator*, i.e., o endereço de uma *webpage*), o HTTP (*Hypertext Transfer Protocol*, código que permite a transferência de hipertexto entre um servidor e o utilizador) e o HTML (*HyperText Markup Language*, a linguagem de formatação da *web*).

*informação não apenas no formato de palavras e números, mas também de imagens e sons»*<sup>16</sup>. A *web* foi um sucesso, uma vez que os utilizadores podiam navegar de fonte em fonte sem esforço, escolher os *links* que pretendiam explorar ou a informação que pretendiam transferir, além de poderem, eles próprios, produzir conteúdos, através da criação de páginas recorrendo à hipermédia<sup>17</sup>. Nos anos 90, com a introdução da prossecução do lucro *online*, a *internet* tornou-se um fenómeno global, com cada vez mais países a juntarem-se à aventura. Em 1995, os *sites* eram já trinta mil, com 16 milhões de computadores conectados à rede, o que levou um dos seus fundadores a afirmar que a *internet* havia «*passado da quase invisibilidade, à quase ubiquidade*» no espaço de um ano<sup>18</sup>. Um ano antes é colocado no mercado o navegador Netscape, que tornava a tarefa de navegar entre o crescente número de *websites* ainda mais fácil. Em 1996, o número de utilizadores da *internet* duplicava para os 36 milhões. Entretanto, a navegação *online*, com a proliferação de utilizadores e *webpages*, era cada vez mais difícil, pelo que novas soluções para encontrar e indexar informação *online* eram imperativas. Nesse mesmo ano, é introduzida a primeira versão do motor de busca Google, com o propósito de organizar a aparente infinita quantidade de informação na *web*. Em 2000, o número de utilizadores da rede chegava aos 361 milhões, navegando em cinquenta milhões de *websites*. Apenas um ano depois, os utilizadores eram já cerca de 513 milhões e o inglês deixava de ser a língua dominante. Na primeira década do novo século, assiste-se a uma proliferação das redes sociais para os mais variados fins, nos mais criativos e inovadores modelos<sup>19</sup>. O vertiginoso crescimento da *internet* não é apenas quantitativo<sup>20</sup>, mas também qualitativo. A este propósito,

---

<sup>16</sup> HEADRICK - *Technology: A World History*. p. 143. São princípios básicos e fundamentais da *internet* e da *web*, desde a sua fundação, a descentralização (a criação de conteúdos online é livre e independente de permissões governamentais, não existe um “controlo central da internet”), a não discriminação ou “*net neutrality*” (independentemente do serviço contratado para aceder à internet, a comunicação faz-se ao mesmo nível), o *bottom-up design* (o código da *web* não é controlado por um pequeno grupo de especialistas, antes é escrito e conhecido por todos, encorajando a máxima participação), a universalidade (todos os equipamentos da rede falam a mesma linguagem) e o consenso (para que os *standards* universais possam ser aplicados).

<sup>17</sup> ALMAGOR-COHEN, Raphael - *Internet History*. International Journal of Technoethics. n.º 2 (2011). p. 53.

<sup>18</sup> CERF, Vinton G. - *Computer Networking: Global Infrastructure for the 21st Century*. [Em linha] [s.l.]: [s.n.], 1995.

<sup>19</sup> Em 2003, é lançado o Myspace, sendo logo seguido (em 2004) pelo fenómeno Facebook, cujo número de utilizadores ativos ascendia, em 2019, a uns estonteantes 2,5 mil milhões, fazendo do Facebook a maior rede social do universo, maior do que qualquer país. Cfr. <https://tinyurl.com/ybcbcr4e>. Consultado em 26/01/2020.

<sup>20</sup> Em 2019, segundo dados da UIT, estimava-se que 4,1 mil milhões de pessoas tenham estado *online*, o que equivale a cerca de 53,6% da população mundial. O desafio continua a ser o do combate à disparidade e desigualdade no acesso à *web*, porquanto 87% do mundo desenvolvido já esteja *online*, contra apenas 19,1% dos cidadãos nos países em desenvolvimento. Para estes números contribui o facto de a conexão com a *internet* se fazer cada vez menos através de computadores, mas via telemóvel, principalmente nos países em desenvolvimento, onde os planos de dados móveis se vão tornando acessíveis a todos. Em alguns países africanos, inclusive, e à conta dos pacotes de dados que oferecem navegação gratuita nas redes sociais, muitas pessoas creem que o Facebook é a *internet*, pelo que não a conhecem nem exploram para além disso. Cfr. INTERNATIONAL TELECOMMUNICATION UNION - *Measuring digital development...*

é possível dividir o desenvolvimento da *web* em três fases principais<sup>21</sup>, com uma quarta já à espreita. A primeira, a Web 1.0, corresponde a um modelo essencialmente estático e sem interação, em que a *internet* serve para depositar, encontrar e ler informação. A Web 2.0 surge, a partir de 2004, com o advento dos blogs, das redes sociais, das *wikis*, dos *tags*<sup>22</sup> e dos *podcasts*, não sendo propriamente uma nova fase, mas antes o aprofundar da potencialidade original da *web*<sup>23</sup>. Nesta *web*, o utilizador não se limita a consultar conteúdos, interagindo com eles e criando-os. A *internet* passa a ser entendida como uma plataforma participativa, onde existe colaboração entre consumidores, criadores de conteúdos, prestadores de serviços e organizações. Uma terceira fase de desenvolvimento da *web* começa em meados da década de 10, designando-se ora por Web 3.0, ora por *web semântica* ou *inteligente*. Neste personalizado mundo *online*, a introdução de novas linguagens de programação permite que as máquinas não só processem, mas *compreendam* a vastidão de dados que se encontram alojados na *internet* de forma muito semelhante à humana<sup>24</sup>. A face mais visível da Web 3.0 é a organização dos conteúdos apresentados ao utilizador de acordo com o seu histórico de pesquisa, de modo a corresponderem aos seus interesses e desejos percebidos. A partir de 2020 é previsível que se inicie a generalização da Web 4.0, *web simbiótica* ou *web das coisas*, referente «à ideia de interação entre humanos e máquinas em simbiose»<sup>25</sup>. Ainda não é claro a que corresponderá exatamente esta fase de evolução da *web*, esperando-se, todavia, que a ubiquidade da *internet* seja reforçada através da integração de várias tecnologias em rede, tais como dispositivos móveis, sensores, eletrodomésticos e equipamentos eletrónicos no geral. Assim, a comunicação máquina-máquina e a Inteligência Artificial serão realidades permanentes. Os termos IoT, IoP e IoE descreverão um ambiente em que pessoas e objetos (virtuais e reais) estão completamente integrados, alimentando constantemente a rede com dados (dando origem ao *big data*), que, depois de convertidos em informação útil, são usados para apoiar o processo de decisão das organizações e dos próprios indivíduos.

Não é accidental o facto de a maioria das gigantes tecnológicas serem americanas ou asiáticas. Realmente, e contrariando a sua pujança secular, a Europa só a custo tem acompanhado as

<sup>21</sup> CHOUDHURY, Nupur - *World Wide Web and Its Journey from Web 1.0 to Web 4.0*. International Journal of Computer Science and Information Technologies. Vol. 5, n.º 6 (2014). p. 8096.

<sup>22</sup> Um *wiki* é uma página *online* que pode ser facilmente editada por qualquer utilizador com permissões (v.g.: Wikipédia). Um *tag* corresponde a uma palavra-chave usada para descrever um determinado conteúdo.

<sup>23</sup> Neste sentido, cfr. ANDERSON, Paul - *What is Web 2.0? Ideas, technologies and implications for education*. [s.l.]: JISC Technology and Standards Watch, 2007.

<sup>24</sup> RUDMAN, Riaan; BRUWER, Rikus - *Defining Web 3.0: opportunities and challenges*. The Electronic Library. Vol. 34, n.º 1 (2016). p. 136 e ss.

<sup>25</sup> VESNIC-ALUJEVIC, Lucia; STOERMER, Eckhard; RUDKIN, Jennifer-Ellen; SCAPOLO, Fabiana; KIMBELL, Lucy - *The Future of Government 2030+: A Citizen-Centric Perspective on New Government Models*. Luxemburgo: Publications Office of the European Union, 2019. p. 40.

grandes potências tecnológicas<sup>26</sup>. Não obstante, as então Comunidades Europeias compreenderam a importância da revolução que se avizinhava, ainda que, em certos momentos, tenham persistido algo relutantes quanto ao desenvolvimento da *internet*<sup>27</sup>. Em 1971, o Conselho adota o primeiro plano visando coordenar a ação dos EM em matéria de informação e documentação técnica e científica e, designadamente, em matéria de «*promoção do progresso tecnológico em informática documental e em ciências da documentação*»<sup>28</sup>. Em 1975, aquando da aprovação do plano de ação inicial na área da informação e documentação técnica e científica<sup>29</sup>, já o Conselho reconhecia a «*proliferação dos sistemas de informação e o seu rápido, mas díspar, crescimento, por força da competição entre múltiplos empreendedores públicos e privados*»<sup>30</sup>, o que tornava «urgente» o estabelecimento de uma rede europeia de informação e documentação. Neste âmbito, a CEE apoiou a criação da EIN (*European Informatic Network*), cujas operações se iniciam em 1976, mas sem particular sucesso. Em 1979, o segundo plano de ação cria a EURONET, «*uma rede online operacional de informação pública*»<sup>31</sup> com o objetivo de coordenar a nível europeu os esforços no sentido da digitalização e alcançar um certo grau de cooperação entre EM que conduzisse à standardização internacional da rede, mote das Comunidades nos anos seguintes. Refere SHAHIN, «*estes esforços europeus não eram a internet, e, nesta fase, não era claro que a Comissão fosse apoiar a internet ou, na verdade, qualquer rede global de comunicações que não utilizasse standards de origem europeia ou oficialmente aceites na Europa*»<sup>32</sup>. Os anos 80 não trouxeram revoluções significativas na política europeia, iniciando a CEE uma espécie de corrida contra o prejuízo, procurando destacar-se enquanto *player* no mercado das tecnologias de informação, fazendo face ao domínio americano e japonês, já reconhecendo, contudo, tratar-se esta de uma «*nova revolução industrial*»<sup>33</sup>. Em termos legislativos, a aposta foi sobretudo na criação de um mercado de informação para a Europa<sup>34</sup>, que pressupunha a liberalização e harmonização no domínio das telecomunicações<sup>35</sup>. Em todo o caso, o investimento da UE estava mais orientado

<sup>26</sup> HEADRICK - *Technology: A World History*, p. 142.

<sup>27</sup> A afirmação é de SHAHIN, Jamal - *A European history of the Internet*. Science and Public Policy. Vol. 33. n.º 9 (2006). p. 681.

<sup>28</sup> JO C 122 de 10.12.1971, p. 7.

<sup>29</sup> JO L 100 de 21.4.1975, p. 18.

<sup>30</sup> É de notar que o setor das telecomunicações na Europa surge em circunstâncias distintas das norte-americanas, uma vez que os serviços postais, de telegrafo e telefone foram desde início monopólios estatais. Vide SHAHIN - *A European history of the Internet*, p. 682.

<sup>31</sup> JO L 311 de 04.11.1978, p. 1 e ss.

<sup>32</sup> SHAHIN - *A European history of the Internet*. p. 684.

<sup>33</sup> JO C 184 de 11.07.1984, p. 1.

<sup>34</sup> JO L 314 de 04.12.1984, p. 19.

<sup>35</sup> JO L 36 de 07.02.1987, p. 31. Isso mesmo resulta do *Livro Verde da Comissão sobre o desenvolvimento da normalização europeia: ações para uma integração tecnológica mais rápida na Europa*, publicado em 1990, e que, mais tarde, em 1998, esteve na base da criação do *European Telecommunications Standards Institute*.

para a conceção de uma rede pan-europeia do que propriamente para ligar a Europa à *internet* “americana”. Esta desconfiança face à rede criada do outro lado do Atlântico só a partir dos anos 90 é ultrapassada com a adoção generalizada do protocolo TCP/IP. O advento da *web*, invenção reclamada pela Europa, evidencia as potencialidades do mundo *online*, principalmente para o mercado interno: a sociedade de informação estava ao virar da esquina e a Europa tinha de estar no pelotão da frente. É essa ideia que perpassa no Livro Branco «*Crescimento, competitividade e emprego: os desafios e as pistas para entrar no século XXI*», publicado em 1994 e da responsabilidade da Comissão presidida por Jacques Delors<sup>36</sup> e, mais tarde, na Resolução do Conselho sobre os aspetos industriais para a UE no âmbito do desenvolvimento da sociedade da informação, onde se lia: «*a reação aos desafios da sociedade da informação constitui para a UE uma prioridade política ao serviço dos objetivos da criação de emprego, da melhoria da qualidade de vida dos cidadãos, do aumento da competitividade do sistema de produção e de incremento da coesão económica e social*»<sup>37</sup>.

No curso da primeira década deste século, a UE emergiu por completo na sociedade de informação, aderindo, sem reservas, ao modelo global de *internet*, procurando colocar em linha cada vez mais cidadãos e empresas. Ao mesmo tempo, empenhou-se em ter um papel mais preponderante na definição do presente e futuro da *web*, colocando-se na linha da frente da regulação e monitorização do espaço digital. O Conselho Europeu extraordinário de Lisboa de março de 2000 estabeleceu o objetivo de tornar a Europa a economia mais competitiva e dinâmica do mundo até 2010<sup>38</sup>, alertando logo para a prioridade de se «*garantir uma oferta adequada de conteúdos digitais de qualidade na Internet*»<sup>39</sup>. Em 2002, a nova agenda «*eEuropa 2005 – Uma Sociedade de Informação para Todos*»<sup>40</sup> foca-se já na dotação da UE das infraestruturas de banda larga que garantissem o acesso à *internet* através de outros dispositivos que não o computador, como a televisão digital e o 3G. Assim, previa-se que até 2005 todos os EM disponibilizassem redes de banda larga, e desenvolvessem e adotassem o Protocolo da

---

<sup>36</sup> COMISSÃO EUROPEIA - *Crescimento, Competitividade, Emprego. Os desafios e as pistas para entrar no século XXI* — «*Livro Branco*». Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias, 1994.

<sup>37</sup> JO C 341 de 19.12.1995, p. 6.

<sup>38</sup> O que passava, principalmente, pela penetração das tecnologias digitais. Em face deste objetivo, a Comissão publica, em 2000, o Plano de Ação «*eEurope 2002 - Uma Sociedade da Informação para Todos*» onde se elencavam, enquanto principais metas a alcançar até 2002, o acesso mais barato, rápido e seguro à *internet*, o investimento nas competências digitais e o estímulo à utilização da *internet* pelas pessoas, empresas e administrações públicas.

<sup>39</sup> COMISSÃO DAS COMUNIDADES EUROPEIAS – *eEurope 2002. Uma Sociedade da Informação para Todos. Projecto de Plano de Acção preparado pela Comissão Europeia para o Conselho Europeu da Feira 19-20 de junho*. COM (2000) 330 final. Bruxelas, 24.5.2000. p. 3.

<sup>40</sup> COMISSÃO DAS COMUNIDADES EUROPEIAS – *Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité Económico e Social e Comité das Regiões. eEurope 2005: Uma Sociedade da Informação para todos*. COM(2003) 263 final. Bruxelas, 28.05.2002.

próxima geração da *internet*, IPv6, cujo desenvolvimento a Comissão apoiou fortemente, enquanto projeto europeu. Na última década e meia, a UE, em busca da neutralidade climática até 2050, vê na completa transição digital da Europa um «*fator essencial para a realização dos seus objetivos de sustentabilidade*»<sup>41</sup>, centrando a sua aposta na tecnologia 5G<sup>42</sup>, mas já com o 6G à vista<sup>43</sup>, na inteligência artificial<sup>44</sup>, na computação em nuvem e na gestão de dados<sup>45</sup> e na finalização do Mercado Único Digital<sup>46</sup>. Essa transição está ancorada em três dimensões essenciais: «*a tecnologia ao serviço das pessoas, uma economia justa e competitiva e uma sociedade aberta, democrática e sustentável*»<sup>47</sup>. Para o efeito, encontra-se em fase de aprovação um programa de financiamento intitulado “Europa Digital” (2021-2027) abrangendo cinco domínios essenciais (supercomputação, IA, cibersegurança, competências digitais avançadas e utilização generalizada das tecnologias digitais em toda a sociedade) e que tem como objetivo apoiar e acelerar a transformação digital, contribuindo para colmatar o fosso digital na União e reforçar a sua autonomia estratégica. Entretanto, e já em resultado da pandemia de COVID-19, o Conselho Europeu e o Conselho da UE salientaram que o recuso às tecnologias digitais durante a situação pandémica «*veio pôr ainda mais em evidência a necessidade de acelerar a transição digital na Europa*»<sup>48</sup>, a qual desempenhará um papel essencial na recuperação económica no período pós-crise<sup>49</sup>, razão pela qual 20% dos fundos do Mecanismo de Recuperação e Resiliência serão aplicados na transição digital.

Nos alvares da terceira década do século, a Era Digital é elemento incontornável, tendo

---

<sup>41</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Pacto Ecológico Europeu.* COM(2019) 640 final. Bruxelas, 11.12.2019. p. 10.

<sup>42</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. 5G para a Europa: um Plano de Ação.* COM(2016) 588 final. Bruxelas, 14.9.2016.

<sup>43</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité das Económico e Social Europeu e ao Comité das Regiões. Uma nova estratégia industrial para a Europa.* COM(2020) 102 final. Bruxelas, 10.03.2020. p. 4.

<sup>44</sup> COMISSÃO EUROPEIA – *Livro Branco sobre inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança.* COM(2020) 65 final. Bruxelas, 19.2.2020.

<sup>45</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Uma estratégia europeia para os dados.* COM(2020) 66 final. Bruxelas, 19.2.2020.

<sup>46</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital. Um Mercado Único Digital conectado para todos.* COM(2017) 228 final. Bruxelas, 10.5.2017.

<sup>47</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Construir o futuro digital da Europa.* COM(2020) 67 final. Bruxelas, 19.2.2020.

<sup>48</sup> CONSELHO EUROPEU – *Conclusões da Reunião extraordinária do Conselho Europeu (1 e 2 de Outubro de 2020).* EUCO 13/20. Bruxelas, 2.10.2020.

<sup>49</sup> CONSELHO DA UNIÃO EUROPEIA – *Conclusões do Conselho (9 de junho de 2020). “Construir o futuro digital da Europa”.* 8711/20. Bruxelas, 9.06.2020.

originado, em grande medida, uma nova forma de organização social, marcada por certas características basilares, que CASTELLS descreve assim<sup>50</sup>: a informação é a sua própria matéria-prima, uma vez que as tecnologias são usadas para atuar sobre a informação e o conhecimento e já não o contrário, como acontecia em revoluções tecnológicas anteriores. Por outro lado, a penetração dos efeitos das novas tecnologias é imenso, estendendo-se a todos os processos da nossa existência individual e coletiva, moldando-os. No mesmo sentido, a lógica de redes passou a ser amplamente usada em qualquer sistema ou conjunto de relações, sendo penalizante estar fora da rede em virtude do número decrescente de oportunidades. Finalmente, duas mais características da Era Digital são apontadas: flexibilidade e convergência; flexibilidade porque tudo – desde sistemas a organizações – pode ser modificado e fundamentalmente alterado pela reorganização dos componentes; convergência porque as tecnologias, ainda que distintas e específicas, estão ligadas num sistema altamente integrado.

## **Secção II – Por uma compreensão atualista da teoria do risco: os (novos) riscos (tecnológicos) mundiais.**

É consensual que a digitalização acarreta novos e desconhecidos riscos para o modo de organização das nossas sociedades. Como reconhece INGOLF PERNICE, «na “constelação digital” somos confrontados com novos riscos e ameaças à escola global, independentes de fronteiras e distâncias geográficas»<sup>51</sup>. Importa, pois, tentar compreender o que é, afinal, um risco. Antes de mais, e como ensina ULRICH BECK, «não existe “o” risco, mas sim duas visões do mesmo risco, que se excluem mutuamente e se enfrentam de forma mais ou menos inconciliável»<sup>52</sup>. Nesta dicotomia, uma visão encara o risco associado ao mundo moderno enquanto oportunidade. Aqui, a atenção concentra-se «nas potenciais vantagens para o decisor, enquanto indivíduo ou enquanto empresa, Estado, região»<sup>53</sup>. Para outra visão, as decisões e práticas que acompanham o desenvolvimento tecnológico constituem um perigo, «uma ameaça problemática, questionável e até inaceitável à própria vida social»<sup>54</sup>, até porque acontecem sem debate público e sem consensos. Neste esquema, «o risco tornou-se o modo central da construção e organização da sociedade»<sup>55</sup>, por via da intensificação da lógica

<sup>50</sup> CASTELLS - *A Era da Informação...* Vol. I., p. 87 e ss.

<sup>51</sup> PERNICE, Ingolf - *Risk management in the digital constellation - a constitutional perspective (part I)*. Revista D'Internet, Dret i Política. N.º 26 (2018). p. 85.

<sup>52</sup> BECK, Ulrich - *Sociedade de risco mundial: em busca da segurança perdida*. Lisboa: EDIÇÕES 70, 2016. p. 293 e ss.

<sup>53</sup> *Ibid.*

<sup>54</sup> *Ibid.*, p. 294.

<sup>55</sup> *Ibid.*

dicotómica do conflito, o qual não se limita nem à economia, nem à política, e ainda menos ao espaço nacional. Numa palavra, «*a categoria do risco consume e transforma tudo*»<sup>56</sup>. O “risco” enquanto categoria sociológica, representa a forma de se lidar com a insegurança, resultante já não do desconhecimento, mas do progresso. Assim, um risco corresponde sempre a um acontecimento ou, mais corretamente, à probabilidade de um acontecimento, representável e calculável em termos estatísticos. Já um perigo é um contributo negativo, também por acontecer, na materialização de um risco. Com efeito, qualquer risco pode materializar-se, na pior das hipóteses, numa catástrofe ou, na melhor das hipóteses, numa oportunidade. O cerne da teoria do risco está no processo de decisão, uma vez que os riscos – em termos de perigos e oportunidades – devem ser equacionados no momento da tomada de decisões<sup>57</sup>.

No início do século, identificavam-se três grandes novos riscos globais: as crises ecológicas, as crises financeiras e as ameaças terroristas. Estes riscos têm em comum o facto de resultarem já não das limitações da sociedade, mas, *a contrario*, do seu desenvolvimento. Num certo sentido, estes riscos reportam-se a vitórias ou triunfos técnico-científicos do desenvolvimento civilizacional. Com propriedade, pode dizer-se que correspondem a *efeitos secundários* do progresso. Assim, quando pensamos em catástrofes nucleares, na poluição generalizada e resultante da industrialização e nas alterações climáticas não nos estamos já a referir a riscos externos, atribuíveis a entes sobrenaturais ou à própria natureza, mas a riscos internos à sociedade, resultantes da modernização. Ora, os grandes novos riscos tecnológicos obedecem a este esquema: eles são fruto não do fracasso, mas de decisões conscientes associadas ao cálculo do benefício económico. Segundo BECK, os novos riscos mundiais obedecem a três grandes características<sup>58</sup>: [i.] deslocalização, [ii.] imprevisibilidade e [iii.] não-compensabilidade. A deslocalização reporta-se ao facto de as causas e efeitos dos riscos modernos não se encontrarem limitadas a um espaço sócio-geo-temporal, sendo, por princípio, omnipresentes. Os novos riscos propagam-se além das fronteiras dos Estados (v.g.: alterações climáticas), possuem longos períodos de latência no tempo, pelo que as suas consequências futuras têm sempre um certo grau de indeterminabilidade (v.g.: catástrofes nucleares), resultando de complexos processos e cadeias de impacto que tornam difícil a tarefa de determinar as suas causas, efeitos e responsabilidades (v.g.: crises financeiras). A imprevisibilidade decorre do facto de as consequências dos novos riscos serem, em regra, incalculáveis; a não-compensabilidade da circunstância de, ao contrário dos riscos tradicionais

<sup>56</sup> BECK, Ulrich - *Critical Theory of World Risk Society: A Cosmopolitan Vision*. Constellations. Vol. 16. n.º 1 (2009). p. 3.

<sup>57</sup> LUHMANN, Niklas - *Risk: a sociological theory*. New York: Routledge, 2002. p. 22.

<sup>58</sup> BECK, *Sociedade de risco mundial...*, p. 106 e ss.

– que se distinguem pela sua segurabilidade (v.g.: acidentes de viação) –, não ser possível anular os seus efeitos nocivos através de compensações. Nos riscos modernos a lógica da compensação é substituída pelo *princípio da prevenção*. PERNICE destaca outras características destes riscos<sup>59</sup>: eles são inintencionais e «efeitos secundários implícitos» da modernização; são universais e difíceis de imputar a indivíduos ou organizações particulares; produzem iniquidades a todos os níveis, incluindo o internacional<sup>60</sup>. Não obstante o antedito, os riscos emergentes da “constelação digital” não se subsumem por completo a esta caracterização. Antes, os ciber-riscos (ou riscos digitais) apresentam-se geralmente como «explícitos, concretos e visíveis»<sup>61</sup>, ainda que os seus efeitos sejam também deslocalizados, uma vez que afetam não apenas indivíduos, mas empresas, serviços públicos, órgãos de soberania, infraestruturas críticas e estratégicas (tais como redes elétricas e de abastecimento de água, centrais nucleares, aeroportos, redes ferroviárias, rede bancária, etc.) ou, em abstrato, tudo quanto esteja ligado à *internet* ou dela dependa. Segundo o Autor, apesar de estes riscos poderem alcançar uma dimensão global, os perigos que lhes estão associados são intencionais, não provindo de «fontes difusas, como no caso da poluição do ar ou da desflorestação, mas tendo sempre origem numa fonte determinável, muitas vezes indivíduos, mas também grupos, empresas ou Estados»<sup>62</sup>. Porém, apesar de *determináveis*, subsiste ainda, muitas vezes, uma impossibilidade tecnológica na identificação das concretas fontes responsáveis pelos perigos, o que gera a perceção errónea de que se tratam de catástrofes assimiláveis a outros riscos modernos. Assim, podemos até certo ponto distinguir os ciber-riscos e os demais riscos modernos usando o critério da intencionalidade: ao passo que estes últimos correspondem, segundo BECK, a efeitos secundários *inintencionais* do progresso, os primeiros são sempre efeitos secundários *intencionais* da digitalização da sociedade. Não obstante, este critério tem de ser lido em conjunto com a possibilidade da existência de perigos não intencionais, inevitáveis com a complexificação tecnológica, como o erro técnico ou a falha de sistema, ainda que estes fiquem fora do escopo do presente trabalho.

### **Secção III – A União Europeia e o Estado de Direito democrático.**

O Preâmbulo do TUE refere, logo no seu segundo considerando, que os Estados-Membro se

<sup>59</sup> PERNICE, *Risk management in the digital constellation...*, p. 85.

<sup>60</sup> A este propósito tem relevo a expressão «*antagonismo do risco*», que traduz precisamente a ideia de que aqueles que beneficiam das oportunidades oferecidas pelos riscos não são, por regra, os mesmos que suportarão os seus efeitos negativos. Para mais desenvolvimentos, cfr. BECK - *Critical Theory of World Risk Society...*, p. 9.

<sup>61</sup> PERNICE - *Risk management in the digital constellation...*, p. 86.

<sup>62</sup> *Ibid.*

inspiraram, para a criação de *uma* União Europeia, no «*património cultural, religioso e humanista da Europa*» de onde emanam, enquanto «*valores universais*», entre outros, a «*liberdade, a democracia, a igualdade e o Estado de direito*». A União Europeia funda-se nestes quatro princípios tidos por universalmente aceites ou, pelo menos, tidos por comuns a todos os EM, como confirma o art.º 2.º do TUE<sup>63</sup>. A verdade é que «*com o fim da Guerra Fria e com aquilo que parecia, durante um curto período de tempo, o triunfo universal e permanente do modelo liberal e democrático do Ocidente, os países Europeus comprometeram-se a promover os direitos humanos, a democracia e o Estado de direito como os três princípios fundamentais sob os quais a “nova Europa” deveria ser fundada*»<sup>64</sup>. A partir deste momento, o Estado de Direito parece ter-se tornado um conceito dominante no discurso político e académico, o que reverberou no Direito Primário da União. Todavia, só por excessivo apego legalista poderíamos afirmar que a primeira referência ao Estado de Direito enquanto princípio constitucional da UE ocorreu em Amesterdão. Na verdade, já antes o TJUE havia estabelecido, num emblemático Acórdão, que «*a Comunidade Económica Europeia é uma comunidade de direito*»<sup>65</sup>, muito embora limitando o escopo dessa afirmação a uma versão formalista do *rule of law*, baseada na fiscalização pelos tribunais comunitários da conformidade dos atos das instituições e dos EM «*com a carta constitucional de base que é o Tratado*», fórmula que haveria de ser sucessivamente repetida.

É necessário começar por notar que o Estado de Direito é um princípio basilar da tradição constitucional ocidental, o que obviamente abrange todos os EM. Assim, antes de ser um valor da União, o Estado de Direito é um princípio constitucional nacional, razão pela qual integra a *tradição constitucional comum dos EM*, expressamente recebida pelo DUE no que toca ao reconhecimento e aplicação dos Direitos Fundamentais (cfr., *inter alia*, o art.º 6.º, n.º 3 TUE). Os EM decidiram, todavia, na senda do aludido espírito de promoção do Estado de Direito democrático e dos direitos fundamentais, atribuir crescente relevância àqueles princípios, não

<sup>63</sup> Nem sempre foi assim: as primeiras referências nos Tratados ao Estado de Direito enquanto princípio enformador das Comunidades surgem, timidamente, em Maastricht, momento em que os EM «*confirmam*», no Preâmbulo, «*o seu apego aos princípios da liberdade, da democracia, do respeito pelos direitos do Homem e liberdades fundamentais e do Estado de direito*». Só mais tarde, em 1997, com o Tratado de Amesterdão, se afirma expressamente o caráter fundacional do Estado de Direito, enquanto princípio, no então n.º 1 do art.º F. Haverá razões substantivas que justifiquem a alteração terminológica ocorrida com o Tratado de Lisboa (de *princípios* para *valores*)? Duas respostas podem ser aventadas: ou a alteração ocorreu com o objetivo de salientar o caráter *mais* indeterminado dos valores face aos princípios; ou a modificação prende-se com a necessidade de distinguir os princípios *fundacionais* da União (os valores nucleares) de outros princípios *não-fundacionais*. Cfr. PECH, Laurent - *Rule of Law as a Guiding Principle of the European Union's External Action*. Hague: Centre for the Law of EU External Relations, 2012. p. 10.

<sup>64</sup> PECH, Laurent - *The Rule of Law as a Constitutional Principle of the European Union*. New York: NYU School of Law, 2009. p. 19.

<sup>65</sup> Ac. TJUE de 23.04.1986, C-249/83 (Os Verdes), n.º 23. Mais impressionantemente em inglês: «*the European Economic Community is a Community based on the rule of law*».

só enquanto valores intrínsecos à UE, mas também enquanto parâmetros de atuação das instituições, de adesão e de permanência na organização, o que aponta para uma dimensão simultaneamente interna e externa do princípio. Mas o que é o Estado de Direito? À semelhança do que acontece com a maioria dos ordenamentos jurídicos nacionais, o DUE não oferece nenhuma definição do conceito<sup>66</sup>, deixando a tarefa à doutrina. Essa ausência de conceito, relaciona-se, por um lado, com a própria especificidade linguística do termo, variável e sem total correspondência entre EM<sup>67</sup> e, por outro lado, com o carácter «*esquivo e controverso*» do conceito<sup>68</sup>. Não obstante, cremos que essas visões próprias e distintas do que seja o Estado de Direito não adquirem relevância tal que, genericamente, não permitam afirmar que existe um consenso alargado sobre o significado do princípio. Na verdade, esse consenso resulta, em parte, do trabalho da Comissão de Veneza do Conselho da Europa que, no seu *Relatório sobre o Estado de Direito*<sup>69</sup>, oferece uma tentativa de definição que tem granjeado generalizada aceitação<sup>70</sup>. Para a Comissão de Veneza, são seis os elementos necessários ao Estado de Direito: (1) legalidade (primado do direito), nos termos do qual as normas devem ser respeitadas quer pelos cidadãos, quer pelas pessoas colectivas públicas ou privadas (incluindo os órgãos de soberania), uma vez adotadas segundo um processo democrático transparente e responsável; (2) certeza e segurança jurídica, o que implica, entre outros, a promoção da acessibilidade às normas vigentes, a sua aplicação de forma previsível e consistente, a precisão e clareza das leis, a limitação dos poderes discricionários, a proteção das legítimas expectativas dos cidadãos na sua relação com o poder público, a aplicação, na realidade, do direito vigente; (3) proibição da

<sup>66</sup> Recentemente, a Comissão, na Proposta (ainda não adotada) de Regulamento do Parlamento Europeu e do Conselho sobre a proteção do orçamento da União em caso de deficiências generalizadas no que diz respeito ao Estado de direito nos Estados-Membros, definiu o Estado de Direito como «um dos valores da União, consagrado no artigo 2.º do Tratado da União Europeia, que inclui os princípios da legalidade, que supõe um processo transparente, responsável, democrático e pluralista para a adoção de legislação; da segurança jurídica; da proibição da arbitrariedade nos poderes executivos; da proteção judicial efetiva por tribunais independentes, nomeadamente dos direitos fundamentais; da separação de poderes e da igualdade perante a lei». Cfr. COMISSÃO EUROPEIA – Proposta de Regulamento do Parlamento Europeu e do Conselho sobre a proteção do orçamento da União em caso de deficiências generalizadas no que diz respeito ao Estado de direito nos Estados-Membros. COM (2018) 324 final. Bruxelas, 2.5.2018. p. 6.

<sup>67</sup> É possível observar que *rule of law*, *Rechtsstaat* e *Etat de droit* não são termos que se sobreponham completamente, sendo distintas as tradições de que partem. A uma conceção mais formalista do Estado de Direito típica do sistema anglo-saxónico, contrapõe-se uma conceção mais substancial dado pelo sistema germânico, particularmente no pós-2.ª Guerra Mundial. Vide, para uma análise mais detalhada, PECH - *The Rule of Law as a Constitutional...*, p. 24 e ss.

<sup>68</sup> CARRERA, Sergio; GUILD, Elspeth; HERNANZ, Nicholas - *The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU: Towards an EU Copenhagen Mechanism*. [s.l.]: Centre for European Policy Studies, 2013. p. 16.

<sup>69</sup> EUROPEAN COMMISSION FOR DEMOCRACY THROUGH THE LAW (VENICE COMMISSION) - *Report on the Rule of Law*. Strasburg: Council of Europe, 2011.

<sup>70</sup> Essa definição parte essencialmente do trabalho de BINGHAM, Tom - *The Rule of Law*. London: Penguin Books Ltd, 2011, que entende o Estado de Direito como a «vinculação (em termos de direitos e deveres) de todas as pessoas e autoridades do estado, públicas ou privadas, às normas aprovadas segundo procedimentos conhecidos, as quais só produzem efeitos, em regra, para o futuro, sendo publicamente aplicadas pelos tribunais».

arbitrariedade; (4) acesso à justiça e a tribunais independentes e imparciais; (5) respeito pelos direitos fundamentais; (6) proibição da discriminação e igualdade perante a lei. O que este conjunto de elementos evidencia, aliás em linha com as concepções modernas acerca do Estado de Direito, é que este corresponde a um multifacetado “princípio chapéu” composto por elementos formais, destinados essencialmente a garantir a sujeição de todos os membros da comunidade política às normas aprovadas segundo um determinado procedimento previamente fixado<sup>71</sup>, e por elementos substanciais, os quais apontam para parâmetros relacionados com o conteúdo e com os objetivos substantivos prosseguidos pelas normas e demais atos públicos. De facto, poucas objeções se levantarão hoje à necessidade de um Estado de Direito simultaneamente formal e substancial, a menos que admitamos que se enquadra no Estado de Direito um qualquer regime que, ainda respeitando determinados princípios externos, produza legislação e adote atos *externamente válidos de conteúdo interno* absolutamente abomináveis. Ora, é precisamente para evitar situações deste género que do Estado de Direito não deve ser dissociada uma faceta substantiva<sup>72</sup>, que opere em várias dimensões: em primeiro lugar, é necessário reconhecer que é do próprio conceito que resultam uma série de direitos fundamentais<sup>73</sup>. Em segundo lugar, a limitação do poder do Estado, que se encontra submetido ao Direito que edita, implica não só o respeito por determinados atributos da ordem jurídica, como também o respeito (e a promoção) de todos os direitos fundamentais reconhecidos em instrumentos nacionais, supranacionais ou internacionais. Em terceiro lugar, não se pode dissociar do princípio do Estado de Direito a própria noção de democracia enquanto forma de governo «*of the people, by the people, for the people*», na expressão de LINCOLN.

A União Europeia não é, obviamente, um *Estado* de Direito, aliás como bem encapsula a formulação do Acórdão *Os Verdes*, mas antes uma *União de Direito*, sem que isso implique, na nossa ótica, nenhuma modificação substancial dos subprincípios contidos e deduzidos do princípio constitucional do Estado de Direito. Não obstante, o carácter não-estadual da UE implica que o princípio adquira «*um âmbito de aplicação mais amplo*»<sup>74</sup>, servindo,

<sup>71</sup> Cfr. CRAIG, Paul - *The Rule of Law*. London: House of Parliament, 2007.

<sup>72</sup> É esta também a posição defendida por DWORKIN, quando distingue duas concepções de Estado de Direito. Uma a que chama concepção «*rule book*» que insiste que o poder do Estado não pode ser exercido contra os cidadãos a não ser em conformidade com um conjunto de normas específicas, transparentes e publicitadas, regras essas que são aprovadas e modificadas segundo um outro conjunto de normas. A segunda concepção, designada «*rights-based*», pressupõe que os cidadãos têm direitos e deveres morais entre si e direitos políticos perante o Estado como um todo, sendo exigível ao Estado que reproduza nas normas que edita esses direitos e deveres morais e os aplique judicialmente. Cfr. DWORKIN, Ronald - *Levando os direitos a sério*. São Paulo: Martins Fontes, 2002. p. 6 e ss.

<sup>73</sup> Desde logo, e partindo apenas da CDFUE, o direito à ação e a um tribunal imparcial (art.º 47.º), a presunção de inocência e o direito de defesa (art.º 49.º), o princípio da legalidade e da proporcionalidade dos delitos e das penas (art.º 49.º), o direito a não ser julgado ou punido penalmente mais de que uma vez pelo mesmo delito (*ne bis in idem*), o direito a uma boa administração e o direito de acesso aos documentos (art.º 41.º e 42.º).

<sup>74</sup> PECH - *The Rule of Law as a Constitutional...*, p. 50.

designadamente, como *standard* ou requisito político de acesso e permanência dos EM, além de ser um objetivo de ação no âmbito da política externa. Sublinha PEECH que «*essas características distintivas não provêm de um entendimento alternativo do que deve acarretar ao nível supranacional o Estado de Direito. Antes, elas refletem a natureza constitucional original da UE. Como organização supranacional e "dinâmica", teoricamente aberta a todos os países europeus que compartilham os mesmos valores [...], a UE tem naturalmente usos adicionais para o Estado de Direito*»<sup>75</sup>. Ora, o Estado de Direito na UE assume, também, uma função de articulação da organização com os EM, uma vez que «*exprime o respeito devido aos valores constitucionais nacionais*»<sup>76</sup>, querendo evitar um conflito entre os valores nacionais e os valores supranacionais. Para tal, a UE baseia os seus fundamentos constitucionais nos princípios constitucionais comuns aos EM. A questão do âmbito de aplicação do Estado de Direito na UE entronca nos mecanismos internos de garantia de respeito pelo princípio. Antes da adesão à União (controlo *ex ante*), e conforme declara o art.º 49.º TUE, (só) podem pedir para ser membro da UE os Estados europeus que respeitem os valores referidos no art.º 2.º TUE e estejam empenhados em promovê-los, conforme também resulta dos Critérios de Copenhaga, os quais aludem à existência de instituições que garantam a democracia, o Estado de Direito, os direitos humanos e o respeito pelas minorias e sua proteção<sup>77</sup>. Depois da adesão, os EM ficam sujeitos a vários controlos *ex post*<sup>78</sup> de modo a assegurar o cumprimento dos princípios ou valores fundacionais da União, como condição (pelo menos em teoria) de permanência na organização. Esses mecanismos podem ter assento nos Tratados, ter uma ligação indireta com o direito primário da União ou nem sequer resultarem de qualquer instrumento jurídico, antes originando na *soft-law*. Por esta razão, aqueles mecanismos vinculam de forma distinta os EM. A Comissão identifica como «*instrumentos centrais*» de proteção do Estado de Direito os seguintes<sup>79</sup>: art.º 7.º TUE, procedimentos de infração (art.º 258.º e ss. TFUE), semestre europeu, Painel de Avaliação da Justiça na UE, Mecanismo de Cooperação e Verificação para a Bulgária e Roménia, Programa de Apoio às Reformas Estruturais, Fundos Europeus e o proposto mecanismo de proteção do orçamento da União em caso de deficiências generalizadas no que

---

<sup>75</sup> *Ibid.*

<sup>76</sup> Conclusões do Advogado-Geral M. Poiares Maduro de 21.05.2008, C-127/07 (*Arcelor Atlantique e Lorraine e o.*), n.º 16.

<sup>77</sup> CONSELHO EUROPEU – Conselho Europeu de Copenhaga 21-22 de Junho de 1993. Conclusões da Presidência. Disponível em: <https://www.consilium.europa.eu/media/21225/72921.pdf>.

<sup>78</sup> Para um estudo compreensivo destes mecanismos, veja-se CARRERA et. al. - *The Triangular Relationship...*, p. 12. e ss.

<sup>79</sup> COMISSÃO EUROPEIA - *The EU's Rule of Law toolbox*. 2019. Disponível em: [https://ec.europa.eu/info/sites/info/files/rule\\_of\\_law\\_factsheet\\_1.pdf](https://ec.europa.eu/info/sites/info/files/rule_of_law_factsheet_1.pdf). Consultado em: 15/06/2020.

diz respeito ao Estado de Direito nos Estados-Membro<sup>80</sup>. Merece especial e breve referência o instrumento de supervisão previsto no art.º 7.º TUE, a que está associado um braço corretivo ou preventivo, sempre que se verifique a «*existência de um risco manifesto de violação grave dos valores referidos no artigo 2.º por parte de um Estado-Membro*» (n.º 1), o que permite ao Conselho emitir recomendações a esse EM no sentido de repor o respeito pelos valores fundacionais da UE, e um braço punitivo (n.º 2 e 3) para aquelas situações em que se verifique, já não um risco, mas uma «*violação grave e persistente*» do art.º 2.º TUE, estando o Conselho habilitado a sancionar o EM que viole o art.º 2.º, suspendendo determinados direitos, desde logo o voto desse EM no Conselho. Desde o seu surgimento, com o Tratado de Amesterdão, o art.º 7.º foi sempre descrito pela cúpula da UE como uma «*opção nuclear*»<sup>81</sup> de natureza política, razão pela qual se tenha resistido por mais de uma década à sua utilização. Todavia, fruto da evolução política e constitucional em alguns Estados-Membro, designadamente na Polónia e na Hungria, as instituições têm reputado por necessário o recurso a este mecanismo “forte”. O Estado de Direito desempenha ainda, na UE, uma função externa enquanto “objetivo” de política internacional (art.º 21.º, n.º 1 e n.º 2, al. b) TUE). Neste contexto, o princípio deixa de desempenhar uma função constitucionalmente vinculante, transformando-se, antes, numa “política” que deve guiar os atores europeus na arena internacional, de modo a que seja exportado além das fronteiras europeias através da «*persuasão, incentivo e negociação*»<sup>82</sup>. Também no domínio da política externa, o Estado de Direito aparece como inseparável dos valores da democracia e da defesa dos direitos fundamentais. Em suma, é hoje inquestionável que o Estado de Direito é um princípio constitucional juridicamente vinculativo de DUE<sup>83</sup>.

<sup>80</sup> São notáveis os esforços da Comissão em continuamente acrescentar novas camadas de proteção dos valores fundacionais da UE, naquilo que já é uma complexa estrutura multinível, revelando, deste modo, uma certa ineficiência ou inoperância dos instrumentos existentes (que ou dependem da coragem política dos pares, ou estão sujeitos a maiorias muito reforçadas, ou sequer são vinculativos) e que amiúde esbarram com a relutância nacional em proceder a verdadeiras reformas. A título de exemplo, veja-se a proposta de criação de um “ciclo de análise do Estado de Direito” e de um novo “relatório anual sobre o Estado de Direito”, que foi recentemente publicado. Cfr. COMISSÃO EUROPEIA - *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões. Reforçar o Estado de direito na União. Plano de Ação*. COM(2019) 343 final. Bruxelas, 17.7.2019.

<sup>81</sup> Vide o discurso do “Estado da União” proferido pelo Presidente da Comissão Europeia José Manuel Barroso perante o Parlamento Europeu em 11/09/2013. Disponível em <https://tinyurl.com/yyybzzrs>.

<sup>82</sup> PECH - *The Rule of Law as a Constitutional...*, p. 69.

<sup>83</sup> A este respeito, o TJUE tem sido consistente ao declarar que do Estado de Direito se podem deduzir outros princípios que designa por “princípios gerais de direito que decorrem das tradições constitucionais comuns aos Estados-Membro”, tais como o princípio da legalidade (Ac. de 29.04.2004, C-496/99 P (*Comissão/CAS Succhi di Frutta SpA*), n.º 63), o princípio da segurança jurídica (Ac. de 12.11.1981, C-212/80 (*Meridionale Industria Salumi e o./Amministrazione delle finanze dello Stato*), n.º 10), a proibição da arbitrariedade dos poderes executivos (Ac. de 21.09.1989, C-46/87 (*Hoechst/Comissão*), n.º 19), o controlo judicial independente e eficaz, incluindo o respeito pelos direitos fundamentais - controlo esse que é, segundo o TJUE, uma expressão concreta do Estado de Direitos – (cfr., *inter alia*, Ac. de 27.02.2018, C-64/16 (*Associação Sindical dos Juizes Portugueses/Tribunal de Contas*), o direito a um julgamento equitativo e a separação de poderes (Ac. de 22.12.2010, C-279/09 (*DEB*) e a igualdade perante a lei (Ac. 14-09-2010, C-550/07 P (*Akzo Nobel Chemicals e Akcros Chemicals/Comissão*), n.º 54).

O tratamento até aqui dado ao Estado de Direito justifica-se pela dificuldade na delimitação do princípio, sem que isso signifique que o conceito de democracia seja menos complexo, estando a grande diferença na percepção que a maioria de nós partilha de saber o que é um governo democrático, o que explica a ausência de extensas considerações<sup>84</sup>. Enfim, dizer-se que a democracia se baseia no princípio da igualdade entre cidadãos (ou um *demos*) com direito à sua autodeterminação política ou que corresponde ao sistema político em que o poder do Estado reside no povo que o exerce direta ou indiretamente através de representantes eleitos, é, além de simplista, incapaz de descrever a imensidão de possibilidades *democráticas* (e seus modelos) existentes ou pensadas. À parte estas considerações, interessa-nos referir que tudo o antedito acerca do Estado de Direito na UE é, *mutatis mutandis*, válido para os valores da democracia e da proteção dos direitos fundamentais. Esta adivinhada sobreposição implica que nem sempre seja fácil distinguir os valores referidos no art.º 2.º TUE. Estes valores, ainda que possam existir e ser analisados de forma independente uns dos outros, têm de ser sempre encarados em conjunto, o que nos leva à conclusão de que, na verdade, existe uma indivisibilidade e interconetividade entre Estado de Direito, democracia e direitos fundamentais<sup>85</sup>. Assim, «*no Direito Constitucional Europeu, o Estado de Direito partilha uma ligação substancial, até mesmo orgânica, com os restantes princípios fundacionais*» mencionados no art.º 2.º TUE, daqui resultando que «*todos os princípios referidos*» no art.º 2.º TUE «*são interdependentes e devem ser construídos à luz uns dos outros*»<sup>86</sup>. Nestes termos, a UE é fundada *simultânea e necessariamente* em todos os valores mencionados no art.º 2.º TUE. Logo, a violação de um desses valores significa que nenhum dos outros pode ser verdadeiramente respeitado, precisamente pela relação de interdependência em que se encontram. De tal forma assim é que há autores que defendem que entre democracia, Estado de Direito e direitos fundamentais se estabelece, na UE, uma «*relação triangular*» representada num «*diagrama de venn*»<sup>87</sup>. Essa relação parte do reconhecimento de que estamos perante três pilares de um edifício que ruirá se um estiver em falta. É, então, do reconhecimento de que sem Estado de Direito não existe democracia e proteção dos direitos fundamentais e vice-versa, uma vez que cada elemento é intrínseco aos outros, que chegamos ao Estado de Direito democrático. O Estado de Direito democrático pressupõe um processo de adoção de normas e prioridades políticas democrático,

<sup>84</sup> Para mais, vide FRANKENBERG, Günter - *Democracy*. In ROSENFELD, M.; SAJÓ, A. - *The Oxford Handbook of Comparative Constitutional Law*. Oxford: Oxford University Press, 2012. p. 234 e ss.

<sup>85</sup> De acordo com a Carta de Paris para uma Nova Europa, o «*governo democrático baseado na vontade do povo, expressa regularmente através de eleições livres e justas. A Democracia funda-se no respeito pela pessoa humana e no Estado de Direito*»

<sup>86</sup> PECH - *The Rule of Law as a Constitutional...*, p. 54.

<sup>87</sup> CARRERA et. al. - *The Triangular Relationship...*, p. 27 e ss..

pluralista, transparente, equilibrado, legítimo e credível, em que se respeitem quer os elementos formais, quer os elementos substanciais. Pressupõe, também, que as eleições sejam livres, justas e imparciais, antecedidas de um debate de ideias ancorado numa opinião pública racional em que todos os agentes e visões se encontram, à partida, em pé de igualdade, e em que a opinião da maioria se encontra limitada pelo Estado de Direito e pelos direitos fundamentais<sup>88</sup>. Se estas características estiverem em crise, ora porque inexistem, ora porque estão a ser viciadas, é o próprio Estado de Direito democrático que está em causa.

## CAPÍTULO II – QUE PERIGOS?

Numa entrevista de 2017, EVAN WILLIAMS, um dos cofundadores do Twitter, passando em revista a ascensão das redes sociais, dizia ter acreditado que *«assim que toda a gente pudesse falar livremente e trocar informação e ideias, o mundo seria, automaticamente, um lugar melhor»*, para logo acrescentar que *«estava enganado»*<sup>89</sup>. EVGENY MOROZOV, referindo-se à (des)ilusão da *internet*, nota que *«para quem deseja que a democracia prevaleça nos ambientes mais hostis e improváveis, a primeira década do novo milénio foi marcada por um sentimento de amarga decepção, senão mesmo de absoluta desilusão»*<sup>90</sup>. De facto, a alvorada da tecnologia digital foi vista não só como marco histórico, mas como via democrática promissora, não sendo exagerado dizer que ainda hoje persiste um certo “endeusamento” das tecnologias digitais nas suas variadas expressões. A Era Digital, na sua ubiquidade e conectividade, pode, realmente, resultar num importante contributo para o aperfeiçoamento do processo democrático e de participação política e cívica. Todavia, seria ingénuo não reconhecer que a “hiperconectividade” em que nos movemos neste princípio de década vem transformando os valores e as identidades individuais (quantas vezes no sentido de seu empobrecimento) e, por consequência, as próprias sociedades. Assim, se a massificação dos *digital media* resulta em mais (liberdade de) expressão (e) de opinião, o aumento da participação pode não ser necessariamente benéfico para o Estado de Direito democrático. Do mesmo passo, a expansão em linha, virtualmente ilimitada, dos horizontes das liberdades tem tornado públicos novos e crescentes anátemas para as mais diversas áreas da vida comum. Paradoxalmente, o combate a estes novos perigos, ainda que dentro das regras do jogo democrático, pode, como veremos, causar constrangimentos inadmissíveis à liberdade de expressão, de opinião, de informação e

<sup>88</sup> MIRANDA, Jorge – *Manual de Direito Constitucional*. 4.<sup>a</sup> ed. (rev. e atual.) Coimbra: Coimbra Editora, 2008. Tomo IV – Direitos Fundamentais. p. 227.

<sup>89</sup> *Apud* STREITFELD, David - *The Internet Is Broken*. The New York Times. (20 Mai. 2017).

<sup>90</sup> MOROZOV, Evgeny - *The Net Delusion: how not to liberate the world*. London: Penguin Books, 2011. p. ix.

de imprensa, num continuado e difícil equilíbrio em que os líderes atuam como funâmbulos.

### Secção I – Verdade e desinformação.

Em 2016, no rescaldo do referendo relativa à permanência ou saída do Reino Unido na União Europeia e das eleições presidenciais nos Estados Unidos, os dicionários Oxford elegeram “pós-verdade” como a palavra do ano, relacionando-a com as *«circunstâncias em que as pessoas respondem mais a emoções e crenças do que a factos»*<sup>91</sup>. Na mesma linha, vários autores destacam que na era da pós-verdade os factos e as evidências (muitas delas científicas, como acontece com a negação das alterações climáticas) são postergados em benefício das crenças pessoais e das emoções habilmente exploradas na esfera pública digital<sup>92</sup>, construindo-se *«narrativas sobre os acontecimentos do mundo que se impõem aos próprios acontecimentos ou factos ditos “objetivos”, sobretudo pela forma como são “costuradas” e repetidas ou “viralizadas” nos media digitais»*<sup>93</sup>. Neste ambiente, crenças e informações cuja credibilidade se queda por verificar são difundidas como se de factos reais se tratassem, o que dá origem a uma terceira categoria que vai além da verdade e da mentira, e se situa numa *«zona eticamente cinzenta»*<sup>94</sup> onde informação falsa, dúbia, ambígua ou inverificável é, ao estilo nietzschiano, apresentada apenas como uma outra (ou apenas mais uma) interpretação (ou versão) de certa realidade ou acontecimento<sup>95</sup>. Para alguns autores as *fake news* são *«o rosto mais visível da pós-verdade»*<sup>96</sup>. Debruçando-se sobre a temática, e usando como exemplo a negação das alterações climáticas, LEWANDOWSKY et. al. concluiu que a *pós-verdade* está diretamente relacionada como um novo *«espaço epistémico»* em que se *«abandonaram os critérios convencionais de evidência, de consistência interna e de verificação de factos»*. Assim, *«a maioria das afirmações pós-verdadeiras não pretendem estabelecer um modelo coerente da realidade. Pelo contrário, elas erodem a confiança nos factos e na realidade ao ponto de os factos não mais interessarem ou não mais serem reconhecidos como reais»*<sup>97</sup>. A

<sup>91</sup> Vide <https://www.oxfordlearnersdictionaries.com/definition/english/post-truth?q=post-truth>.

<sup>92</sup> ROCHLIN, Nick - *Fake news: belief in post-truth*. Library Hi Tech. Vol. 35. n.º 3 (2017).

<sup>93</sup> PRIOR, Hélder - *Em nome do povo: populismo e o novo ecossistema mediático*. In FIGUEIRA, J.; SANTOS, S. - *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Coimbra: Imprensa da Universidade de Coimbra, 2019. p. 139.

<sup>94</sup> KEYES, Ralph - *The Post-Truth Era*. New York: St. Martin's Press, 2004. p. 16.

<sup>95</sup> Ou, nas palavras virais de Kellyanne Conway aquando do “debate” em torno do número de pessoas que assistiu à tomada de posse do Presidente dos EUA, “*factos alternativos*”.

<sup>96</sup> AMARAL, Inês; SANTOS, Sofia José - *Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade*. In FIGUEIRA, J.; SANTOS, S. - *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Coimbra: Imprensa da Universidade de Coimbra, 2019. p. 71.

<sup>97</sup> LEWANDOWSKY, S.; ECKER, U.; COOK, J. - *Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era*. Journal of Applied Research in Memory and Cognition. Vol. 6. n.º 4 (2017). p. 360. e ss.

contribuir para este estado de coisas, os Autores apontam algumas tendências, como o declínio do “capital social” (identificado como boa-vontade, empatia, confiança entre os cidadãos e nas instituições e envolvimento cívico), a crise de valores, as crescentes desigualdade, o recrudescimento da polarização<sup>98</sup>, o declínio de confiança na ciência e nas instituições e a gradual fragmentação da paisagem mediática, com destaque para o papel informativo hoje desempenhado pelas redes sociais e as suas *filter bubbles* e *echo chambers* que *infra* analisaremos<sup>99</sup>. Ora, estando a “*pós-verdade*” reportada, sobretudo, a uma zona emocional e irracional, a sua prevalência no discurso público tem consequências no funcionamento das democracias. De facto, qualquer modelo político que se baseie numa democracia deliberativa como modelo de legitimação das decisões e escolhas políticas, deve olhar com cautela para o “uso público da razão”, na celebrizada expressão de Kant. Ora, sendo a deliberação pública essencial à democracia liberal, e partindo esta de um esforço racional em que cidadãos com visões políticas, religiosas e sociais distintas chegam a um consenso quanto à «*mais razoável conceção política de justiça*»<sup>100</sup>, a emocionalização do discurso na esfera pública cria distorções e pode levar ao retrocesso da democracia e do Estado de Direito<sup>101</sup>. Aberta esta via, é mais ou menos óbvia a relação entre poder/política e verdade, na medida em que o primeiro sempre se vê tentado a interferir (senão mesmo ditar) a segunda<sup>102</sup>. Identificando as «*más relações*» entre a verdade e a política, HANNAH ARENDT explica que «*as mentiras foram sempre consideradas como instrumentos necessários e legítimos, não apenas na profissão de político ou demagogo, mas também na de homem de estado*»<sup>103</sup>. Invocando a tradição da filosofia pré-moderna de que o homem não é capaz de verdade, sendo todas as verdades simples opiniões, ARENDT tenta gizar a diferença entre factos (verdades) e opiniões, dizendo que «*os factos e as opiniões não se opõem uns aos outros, pertencem ao mesmo domínio. Os factos são a matéria das opiniões, e as opiniões, inspiradas por diferentes interesses e diferentes paixões, podem diferir largamente e permanecer legítimas enquanto respeitarem a verdade de facto*». Embora reconheça a

<sup>98</sup> Relativamente à polarização política, social e ideológica das sociedades, vide NEUDERT, Lisa Maria; MARCHAL, Nahema - *Polarisation and the use of technology in political campaigns and communication*. Brussels: European Parliamentary Research Service, 2019.

<sup>99</sup> LEWANDOWSKY et. al., *Beyond Misinformation...*, p. 357 e ss.

<sup>100</sup> RAWLS, John - *The Idea of Public Reason Revisited*. The University Of Chicago Law Review. Vol. 64. n.º 3 (1997). p. 773.

<sup>101</sup> Já LOEWENSTEIN ensinava em 1937 que os governos autoritários e ditatoriais se fundam em técnicas emocionalistas, tais como o entusiasmo nacionalista, a política coerciva do medo, a intimidação e a aterrorização aplicados com laivos científicos. Cfr. LOEWENSTEIN, Karl - *Militant Democracy and Fundamental Rights, I*. The American Political Science Review. Vol. 31. n.º 3 (1937).

<sup>102</sup> A propósito da relação entre poder, política e verdade vide o interessante texto, que aqui seguiremos, de SÁ, Alexandre Franco de - *Pré-verdade, verdade e pós-verdade: um percurso rumo à política contemporânea*. In FIGUEIRA, J.; SANTOS, S. - *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Coimbra: Imprensa da Universidade de Coimbra, 2019.

<sup>103</sup> ARENDT, Hannah - *Entre o Passado e o Futuro*. Lisboa: Relógio D'Água, 2006. p. 237.

dificuldade em separar a opinião e a interpretação do facto, a Autora defende que «*mesmo se admitirmos que cada geração tem o direito de escrever a sua história, recusamo-nos a admitir que cada geração tenha o direito de recompor os factos de harmonia com a sua própria perspectiva; não admitimos o direito de se atentar contra a própria matéria factual*», até porque todas as verdades (i.e., todos os factos) são diferentes das opiniões (e das interpretações) no momento da asserção da sua validade, uma vez que «*a verdade contém em si mesma um elemento de coerção*» e um «*caráter despótico*», estando para lá da discussão, do acordo e do debate<sup>104</sup>. Apesar de ser assim, e porque os factos teriam sempre podido ser outros, «*a verdade de facto não é mais evidente que a opinião*», sendo essa uma das razões pelas quais os detentores de opinião consideram relativamente fácil rejeitar a verdade como se fosse uma opinião. Nesta encruzilhada, ARENDT procura, enfim, uma «*marca distintiva*» para a verdade de facto, concluindo que ela só pode ser a circunstância de o contrário da verdade não ser nem o erro (apesar de ele existir), nem a ilusão, nem a opinião, «*mas a falsidade deliberada ou a mentira*». A confusão entre factos e opiniões serve a tentativa de destruição de um mundo político plural, fragilizando a política contemporânea.

Aqui chegados, e sabendo que as tentativas de influenciar os membros de uma comunidade política são tão antigas quanto a existência dessas mesmas comunidades<sup>105</sup>, pode parecer estranho o exacerbamento desta temática a partir de 2016, que, no caso da União Europeia, culminou com uma preocupação sem precedentes com a integridade das eleições de 2019 para o Parlamento Europeu<sup>106</sup>. Na verdade, o que parece tornar este momento peculiar é a ocorrência de campanhas de desinformação estrategicamente organizadas (com profissionais e planos de ação concertadas), bem financiadas, com a intenção de influenciar os processos políticos<sup>107</sup> ou de atentar contra certos bens e valores públicos. Conforme a análise dos casos mais mediáticos tem demonstrado<sup>108</sup>, essas campanhas de desinformação podem ter origem interna ou externa,

<sup>104</sup> Para ilustrar esta ideia, refere a Autora que «*pode-se discutir uma opinião importuna, rejeitá-la ou transigir com ela, mas os factos importunos têm a exasperante tenacidade que nada pode abalar a não ser as mentiras puras e simples. O aborrecido é que a verdade de facto, como toda a verdade, exige perentoriamente o reconhecimento e recusa a discussão enquanto que a discussão constitui a própria essência da vida política*».

<sup>105</sup> Para mais sobre a história da propaganda e da persuasão vide JOWETT, Garth S.; O'DONNELL, Victoria - *Propaganda and persuasion*. 5ª ed. Washington DC: SAGE, 2012. p. 51 e ss.

<sup>106</sup> De facto, no seu discurso do Estado da União 2018, o então Presidente da Comissão, Jean-Claude Juncker, sublinhou a urgência do momento, reiterando que «*no nosso mundo em linha, o risco de interferência e de manipulação [das eleições europeias] jamais foi tão elevado. Chegou o momento de adaptar as nossas regras eleitorais à era digital, a fim de proteger a democracia europeia*» (vide <https://tinyurl.com/y69ec1ll>).

<sup>107</sup> BAYER, Judit; BITIUKOVA, Natalija; BÁRD, Petra; SZAKÁCS, Judit; ALEMANN, Alberto; USZKIEWICZ, Erik - *Disinformation and propaganda - impact on the functioning of the rule of law in the EU and its Member States*. [s.l.]: European Parliament, 2019. p. 15.

<sup>108</sup> A preocupação da opinião pública em torno destas temáticas é, também, crescente: em 2018, num Eurobarómetro antevendo as eleições para o Parlamento Europeu do ano seguinte, 61% dos cidadãos da UE

sendo comuns a todo o espectro político. Segundo um estudo de 2018 do *Oxford Computational Propaganda Research Project*, dos 48 países analisados, em todos foram encontradas evidências de campanhas de desinformação organizadas através das redes sociais<sup>109</sup>. A ocorrência cada vez mais frequente de episódios de desinformação está relacionada com o aparato tecnológico da Era Digital, que, por um lado, torna mais fácil e menos dispendiosa a organização destas campanhas, a que se associa a maior probabilidade do seu sucesso e a virtual ausência de riscos<sup>110</sup>. Por outro lado, a forma como a informação é produzida e distribuída transformou-se, tendo dado origem a um ambiente informativo caracterizado pela facilidade e rapidez de criação e distribuição de conteúdos, pelo consumo público, em lugar de privado, da informação (sobretudo nas redes sociais), e pela ausência de uma rede de *gatekeepers* que confirmem credibilidade à informação transmitida<sup>111</sup>.

Antes de avançarmos mais, convém proceder a algumas precisões terminológicas. O termo popularizado a partir das eleições presidenciais americanas para descrever um conjunto muito lato de fenómenos relacionados com a “desordem informativa”, foi o de *fake news*. Todavia, vários autores concordam que o termo, por ser vago e ambíguo<sup>112</sup>, não é o mais adequado para descrever a complexidade do fenómeno da desinformação, uma vez que este não se limita às notícias, mas a «*todo um ecossistema informativo*»<sup>113</sup>, que inclui o recurso à automatização, à manipulação ou fabricação de elementos vídeos e imagens, ao *trolling*, ao *microtargeting*, à forma de circulação dessa informação, entre outros. Por outro lado, o termo tem, ao longo dos anos, servido para descrever outras realidades, como notícias satíricas, paródias, manipulação, propaganda e publicidade<sup>114</sup>. Por fim, a designação pode, em si mesmo, induzir em erro, uma vez que as *fake news* não têm necessariamente de ser absolutamente falsas, podendo, v.g., partir de uma base factual descontextualizada ou imprecisa. Não obstante, vários têm sido os esforços para encontrar uma definição para *fake news*. Seguindo de perto a definição oferecida por REGINA RINI, uma notícia falsa é aquela que pretende, aparentemente, descrever um ou mais

---

inquiridos temiam que as eleições pudessem ser manipuladas, 59% temiam que essa manipulação pudesse ter origem em intervenientes externos e grupos criminosos, ao passo que 67% dos inquiridos receava que os dados pessoais *online* pudessem ser utilizados para o micro-direcionamento de mensagens políticas. COMISSÃO EUROPEIA – *Eurobarómetro Especial 477 – Setembro 2018. Democracia e eleições. Sumário*. Bruxelas, 2018.

<sup>109</sup> BRADSHAW, Samantha; HOWARD, Philip N. - *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. The Computational Propaganda Project, 2018.

<sup>110</sup> BAYER et. al. – *Disinformation and propaganda...* p. 15.

<sup>111</sup> WARDLE, Claire; DERAKHSHAN, Hossein - *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Strasbourg: Council of Europe, 2017. p. 11 e ss.

<sup>112</sup> Num sentido latíssimo, ROCHLIN, *Fake news: ...*, p. 388, refere que o termo *fake news* veio significar «qualquer história que atenta contra as crenças e as emoções de uma pessoa».

<sup>113</sup> WARDLE, Claire - *Fake news. It's complicated*. First Draft. [Em linha] (2017).

<sup>114</sup> Uma outra razão avançada por WARDLE et. al. – *Information Disorder...*, p. 16 para se evitar a utilização do termo *fake news* é a circunstância de o mesmo ser aproveitado por vários atores políticos para descrever organizações notícias e jornalistas cuja cobertura noticiosa é considerada contrária aos seus interesses e visões.

eventos reais, normalmente mimcando as fórmulas noticiosas dos meios de comunicação tradicionais, atuando os seus autores, todavia, com a consciência de que aquela notícia é significativamente (podendo não ser totalmente) falsa, enganadora, imprecisa ou distorcida, sendo intencionalmente transmitida com pelo menos um de dois objetivos: ser retransmitida em grande escala e ludibriar parte da sua potencial audiência<sup>115</sup>. Nestes termos, as *fake news* não incluem os erros jornalísticos (por falta do elemento intencional), nem, a nosso ver, as paródias ou sátiras sobre a forma de notícia que possam facilmente ser identificadas como tal<sup>116</sup>, e os rumores ou teorias da conspiração que não emergem de um artigo noticioso. MARTENS et. al. distinguem entre um conceito estrito e um conceito lato de *fake news*, limitando-se o primeiro apenas a informações falsas que possam ser verificáveis enquanto tal através, por exemplo, do *fact-checking*, ao passo que o conceito lato abrange também tentativas deliberadas de distorcer e manipular a informação criada, produzida, apresentada e distribuída *online*<sup>117</sup>. Assim, e na ausência de um conceito consensualmente aceite pela doutrina, há pelos menos dois elementos essenciais em qualquer notícia falsa: [i] a intenção de enganar ou ludibriar [ii.] e o elemento manipulativo, que tanto pode corresponder a uma narrativa completa ou parcialmente falsa (na sua aceção mais restrita), como a uma narrativa descontextualizada, confusa, imprecisa, contraditória, obscura ou, simplesmente, inverificável (na aceção ampla).

WARDLE et. al. introduziram no debate o termo “desordem informativa” para abranger três distintas categorias de conteúdos: *dis-information*, *mis-information* e *mal-information*<sup>118</sup>. A categorização ora encetada baseia-se em duas questões: os conteúdos são verdadeiros (mas ainda assim têm como objetivo prejudicar ou casuar dano a terceiros)? Os conteúdos são criados, produzidos ou distribuídos com a intenção de enganar? Ora, se os conteúdos não são verdadeiros e são criados, produzidos ou distribuídos com a intenção de ludibriar (independentemente do objetivo), então estaremos perante um fenómeno de *dis-information*. Se, todavia, os conteúdos não forem verdadeiros, mas faltar o elemento intencional, estaremos já perante um caso de *mis-information*. Contudo, se os conteúdos forem verdadeiros, mas existir, desta feita, uma intenção de causar dano ou de prejudicar uma pessoa, uma organização, instituição ou um Estado, essa será uma situação de *mal-information*. Caem nesta última categoria o discurso de ódio, o assédio *online* e os *leaks*. Na categoria da informação errónea cabem, por exemplos, os erros jornalísticos. Na *dis-information* raentram conteúdos sem

<sup>115</sup> RINI, Regina - *Fake news and partisan epistemology*. Kennedy Institute of Ethics Journal. Vol. 2. n.º 2 (2017).

<sup>116</sup> Típicas de jornais como o «The Onion» ou, em Portugal, o «Inimigo Público».

<sup>117</sup> MARTENS, Bertin; AGUIAR, Luis; HERRERA-GOMEZ, Estrella; MUELLER-LANGER, Frank - *The digital transformation of news media and the rise of disinformation and fake news*. Seville: Comissão Europeia, 2018.

<sup>118</sup> WARDLE et. al., *Information Disorder...*, p. 20. Apesar da dificuldade, traduziríamos estras três categorias para português do seguinte modo: desinformação, informação errónea ou errada e informação danosa.

correspondência com a realidade, artigos cujo título, subtítulo, imagens ou legendas não tenham correspondência com o conteúdo, conteúdos genuínos, mas partilhados com contextos falsos, conteúdos totalmente fabricados ou manipulados<sup>119</sup>. Apesar destas distinções, é comum que os termos *disinformation* e *misinformation* sejam utilizados como sinónimos.

Acrescentando mais um elo à cadeia, a categorização analisada parte da dicotomia entre verdade e falsidade dos conteúdos informativos que circulam no espaço público. Porém, e como reconhece BAYER et. al., a prática tem revelado que os agentes responsáveis pelos atos de manipulação não se posicionam necessariamente nessa dicotomia entre o facto e o não-facto, antes podendo produzir conteúdos insuscetíveis de prova, inverificáveis ou carregados de efeitos emocionais, destinados a causar o medo ou a exacerbar divisões e polarizações políticas e sociais, naquilo que se traduz em «*manipulação através de práticas informacionais agressivas*»<sup>120</sup>. Estas práticas manipulativas, que podemos exemplificar com a criação e difusão de narrativas distintas e contraditórias entre si<sup>121</sup> ou com a publicação de mensagens contendo juízos de valor impossíveis de verificar objetivamente, não estão abrangidas pelo conceito estrito de *fake news*, embora recaiam no âmbito do conceito amplo, conforme antes explicado. Atendendo à dimensão deste fenómeno e às suas potenciais consequências, designadamente o perigo da polarização e a exploração das vulnerabilidades emocionais dos cidadãos, a manipulação dos cidadãos através de práticas informacionais agressivas não pode ser ignorada, advogando-se aqui uma definição mais inclusiva.

Na senda desta categorização, as instituições europeias e vários governos nacionais optaram por adotar o termo desinformação. No caso da Comissão Europeia, a desinformação é descrita como «*informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público. O prejuízo público abrange ameaças aos processos*

<sup>119</sup> Usando como exemplo as eleições presidenciais francesas de 2017, as notícias que afirmavam que um dos candidatos era financiado pela Arábia Saudita ou a inundação de *tweets* que afirmava que o mesmo candidato tinha um caso com a sua enteada são exemplos claros de desinformação. Já as informações, muitas delas partilhadas nas redes sociais, que sucederam ao ataque nos Campos Elísios (20/04/2017) e que davam conta, por exemplo, da morte de um segundo polícia, são casos de informação errónea, partilhada sem nenhuma intenção de enganar terceiros. Finalmente, um exemplo de *mal-information*, ainda durante essa campanha, foi o *leak* de vários e-mails de campanha publicados poucos dias antes da segunda volta das eleições e já durante o período de reflexão. WARDLE et. al., *Information Disorder...*, p. 21.

<sup>120</sup> BAYER et. al., *Disinformation and propaganda...*, p. 27-28.

<sup>121</sup> A 21 de maio de 2016, no Texas, agentes associados à IRA, uma organização russa encarregue de várias ciberoperações de manipulação e influência interna e externa, convocaram através de duas páginas do Facebook (ambas geridas pela IRA) dois protestos em Houston, o primeiro com o título “*Stop Islamization of Texas*” e o segundo com o título “*Save Islamic Knowledge*”. Em ambos os casos recorreu-se a anúncios pagos micro-direcionados. Os protestos acabaram em confrontos entre os manifestantes. Cfr. UNITED STATES SENATE – *Report on the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*. Vol. 2 (*Russia’s use of social media with additional views*). p. 47.

*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*»<sup>122</sup>. A Comissão parece adotar aqui um conceito restrito de desinformação ao fazer depender a classificação de três eixos principais: [i.] o caráter “comprovadamente” falso ou enganador do conteúdo, o que pressupõe uma qualquer verificação através, por exemplo, do *fact-checking*; [ii.] a intenção subjacente à divulgação dos conteúdos, que só pode ser a obtenção de vantagens económicas e/ou o logro deliberado da opinião pública; e [iii.] a consequência, que se traduz necessariamente num prejuízo público, que tanto pode ser reportado ao processo democrático (por exemplo, a interferência em eleições) como a certos bens públicos<sup>123</sup>. É preciso notar que o conceito de desinformação não abrange conteúdos que já caíam dentro de outras categorias estabelecidas nas legislações nacionais ou europeia, tais como o discurso de ódio, o incitamento à violência, a difamação, a injúria, a ofensa ao bom nome, a violação de direitos da propriedade intelectual, entre outros. Por outro lado, as perturbações originadas pela desinformação estão para além das fraudes, dos mitos e dos logros que há muito são conhecidos dentro e fora do mundo *online*, assumindo, agora, um declarado escopo de interferência no espaço público digital que é potencialmente danoso para a formação e manutenção de uma esfera pública informada e racional sem a qual a democracia deliberativa e participativa é insustentável, além de poder significar um prejuízo real para determinados bens como a saúde humana (potencialmente, as campanhas de desinformação anti-vacinas ou as recentes notícias em torno da COVID-19<sup>124</sup>), o ambiente (sendo o caso paradigmático da negação das alterações climáticas), a verdade científica ou a educação.

Apesar dos esforços até aqui desenhados, é forçoso admitir que tanto o conceito de *fake news*, como as categorias inerentes à “desordem informativa” são esquivas e pouco rigorosas, estando a fixação definitiva dos seus contornos ainda dependente de desenvolvimentos científicos.

<sup>122</sup> Esta definição exclui explicitamente «erros na comunicação de informações, sátiras, paródias ou notícias e comentários claramente identificados como partidários». Cfr. COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Combater a desinformação em linha: uma estratégia europeia*. COM (2018) 236 final, Bruxelas 26.4.2018, p. 4.

<sup>123</sup> Não obstante ser adotada por vários governos nacionais (v.g.: irlandês e belga), a definição de desinformação da CE não é a única em uso na UE. Por exemplo, o Grupo de Especialistas de Alto Nível em *Fake News* e *Desinformação Online* definiu a desinformação como «informações falsas, imprecisas ou enganadoras, criadas, apresentadas e promovidas de modo a causar, intencionalmente, um dano público ou para a obtenção de lucro». HIGH LEVEL GROUP ON FAKE NEWS AND ONLINE DISINFORMATION - *A multi-dimensional approach to disinformation*. Comissão Europeia, 2018. p. 10.

<sup>124</sup> Quer no caso do movimento anti-vacina, quer no caso da informação em torno da COVID-19, não é ainda claro que estejamos perante fenómenos de desinformação no sentido aqui apresentado, precisamente por estar por provar existir – no momento da criação ou da distribuição – o elemento intencional *supra* apontado. Não obstante, dúvidas não se colocam quanto a tratar-se de conteúdos prejudiciais para valores e bens públicos como a saúde. Com razão, o Organização Mundial de Saúde refere que, além da pandemia, temos também de aprender a lidar com uma “infodemia”, caracterizada por um excesso de informação – alguma verdadeira e outra não – que torna difícil que os cidadãos encontrem fontes confiáveis num momento em que mais delas precisam.

Nesta sede, uma das grandes dificuldades é a sobreposição e multiplicação *ad infinitum* de termos, tornando heróica a destriça entre os conceitos e a possibilidade da adoção de uma linguagem comum entre os vários interessados, além de a amplitude com que os conceitos são tratados contribuir para um certo relativismo terminológico em que tudo é manipulação. Colocados perante a necessidade de tomar posição, e ainda que descrevendo imperfeitamente a complexidade do fenómeno, faremos uso do termo desinformação por ser aquele que tem sido consistentemente adotado na UE. No entanto, e em face da definição avançada pela CE, alargaremos esse conceito para incluir as práticas agressivas, manipulativas e divisionistas *online* que escapam à verdade ou falsidade, antes se concentrando em processos comunicacionais inverificáveis e altamente sugestivos e emotivos.

Ultrapassado o escolho terminológico, é imperativo olhar para o fenómeno desinformativo e questionar “quem?, como?, porquê? e com que consequências?” As respostas a estas questões equivalem à análise dos elementos e das fases da desinformação. Conforme sumariza WARDLE et. al.<sup>125</sup>, os elementos da desinformação são essencialmente três: [i.] o agente, [ii.] a mensagem e [iii.] o intérprete ou destinatário; igualmente três são as fases do fenómeno, designadamente a (1) criação da mensagem, (2) a produção da mensagem (transformada, nesta fase, num produto mediático) e a sua (3) distribuição, a que BAYER et. al. junta uma quarta fase de (4) amplificação da mensagem<sup>126</sup>. Concentrando-nos nos elementos da desinformação, sabemos que os agentes (podemos ter vários agentes diferentes com motivações distintas a atuar em cada uma das fases da desinformação) tanto «*podem ser internos (localizados nos Estados-Membros) ou externos, podendo tratar-se de agentes estatais (ou patrocinados por um governo) ou não estatais*»<sup>127</sup>. Entre os atores oficiais/estatais, o país mais investigado na literatura é a Federação Russa, sistematicamente considerada pelas instituições europeias e pela NATO como uma das maiores ameaças ao ambiente informativo europeu<sup>128</sup>, sobretudo devido

<sup>125</sup> WARDLE et. al., *Information Disorder...*, p. 22 e ss.

<sup>126</sup> BAYER et. al., *Disinformation and propaganda...*, p. 30 e ss. Esta dinâmica pode ser exemplificada com um caso real: durante a campanha para as eleições presidenciais norte-americanas de 2016, uma das peças de desinformação que alcançou enorme audiência nas redes sociais foi a notícia de que o Papa teria “chocado o mundo” ao publicar uma declaração apoiando um dos candidatos. O criador da mensagem não é conhecido (embora pareça existir ligações aos *spammers* da Macedónia), tendo sido a mesma produzida enquanto notícia e publicada num *website* designado “WTOE 5 NEWS”, parte de uma rede composta por quarenta e três *websites* dedicados à publicação de conteúdos fabricados. Depois de publicada, a notícia é distribuída pela rede de *sites* e amplificada através das redes sociais, onde inicialmente é publicada em contas automatizadas, sendo depois partilhado pelos apoiantes do candidato e por outros grupos organizados com interesse em semear a divisão e a confusão (v.g.: a IRA), acabando, por fim, a ser partilhado pelos apoiantes do outro candidato (para provar como o “outro lado” é facilmente manipulável) o que despoleta o interesse dos *media* tradicionais.

<sup>127</sup> COMISSÃO EUROPEIA e ALTA REPRESENTANTE DA UNIÃO PARA OS NEGÓCIOS ESTRANGEIROS E A POLÍTICA DE SEGURANÇA – *Comunicação conjunta ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Plano de Ação contra a Desinformação*. JOIN (2018) 36 final, Bruxelas, 5.12.2018, p. 4.

<sup>128</sup> Cfr., *inter alia*, as Conclusões do Conselho Europeu de 19 e 20 de 2015, p. 5.

à prevalência, no seu discurso militar, do conceito de “guerra de informação”, o qual «*não se limita aos períodos de guerra*», antes correspondendo a uma «*atividade permanente independentemente do estado das relações com o adversário*»<sup>129</sup>. A “guerra de informação”, desenvolvida tanto em tempos de paz como de conflito, abrange um vasto conjunto de atividades e processos que procuram subtrair, plantar, interditar, manipular, distorcer ou destruir informação através dos mais variados canais, incluindo os meios digitais e os *media* tradicionais. Segundo PAUL et. al., o modelo desinformativo contemporâneo da Federação Russa assenta em quatro características distintas, designadamente o enorme volume de conteúdos produzidos e a utilização de vários canais de comunicação, o caráter rápido, continuo e repetitivo da divulgação e amplificação dos conteúdos, e a falta de compromisso com a realidade dos factos (o que não quer dizer que os conteúdos sejam sempre fabricados, embora muitas vezes assim aconteça<sup>130</sup>) ou com a consistência das narrativas, uma vez que é bastante comum a divulgação de mensagens contraditórias e inconsistentes entre si<sup>131</sup>. Entre os meios de comunicação social financiados pelo governo russo destacam-se o canal televisivo “RT” (anteriormente, “*Russia Today*”) e a agência noticiosa “*Sputnik*”, ambos destinados a levar ao ocidente uma “versão alternativa do mundo”. Além destes dois meios, outras técnicas de criação, distribuição e amplificação da desinformação são tipicamente usadas, como o recurso às fábricas ou quintas de *trolls* e aos *bots*, de que serve de exemplo a IRA (ou *Internet Research Agency*), uma organização que, em 2015, empregava centenas de jovens russos na criação, distribuição e amplificação de campanhas de manipulação e desinformação, e que terá tido um papel relevante na interferência nas eleições presidenciais norte-americanas de 2016<sup>132</sup>.

A motivação dos agentes da desinformação é variável, podendo ser política e ideológica, financeira ou social e psicológica<sup>133</sup>. Embora os objetivos políticos possam, à primeira vista,

<sup>129</sup> GILES, Keir - *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016. p. 4

<sup>130</sup> É o caso da cobertura pelos meios de comunicação russos da alegada história de uma menina de russo-alemã de 13 anos que teria sido raptada, espancada e violada por três migrantes de origem árabe na Alemanha. A notícia foi várias vezes desmentida pelas autoridades alemãs, mas os desmentidos não conseguiram superar a cobertura mediática do tema, por exemplo pela estação televisiva russa RT e pelas forças alemãs de extrema-direita, o que levou a protestos nas ruas. Cfr. SINGER, Peter Warren; BROOKING, Emerson T. - *Likewar: the weaponization of social media*. New York: First Mariner Books, 2018. p. 206-7.

<sup>131</sup> Ao ponto de existirem tantas versões contraditórias sobre um determinado evento que se cria no público a convicção de que é impossível encontrar a verdade. Foi precisamente esta a estratégia adotada na cobertura do voo 17 da *Malaysia Airlines*, que se despenhou no leste da Ucrânia, tendo sido avançadas pelos órgãos de comunicação pró-russos dezenas de teorias contraditórias. Como refere VILMER et. al., *Information Manipulation...*, p. 75, «o objetivo do Kremlin não é persuadir-nos da existência de uma verdade alternativa, mas antes acreditarmos que a verdade objetiva nem sequer existe, de modo a semear confusão e a paralisar qualquer ação». Cfr., ainda, PAUL, Christopher; MATTHEWS, Miriam - *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND Corporation, 2016.

<sup>132</sup> Para um olhar sobre os detalhes da operação da IRA cfr. o artigo publicado por CHEN, Adrian – *The Agency*. *The New York Times*. (02 junho 2015).

<sup>133</sup> WARDLE et. al., *Information Disorder...*, p. 33 e ss.

ser os mais óbvios e habituais das campanhas de desinformação, principalmente quando levadas a cabo em períodos eleitorais ou com mensagens eminentemente políticas, as razões financeiras não devem ser ignoradas. De facto, existem modelos de negócio inteiramente baseados nas campanhas de desinformação, graças às formas modernas de obtenção de receitas e lucros *online*<sup>134</sup>. Vários exemplos podem ser dados destas motivações, desde a “quinta ou fábrica de cliques” operada a partir da pequena cidade de Veles na Macedónia, onde mais de cem falsos *websites* noticiosos, publicando milhares de histórias durante as presidenciais norte-americanas de 2016, eram geridos por um grupo de jovens adolescentes que conseguiram arrecadar milhares de dólares em receitas de publicidade. *Idem* para o portal Endingthefed.com, a certa altura responsável por quatro em dez das *fake news* mais populares nas redes sociais, e gerido por um jovem romeno de 24 anos<sup>135</sup>. Finalmente, as motivações sociais ou psicológicas não devem, também, ser ignoradas, havendo agentes empenhados em, independentemente de uma base ideológica, gerar confusão *online* ou fazer parte da indústria do entretenimento, com isso querendo ganhar alguma notoriedade ou apenas por motivos fúteis ou diversão.

Olhando, agora, para as mensagens objeto da desinformação, WARDLE et. al. aponta quatro características principais desses conteúdos, a saber: [i.] as mensagens provocam uma resposta emocional, geralmente destacando e inflamando diferenças e divisões entre ideologias, partidos políticos, nacionalidades, raças, etnias, grupos religiosos, castas, classes sociais, etc., [ii.] têm associado uma forte componente visual<sup>136</sup>, [iii.] descrevem uma narrativa forte ou poderosa, [iv.] e são repetidas até à exaustão<sup>137</sup>. De notar que a desinformação tem assumido cada vez mais a forma de imagens e vídeos em lugar do texto, o que torna o combate ao fenómeno mais difícil, quer do ponto de vista tecnológico (visto que as ferramentas automáticas não funcionam de forma tão eficaz em conteúdos visuais), quer do ponto de vista psicológico do intérprete<sup>138</sup>.

A análise dos processos de desinformação não ficaria completa se não se olhasse para as técnicas digitais empregues na distribuição e amplificação dos conteúdos falsos ou

---

<sup>134</sup> O processo tendente a gerar receita através da publicidade na *internet* é relativamente simples e explora as principais características da “economia da atenção” (cfr. *infra*), baseando-se no número de cliques que uma determinada página onde se encontram os anúncios é capaz de gerar. Assim, o objetivo dos anunciantes, dos intermediários e das plataformas é maximizar o número visualizações dos conteúdos, sendo que a receita obtida é proporcional ao número de visualizações ou cliques que se alcança. Vide TAMBINI, Damian - *How advertising fuels fake news*. Media@LSE blog. [Em linha] (2017).

<sup>135</sup> Ambos são retirados de ALLCOTT, Hunt; GENTZKOW, Matthew - *Social Media and Fake News in the 2016 Election*. Journal of Economic Perspectives. Vol. 31. n.º 2 (2017). p. 217.

<sup>136</sup> Muitas vezes sob a forma de um *meme*, i.e., um conteúdo viral sob a forma de imagem, texto ou vídeo (ou a combinação de alguns destes elementos) que é partilhado, muitas vezes sob as vestes humorísticas, para comentar, parodiar ou referenciar algum símbolo cultural, alguma ideia social ou política ou algum evento da atualidade.

<sup>137</sup> WARDLE et. al., *Information disorder...*, p. 38 e ss.

<sup>138</sup> A pesquisa tem revelado que o processamento de imagens pelo cérebro humano é mais rápido que o processamento de texto, o que parece diminuir as nossas capacidades de raciocínio crítico. Vide WARDLE, et. al., *Information Disorder...*, p. 40.

manipulados. De facto, e como refere BAYER et. al., estas campanhas «*baseiam-se numa série coordenada mas dispersa de atividades que criam a impressão de ação espontânea*»<sup>139</sup>, a qual recorre a diferentes meios de comunicação, *online* e *offline*, provocando quer interações naturais (*natural reach*), quer interações automatizadas, por forma a dificultar a deteção da origem dos conteúdos. Entre os mecanismos digitais mais utilizados para amplificar as mensagens falsas ou manipuladas estão os *bots* (diminutivo para *robot*) e os *trolls*, correspondendo os primeiros a contas e perfis falsos automatizados ou semi-automatizados que permitem a rápida difusão de conteúdos nas redes sociais, através da constante interação nas redes (publicando, partilhando, comentando, gostando, etc.). Os *bots* sociais são particularmente eficientes (até porque financeiramente acessíveis) para tornar determinados tópicos em tendências maioritárias *online* (por exemplo no Twitter, através da repetição exaustiva de determinado *hashtag*), podendo também ser usado para aumentar artificialmente o número de seguidores de uma determinada figura pública ou política (repercutindo-se esse número na atenção mediática que essa figura recebe), para gerar um consenso ou maioria inexistente, ou para “abafar” determinada história através de técnicas de *spam*. Neste contexto, «*o ruído, o spam e a manipulação inerente a várias técnicas que utilizam bots ameaçam perturbar o diálogo cívico em todo o mundo*»<sup>140</sup>. Por outro lado, os *trolls* (por vezes também referidos por *sock-puppets*) são pessoas reais que, por detrás do manto do anonimato, e recebendo contrapartidas financeiras ou não, espalham desinformação e semeiam a discórdia e a confusão, «*saturando determinados websites com comentários, importunando e assediando utilizadores*»<sup>141</sup>. Não obstante, existem diversos tipos de *trolls*, podendo a sua atuação limitar-se ao *endorsement* de determinados conteúdos (v.g. *hashtags*) ou perfis, de modo a dar a certo assunto a aparência de popularidade e apoio maioritário (uma técnica conhecida por “*astroturfing*”), ou assumir posições mais agressivas, intimidando e assediando opositores ou jornalistas. Em conjunto, agentes, *bots* e *trolls* constituem a designadas *cyber troops*, um exército ao serviço da desinformação.

Sem prejuízo da relevância do recurso às redes sociais e à automação, os *media* tradicionais são também parte do problema, principalmente aqueles que são detidos, financiados ou apoiados

<sup>139</sup> BAYER et. al., *Disinformation and propaganda...*, p. 30.

<sup>140</sup> HOWARD, Philip N.; WOOLLEY, Samuel; CALO, Ryan - *Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration*. Journal of Information Technology & Politics. Vol. 15. n.º 2 (2018). p. 86.

<sup>141</sup> VILMER et. al., *Information manipulation...*, p. 84. Segundo o Autor, o processo de *trolling* envolve, geralmente, três fases: numa primeira, o *troll* cria e publica uma mensagem controversa para criar uma reação; se ninguém contestar a mensagem, pode o próprio *troll*, usando um outro perfil, desafiar essa mensagem criando uma discussão artificial *online* que atrairá atenção de utilizadores naturais; assim que um utilizador “morde o isco” e interage na discussão o *troll* desafia sistematicamente os seus comentários, variando os perfis que usa e o tom dos comentários (da ironia ao insulto) para manter a discussão pelo maior tempo possível

pelo Estado. Na dependência do poder, os *media* são muitas vezes instrumentalizados para serem veículos das campanhas de desinformação e manipulação orquestradas por atores oficiais, o que atinge proporções particularmente preocupantes quando esses *media* têm ressonância junto de minorias noutros países (como é o caso da Rússia e das minorias que falam a língua no leste europeu). Por outro lado, há também investigação que sugere que meios de comunicação social excessivamente alinhados politicamente tendem a promover ideias nem sempre exatas, mas alinhadas com a sua ideologia. Finalmente, os próprios *media mainstream* contribuem para a amplificação dos conteúdos desinformativos, noticiando-os, assim expondo os seus espetadores à mensagem desinformativo ou manipulada.

Um estudo de 2018 que analisou cerca de cento e vinte e seis mil histórias publicadas no Twitter entre 2006 e 2017 e partilhadas por mais de três milhões de utilizadores concluiu que as histórias “falsas” se propagaram significativamente *«mais longe, mais rapidamente, mais profunda e amplamente do que a verdade em todas as categorias de informação, sendo os efeitos mais pronunciados em notícias falsas de teor político do que em notícias falsas relacionadas com terrorismo, ambiente, desastres naturais, ciência, lendas urbanas ou informações financeiras»*<sup>142</sup>. Apesar de se dever olhar para estes dados com cautela, uma vez que os mesmos dependem sempre da concreta amostra recolhida e dos métodos utilizados, esta investigação junta-se a outras que em contextos como as eleições presidenciais americanas, o referendo do Brexit, as eleições presidenciais francesas e as eleições alemãs, também sugerem que os conteúdos desinformativos têm um maior alcance do que os conteúdos dos *media* tradicionais. Mas que causas levam a que desinformação chegue mais longe e rapidamente que os factos objetivos? Um fenómeno desta complexidade decorre de vários fatores, alguns conhecidos e outros ainda por desvendar. No entanto, vários autores apontam para uma série de tendências, algumas já abordadas neste trabalho, que contribuem para a “raiz” do enorme alcance da desinformação. Por exemplo, VILMER et. al. aponta dois tipos de causas para a manipulação informativa: causas internas e causas coletivas<sup>143</sup>. A nível interno, perscrutando a psicologia dos indivíduos atuando em comunidade e rede, parecem ter relevância as teorias da preguiça intelectual do cérebro humano, pouco disposto a um raciocínio crítico permanente, preferindo aceitar como válida informação que confirme os nossos pré-juízos e conceitos ou que tenha origem na nossa rede de contactos (“*confirmation bias*”). Por outro lado, como a desinformação é produzida com o propósito da viralidade, ela geralmente explora as fraquezas cognitivas,

<sup>142</sup> VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan - *The spread of true and false news online*. Science. Vol. 359. n.º 6380 (2018).

<sup>143</sup> VILMER et. al., *Information Manipulation*, p. 29.

através do sensacionalismo, da emoção exacerbada, do alarmismo, do medo e da ansiedade. Já a nível coletivo, parece oferecer contributo decisivo, simultaneamente como causa e consequência, num ciclo vicioso, a crise de confiança nas instituições, de que a própria desinformação é também sintoma, a somar a outros como as taxas de abstenção eleitoral, a desconfiança face aos titulares de cargos públicos e as reticências cada vez mais vocais relativas ao próprio modelo democrático e liberal. Assim, a desinformação parece seguir outras tendências, como a rejeição das elites e do *establishment*, a polarização radical das sociedades, a crise do Estado de Direito em muitos países, entre outras. Finalmente, tem também papel relevante a designada “*crise da imprensa tradicional*”, que, não sendo nova, uma vez que a imprensa teve já de se adaptar ao surgimento da rádio e da televisão<sup>144</sup>. A somar a este caldo, e tendo em conta os dados que demonstram que cada vez mais pessoas consomem informação nas e através das redes sociais<sup>145</sup>, é preciso considerar os impactos dos algoritmos (quer das redes sociais, quer dos motores de busca) que, sob o manto da personalização de conteúdos, determinam quais e a ordem das notícias que são apresentados aos utilizadores, funcionando como os novos *gatekeepers*, havendo sérios riscos de enviesamento e manipulação (ou, eufemisticamente, *otimização*)<sup>146</sup>. A CE também destaca que a «*desinformação tem causas económicas, tecnológicas, políticas e ideológicas interligadas*»<sup>147</sup>, associando-a à insegurança económica, ao aumento do extremismo, às mudanças culturais e às transformações no setor dos *media*, e chamando atenção para o facto de algumas plataformas digitais terem vindo a assumir «*funções tradicionalmente associadas aos meios de comunicação social, entrando no negócio das notícias como agregadores e distribuidores de conteúdos, sem terem necessariamente os enquadramentos e capacidades editoriais desses meios tradicionais*». Realmente, uma das mudanças estruturais que ocorreu com a era da informação foi a passagem de uma situação de falta de informação para uma situação de hiper-abundância informativa, o que fez com que a

<sup>144</sup> Como destaca VILMER et. al., *Information Manipulation*, p. 29, a crise dos *media* manifesta-se quer ao nível do modelo de negócio, quer ao nível das normas que orientam o jornalismo. Quanto ao modelo de negócio, «*uma característica central da transformação digital é a substituição de um modelo de negócio linear no offline para um modelo de publicação de notícias multi-canal ou em plataforma*» (MARTENS et. al., *The digital transformation of...*, p. 15. ), o que implica uma dependência ainda maior das receitas provenientes da publicidade cuja rentabilidade *online* é menor, o que obriga ao aumento do número de conteúdos e o recurso a técnicas como o “*clickbait*” (definido como a mensagem curta e forte, nem sempre correspondente com o conteúdo, que tem por objetivo atrair os utilizadores a clicar num *weblink*), e uma tendência para o imediatismo na produção de notícias, muitas vezes em atropelo da qualidade e da verificação de factos.

<sup>145</sup> Em 2020, a maioria das pessoas acedem às notícias *online*, sendo que as redes sociais assumem crescente importância (v.g.: nos EUA 47% acede à informação nas redes sociais, contra 16% na imprensa; na Alemanha a diferença é 39% para 26%; em Espanha de 63% para 28% em Portugal é de 58% para 33%). Vide Newman, Nic; Fletcher, Richard; Schulz, Anne; Andi, Simge; NIELSEN, Rasmus Kleis - *Reuters Institute Digital News Report 2020*. [s.l.]: Reuters Institute for the Study of Journalism, 2020.

<sup>146</sup> MARTENS et. al., *The digital transformation of...*, p. 19

<sup>147</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão... Combater a desinformação em linha...* p. 4.

informação enquanto bem perdesse valor económico. Todavia, como explica HENDRICKS et. al., «o acesso fácil a quantidades imensas de informação, e o facto de frequentemente não ser necessário pagar nada por ela, não significa que a informação seja gratuita; para recebermos informação, nós pagamos com atenção»<sup>148</sup>. Nasce a economia e o mercado da atenção, cujo máxima pode ser assim traduzida: «se não pagamos pelo produto, então é porque nós somos o produto»<sup>149</sup>. Ora, o objetivo na economia da atenção é captar e prender pelo maior tempo possível os consumidores quer seja à televisão, ao Facebook, ao Twitter ou ao Instagram. Quanto mais tempo um consumidor está concentrado numa plataforma maior é a probabilidade de ser persuadido (ou manipulado) pela publicidade (sob a forma de anúncios), que é a base das receitas da televisão, dos motores de busca, dos *websites* e das próprias redes sociais.

## Secção II – Algoritmos, automação, personalização e datificação.

A desinformação ou o recurso a táticas agressivas de manipulação noticiosa não são o único problema que a Era Digital veio colocar aos sistemas democráticos. Na verdade, tem sido cada vez mais estudado os efeitos dos algoritmos e da automação, da personalização e da datificação associada às novas tecnologias, quer numa perspetiva individualista, que atenta sobretudo aos efeitos destes mecanismos na privacidade e autonomia dos indivíduos<sup>150</sup>, quer numa perspetiva comunitarista, que pretende refletir sobre os efeitos dessas novas capacidades técnicas na esfera pública e os impactos que daí resultam para o ideal democrático. Os algoritmos (definidos como «o conjunto de regras que um computador segue para resolver um dado problema ou executar uma tarefa»<sup>151</sup>), visíveis ou invisíveis, são onnipresentes, deles dependendo o pleno funcionamento da Era Digital<sup>152</sup>. Enfim, tarefas como a indexação e organização de informação nos motores de busca ou a organização e apresentação de informação no *feed* de uma rede social dependem de algoritmos, os quais selecionam, de forma automática, mas segundo critérios pré-estabelecidos, de um imenso oceano de dados quais os concretos conteúdos que serão exibidos aos utilizadores da *internet*. Assim, os algoritmos executam tarefas críticas, tomando verdadeiras «decisões», tais como «classificar, priorizar, associar e filtrar. Estas decisões

<sup>148</sup> HENDRICKS, Vincent F.; VESTARGAARD, Mads - *Reality Lost: Markets of Attention, Misinformation and Manipulation*. [s.l.]: Springer, 2019. p. 2.

<sup>149</sup> *Ibid*, p. 11.

<sup>150</sup> Cfr. *inter alia*, Ac. TJUE de 13.05.2014, C-131/12 (“Google Spain”), n.º 99., Ac. TJUE de 09.03.2010, C-518/07 (“Comissão c. Alemanha”), n.º 56. Cfr., *inter alia*,

<sup>151</sup> NEUDERT et. al., *Polarisation and the use of...*, p. 11.

<sup>152</sup> MURTHY, Dhiraj; POWELL, Alison B.; TINATI, Ramine; ANSTEAD, Nick; CARR, Leslie; HALFORD, Susan J.; WAL, Mark - *Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital*. International Journal of Communication. Vol. 10. (2016). p. 4955.

*correspondem a métodos de analisar big data, tornando-a significativa e útil.»*<sup>153</sup>. É preciso notar, no entanto, que um algoritmo, enquanto «objeto político», não é uma «idealização, uma ferramenta linguística ou dispositivo emergente», antes, ele «anima materialidades concretas» e interfere com os «processos sociais [...], mobilizando concretas relações sociais [...], reduzindo a complexidade do mundo social em termos de cálculos [...] que só podem ser entendidos por máquinas»<sup>154</sup>. Ora, é precisamente as consequências sociais e políticas dos algoritmos de que nos ocuparemos, desde já esclarecendo que há uma evidente ligação entre os algoritmos e aquilo que vem sendo designado por *big data* e que pode ser entendida como a «extraordinária quantidade de informação recolhida sobre «muitas pessoas usando muitos dispositivos»<sup>155</sup>, informação essa que – e esse é o cerne do conceito – pode depois ser pesquisada, agregada e triangulada com outros conjuntos de dados. Durante muito tempo, e tendo em conta que os algoritmos são desenhados para executar um conjunto pré-definido de regras, foi dominante a ideia da sua “neutralidade”, pelo que eles não padeceriam dos mesmos vieses da decisão humana. No entanto, as investigações mais recentes têm revelado que os algoritmos não são neutros, verificando-se no seu processo de tomada de decisões preconceitos semelhantes aos dos seus criadores, além de reforçarem os vieses existentes nos conjuntos de dados que depois transformam<sup>156</sup>. Por outro lado, tendo em conta que as regras e os *inputs* de dados que alimentam os algoritmos não são públicas, há, ainda, o risco de manipulação desses sistemas para a prossecução de objetivos particulares. Nestes termos, têm sido expressas preocupações no sentido de os *media* digitais e as redes de dispositivos (principalmente no contexto da IoT, em que os dispositivos se encontram conectados «em espaços tradicionalmente protegidos e íntimos, com capacidade de extrair informações relativas a dados pessoais sensíveis e de os transmitir»<sup>157</sup>) poderem ser utilizadas como ferramentas de controlo social.

A problemática dos *bots* já acima abordado entronca na questão maior dos algoritmos, na medida em que um *bot* é também um algoritmo ou, mais propriamente, um *script* ou programa

<sup>153</sup> SHOREY, Samantha; HOWARD, Philip N. - *Automation, Big Data, and Politics: A Research Review*. International Journal of Communication. Vol. 10. (2016). p. 5033.

<sup>154</sup> SCANNELL, Josh - *What Can an Algorithm Do?* DISMAGAZINE. (2015).

<sup>155</sup> SHOREY et. al. – *Automation, Big Data, ...*, p. 5033.

<sup>156</sup> Assim, há estudos que evidenciam que as decisões baseadas em algoritmos (que por exemplo selecionam candidatos para entrevistas de emprego ou para a atribuição de créditos bancários) reforçam discriminações institucionalizadas contra determinadas minorias (segundo as investigações, até uma pequena distorção pode resultar na segregação de todo um grupo populacional). *Ibid.* pp. 5034 e ss. e MURTHY et. al., *Bots and Political Influence...*, p. 4953.

<sup>157</sup> SILVEIRA, Alexandra; FROUFE, Pedro - *Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos*. UNIO - EU Law Journal. Vol. 4. n.º 2 (2018). p. 6.

que «corre continuamente, formula decisões, atua com base nessas decisões sem qualquer intervenção humana, sendo capaz de se adaptar ao contexto em que opera»<sup>158</sup>. A presença de *bots online* é ubíqua, havendo dados que afirmam que estes programas correspondem a mais de metade do tráfego na *internet*, sendo certo que eles tanto podem desempenhar funções inócuas ou úteis, como podem ser usados «positivamente para ajudar à mobilização de redes de apoio a uma causa»<sup>159</sup>. Porém, os exemplos cada vez mais comuns dos *spambots* e dos *bots* sociais usados no contexto de campanhas de manipulação política, têm feito soar alarmes junto da comunidade científica, sobretudo pela facilidade, baixo custo e eficácia com que estes instrumentos podem ser empregues<sup>160</sup>.

Mas talvez o aspeto mais perverso da utilização de algoritmos, associada ao *big data*, sejam as questões em torno da designada “personalização de conteúdos”. Na verdade, a tentativa de personalizar a experiência de cada utilizador *online*, ajustando os conteúdos que são apresentados, as sugestões de pesquisa e de contactos, é uma tendência que se vem desenvolvendo desde a Web 2.0 e que se relaciona largamente com a economia da atenção e com a transformação da *internet* num espaço publicitário. Assim, se a prioridade é manter o utilizador em linha, é necessário apresentar-lhe exatamente o que ele quer ver, ou, melhor dizendo, aquilo que o algoritmo computa que o utilizador quer ver, com base em preferências percebidas ou comportamentos passados, num esforço de o manter continuamente preso ao dispositivo. A personalização só é possível através da permanente recolha de dados, resultando essa recolha ou de *inputs* voluntários do utilizador (que fornece ao sistema certos elementos, como a sua idade, género, etc.), ou de recolhas abstrusas, como o histórico de pesquisa ou a partilha de localização que o utilizador faz quando acede a uma aplicação. Nestes termos, quando falamos em sistemas de personalização, referimo-nos a algoritmos capazes de prever

---

<sup>158</sup> GORWA, Robert; GUILBEAULT, Douglas - *Understanding Bots for Policy and Research: Challenges, Methods, and Solutions*. [s.l.]: [s.n], 2018. Referem os Autores a existência de vários tipos de *bots*, desde os *webcralers* ou *scrapers* (utilizados pelos motores de busca para “rastejar” a *web* e devolver resultados para uma pesquisa), os *chatbots* (usados muitas vezes pelas redes sociais, empresas e serviços públicos por exemplo para responder a FAQs), os *spambots* (usados para inundar as plataformas de publicidade ou conteúdos maliciosos, e, no contexto político, também para promover e amplificar um conteúdo (de modo a gerar um consenso ou uma maioria artificial em torno de um tópico) ou para suprimir e “enterrar” uma narrativa ou oponente), os *bots sociais* (correspondem a vários tipos de automação que assume a forma de uma identidade fabricada que interage automaticamente nas redes sociais) e os *cyborgs* (que combinam a automação e a intervenção humana).

<sup>159</sup> MURTHY et. al., *Bots and Political Influence...*, p. 4956.

<sup>160</sup> Como refere NEUDERT et. al., *Polarisation and the use...*, p. 28, «a investigação em torno do impacto dos *bots* é controversa, postulando alguns académicos o seu mínimo efeito para a difusão de propaganda, ao passo que outros concluem que os *bots* distorceram estrategicamente o discurso cívico em momentos como o referendo do Brexit». Segundo HOWARD et. al., *Algorithms, bots, and political...*, p. 84 «um número crescente de estudos demonstrou que os *bots* podem ter um impacto político, não tanto por mudarem a opinião do votante, mas ao atacarem jornalistas e desacreditarem líderes políticos – especialmente se essas figuras forem mulheres. Ademais, as campanhas políticas conduzidas através de *bots* tendem a vir dos partidos políticos mais radicais e tendem a amplificar mensagens negativas».

«o que é relevante para o utilizador, filtrando e removendo a informação irrelevante e aumentando aquela considerada importante e pertinente para aquele utilizador individual»<sup>161</sup>.

Se as capacidades técnicas permitem aproveitar a imensidão de dados recolhidos a cada segundo sobre todos os utilizadores em linha para, através de sistemas especializados, prever com bastante rigor comportamentos e preferências, é evidente que essas potencialidades não deixariam de ser aproveitadas, principalmente no domínio dos anúncios *online*. Chegamos, assim, a uma das grandes tendências da Era Digital: o *microtargeting* ou micro-direcionamento, que permite usar a vantagem fornecida pelos algoritmos de perfilagem para expor utilizadores que preencham um perfil específico<sup>162</sup> a determinadas mensagens, alcançando uma segmentação de mercado impossível nos meios tradicionais. Do mesmo modo, possibilita que a mesma mensagem seja trabalhada de forma diferente para melhor se ajustar ao perfil de cada subgrupo de destinatários, o que é frequente no caso da desinformação e das táticas de manipulação agressiva, produzindo-se centenas de conteúdos com a mesma mensagem fundamental, mas pequenas variações de linguagem ou imagem de modo a obter a melhor correspondência possível às preferências percebidas dos vários segmentos. Esta “triagem fina” é cada vez mais utilizada pelos anunciantes nas plataformas digitais para aumentar a eficácia dos conteúdos partilhados, enquanto funcionam como uma relevante fonte de receita para as próprias plataformas ou para terceiros, que fornecem e/ou trabalham os dados dos utilizadores, segmentando-os. Tanto a personalização de conteúdos como o *microtargeting* têm consequências no ambiente digital: é hoje possível – e até comum – que dois utilizadores, usando exatamente a mesma plataforma digital, sejam expostos a conteúdos e mensagens substancialmente diferentes, a que o outro não consegue ter acesso. Desta feita, as plataformas digitais ao apresentarem conteúdos que muito provavelmente nos agradarão, «*reforçam a nossa mundivisão e permitem que continuemos, confortáveis e seguros, encerrados nas nossas câmaras de ressonância*»<sup>163</sup> ou *echo chambers*. Com este efeito, a promessa de que a *internet* transformaria o mundo numa “aldeia global digital” dilui-se, substituída por um conjunto vasto

<sup>161</sup> MITTELSTADT, Brent - *Auditing for Transparency in Content Personalization Systems*. International Journal of Communication. Vol. 10. (2016). p. 4991-5002.

A personalização é possível graças à interação entre [i.] algoritmos de priorização que decidem quais os tópicos *trending*, [ii.] algoritmos de perfilagem (*profiling algorithms*) responsáveis por inferir preferências e atributos dos utilizadores a partir de pequenos padrões ou correlações para depois agruparem os indivíduos de acordo com o seu comportamento, preferências ou outras características e [iii.] *bots* automáticos. De notar que a personalização pode também advir de escolhas do próprio utilizador, uma vez que as plataformas disponibilizam com frequência definições de conteúdo que o utilizador pode alterar, ora descrevendo as suas preferências, ora bloqueando perfis de outros utilizadores.

<sup>162</sup> A perfil pode ser ajustado em função de variadas características, tais como género, idade, orientação sexual ou política, situação laboral, localização geográfica... as possibilidades são virtualmente infinitas.

<sup>163</sup> WARDLE et. al., *Information Disorder...*, p. 49.

de ilhas isoladas e sem contactos, visto que cada utilizador vive numa “bolha” de “conteúdos filtrados” por algoritmos (as “*filter bubbles*”) que apenas apresentam informações que se ajustam às preferências, crenças e ideologias dos indivíduos, nunca desafiando esses pré-conceitos ou apresentando visões, narrativas ou ideologias alternativas. É, todavia, preciso notar que a tendência homofílica, i.e., de associação a grupos que refletem as nossas preferências, é natural no ser humano. O que há de novo, na nossa ótica, é que o meio digital, da mesma forma que pode expandir as possibilidades de contacto com realidades distantes, pode também servir para erigir um muro inultrapassável à volta da nossa cosmovisão, sendo muito difícil encontrar outros pontos de vista. Não obstante, e apesar de existirem “*echo chambers*”, a investigação tem revelado que esse não é, por regra, o ambiente em que se encontra o utilizador médio, sendo antes típico de utilizadores já com convicções ideológicas extremadas<sup>164</sup>.

Quando usados no contexto político, o *big data*, a personalização de conteúdos, o *microtargeting* e a automação através de *bots* podem ter impactos reais. Como já referido, «a personalização algorítmica de conteúdos envolve inevitavelmente escolhas normativas [...]». *O design de um algoritmo reflete os valores do designer e dos usos para que tende*»<sup>165</sup>. Um bom exemplo do uso nefasto associado a estas tecnologias foi conhecido e investigado após o referendo no Reino Unido sobre a permanência na UE. Acompanhando aqui as conclusões do inquérito realizado pela Câmara dos Comuns do Parlamento do Reino Unido<sup>166</sup>, mais do que *fake news*, o que sucedeu no período de campanha anterior à realização do referendo foi o micro-direcionamento contínuo e incessante de mensagens hiper-partidárias explorando os medos e pré-conceitos dos cidadãos, de modo a influenciar o seu comportamento nas urnas<sup>167</sup>. Parte deste esforço foi possível graças à capacidade de perfilagem e análise de dados de empresas como a *Cambridge Analytica* e a *Aggregate IQ*<sup>168</sup>. Um dos debates mais prementes

<sup>164</sup> NEUDERT, *Polarisation and the use...*, p. 17.

<sup>165</sup> MITTELSTADT, *Auditing for Transparency...*, p. 4993.

<sup>166</sup> Cfr. HOUSE OF COMMONS. Digital, Culture, Media and Sport Committee. *Disinformation and 'fake news': Interim Report*. London: [s.n.], 2018. e, ainda, HOUSE OF COMMONS. Digital, Culture, Media and Sport Committee. *Disinformation and 'fake news': Final Report*. London: [s.n.], 2019.

<sup>167</sup> HOUSE OF COMMONS, *Disinformation...: Interim Report*, p. 26.

<sup>168</sup> Estas empresas anunciam os seus serviços como sendo o tratamento de dados e segmentação das audiências, oferecendo uma análise psicográfica e *microtargeting* comportamental que pode ser usado para publicidade “à medida” e mobilização granular de potenciais votantes. Para procederem a esta perfilagem psicográfica, as empresas necessitavam de dados sobre as suas audiências, de modo a determinar o seu perfil psicológico. A *Cambridge Analytica* ficou conhecida por utilizar a análise psicológica OCEAN. Esta análise foi testada junto do público através de uma aplicação que funcionava interligada ao Facebook (e designada GSR App) e na qual eram pagas pequenas quantias para que os utilizadores fizessem o *download* da App e completassem um inquérito *online*. Além das questões a que os utilizadores respondiam, a aplicação acedia também ao uma série de informação do perfil do Facebook do utilizador para conduzir a análise, tal como demografia, comentários, páginas gostadas, listas de amigos, etc. Ao mesmo tempo, e num *data breach* mais tarde reconhecido pelo Facebook, era também possível aceder a várias informações de todos os “amigos” do utilizador, tudo isto sem o seu conhecimento ou

sobre esta matéria gira em torno dos designados “*dark ads*” que apenas são exibidos e micro-direcionados para determinados grupos de utilizadores, quedando-se inacessíveis para os outros, sendo que apenas os anunciantes (políticos ou não) e as plataformas digitais conhecem quer os destinatários quer os critérios utilizados na distribuição da publicidade.

O que está em causa com estes sistemas da Era Digital é um novo paradigma de curadoria, de moderação e de *gatekeeping* digital, paradigma esse que parece comprometer a igualdade de oportunidades e a qualidade do discurso público e político online. «No mínimo, os sistemas personalizados podem enfraquecer o discurso político ao reduzirem a diversidade de ideias que os participantes encontram e ao obscurecerem os mecanismos externos que influenciam as suas crenças. Como gatekeepers informativos, estes sistemas ameaçam o equilíbrio e a abertura do discurso político com uma constante, mas muitas vezes subtil ou secreta, moderação das opiniões dos participantes. As comunidades podem ser segmentadas de tal modo que apenas alguns grupos sejam considerados merecedores de receber certas oportunidades informativas»<sup>169</sup>. Com a transformação dos media e a assunção por parte das plataformas digitais de tarefas antes reservadas a outros atores tradicionais, a “dieta” informativa e propagandística dos cidadãos alterou-se, deixando de ser baseada, por exemplo, em critérios sociodemográficos, para passar a corresponder a critérios comportamentais<sup>170</sup>. Se, até aqui, o *gatekeeping* era visto como o «processo através do qual se determina que conteúdos podem chegar ao público enquanto informação válida e fidedigna», através de um «processo de seleção e filtragem num domínio profissional com regras definidas e, subsequentemente,

---

consentimento. Este método permitiu à empresa recolher perfis de até 87 milhões de utilizadores, mais de 1 milhão dos quais no Reino Unido. Mais do que as respostas aos questionários, relevante foi o acesso aos “gostos” dos utilizadores no Facebook, uma vez que estas interações «são altamente preditivas da personalidade e de um conjunto de outros traços psicodemográficos, tais como idade, género, inteligência e visão política e religiosa» (LAMBIOTTE, Renaud; KOSINSKI, Michal – *Tracking the Digital Footprints of Personality*. Proceedings of the IEEE. Vol. 102, n.º 12 (2014) Com os dados em mão, a Cambridge Analytica colaborou, pelo menos desde 2014, numa série de campanhas eleitorais em vários países, micro-direcionando mensagens políticas para utilizadores de acordo com o seu perfil psicológico. Segundo o relatório interino da Casa dos Comuns, nas eleições intercalares de 2014 dos EUA, o grupo SCL «afirmou que 1,5 milhões de anúncios gerados pelas suas campanhas originaram uma subida de 30% na participação eleitoral dos grupos-alvo em comparação com a participação projetada para esses grupos» (HOUSE OF COMMONS, *Disinformation...: Interim Report*, p. 31). Já a empresa Aggregate IQ, foi, durante o referendo sobre a permanência do Reino Unido na UE, responsável por micro-direcionar mais de 3,6 milhões de libras em anúncios nas redes sociais a favor do *Brexit*. Um dos truques usados pela campanha a favor da saída para recolher dados dos potenciais votantes foi a criação, no Facebook, de um “quiz” prometendo um prémio de 50 milhões de libras para quem previsse com maior exatidão os resultados do campeonato europeu de futebol. Por fim, a AIQ e outras empresas também usaram – e usam – uma ferramenta designada *Facebook Pixels* que funciona como um rastreador online, permitindo, quando incluída num website, registar se um utilizador do Facebook por ali passou, devolvendo essa informação ao Facebook que a pode partilhar com anunciantes de modo a que estes coloquem anúncios nesse website. Assim, as campanhas políticas podiam facilmente controlar qual a publicidade disponível nos websites a que utilizadores com dado perfil acediam.

<sup>169</sup> MITTELSTADT, *Auditing for Transparency...*, p. 4992.

<sup>170</sup> MOLLEN, A.; DHAENENS, F. - *The Co-option of Audience Data and User-Generated Content: Empowerment and Exploitation Amidst Algorithms, Producers and Crowdsourcing*. In DAS, R. & YTRE-ARNE, B. *The Future of Audiences: A Foresight Analysis of Interfaces and...* [s.l.]: Palgrave Macmillan, 2018. p. 45.

*mecanismos de accountability*»<sup>171</sup>, atualmente o processo mercantilizou-se pelo fim essencialmente comercial das plataformas digitais que exercem esse papel ao, através dos algoritmos que criam e exploram, decidirem quais as notícias, informação e demais conteúdos a que os cidadãos têm acesso e ao permitirem que terceiros (bem ou mal intencionais) recolham e utilizem, muitas vezes sem o seu conhecimento ou o consentimento informado, dados dos cidadãos para depois os bombardearem com conteúdos feitos à medida e destinados a explorar a suas fragilidades, medos e preconceitos, o que levanta a questão da responsabilidade das plataformas digitais, que *infra* abordaremos. Por outro lado, o alargamento do número de atores que atuam como *gatekeepers* do discurso público não funcionou, como se pretendia, como um comprimido democratizador e de “empoderamento”, que faria com que todos tivessem a sua voz que podia alcançar o mundo inteiro, com o consequente acesso ilimitado a uma variedade infinita de informação e de ideias, antes tendo redundado no afunilamento e na emocionalização (senão radicalização) do discurso. De facto, a voz de cada utilizador não chega além daquilo que é decidido subjetivamente por uma rede de algoritmos cujas regras se desconhece, mas que depende, pelo menos, do “capital social” nas redes, exceto se, claro está, que se recorrer às ferramentas pagas de *micro-targeting*. A este propósito, MOLLEN et. al. refere que o poder que as tecnologias digitais exercem sobre as audiências obedece, entre outras, às seguintes características: *exploração*, referindo-se ao interesse económico prevalente das companhias digitais quando tornam conteúdos acessíveis às suas audiências, *formação*, que se refere à forma como os produtores e provedores de conteúdos *online* inserem determinadas conceções e funções intrusivas específicas sem transparência, e *exclusão*, significando o cada vez maior desequilíbrio existente entre os cidadãos e os *media* digitais, designadamente a falta de participação das audiências no processo de conceção ou oposição a certas características do *software*, como, por exemplo, os direitos sobre os seus dados<sup>172</sup>.

Nada disto seria possível sem a crescente datificação das sociedades. Segundo ALEXANDRA SILVEIRA et. al., «os dados (inclusivamente os de carácter pessoal) estão na base da revolução algorítmica que está a mudar o mundo», sendo a proteção de dados a «questão jusfundamental identitária dos nossos tempos», «para que o projeto do humanismo não se torne irrelevante»<sup>173</sup>. De acordo com SHOSHANA ZUBOFF viveremos em breve na “Era do Capitalismo de Vigilância”, na qual os cidadãos serão apenas «material gratuito em bruto para práticas comerciais ocultas

<sup>171</sup> AMARAL et. al., *Algoritmos e redes sociais...*, p. 64.

<sup>172</sup> MOLLEN et. al., *Audiences' Coping Practices...*, p. 48 e ss.

<sup>173</sup> SILVEIRA, et. al., *Do mercado interno à cidadania de direitos...*p. 4 e 6.

de extração, predição e vendas»<sup>174</sup>, extirpados da sua soberania graças à acumulação de liberdade e conhecimento desta nova forma de capitalismo, que o torna estruturalmente independente das pessoas (*maxime*, dos consumidores). A preocupação da Autora em torno do “poder invisível” dirige-se essencialmente aos gigantes digitais da atualidade como a Google, o Facebook, o Twitter, a Apple, a Amazon ou a Microsoft, também conhecidas por *big tech*. De facto, e com o desenvolvimento da IoT, em que os objetos que nos rodeiam, todos ligados em rede, permitirão uma ainda mais exata pegada digital e uma vigilância constante dos nossos comportamentos, crescem as preocupações em torno do poder concentrado numa pequeno grupo de empresas capaz de prever, influenciar e moldar os comportamentos, as preferências e o discurso a nível mundial, sem que ainda existam mecanismos eficazes de responsabilização e limitação. Como explica VESNIC-ALUJEVIC et. al., «num mundo hiperconectado, um dos bens mais valiosos é a propriedade dos dados dos indivíduos, visto como uma determinante de poder. A governança dos dados é um desafio importante para qualquer governo. O novo modelo de negócios das companhias digitais e os novos modos de obtenção de receitas, permitem que os dados dos utilizadores sejam recolhidos como um bem gratuito. A partilha de dados entre as diferentes plataformas levanta importantes debates em torno da privacidade, segurança e confiança»<sup>175</sup>. Estas preocupações assumem uma premência maior quando a pegada digital tanto pode resultar de comportamentos voluntários, como de comportamentos involuntários, em que os indivíduos, «confrontados com termos de uso de serviços e políticas de privacidade, incompreensíveis e extensas, necessários à utilização de interfaces digitais e objetos inteligentes, precisam de se submeter a essas políticas para poderem utilizar os serviços»<sup>176</sup>. Ora, do nosso ponto de vista, o processo de datificação é inevitável, na medida em que, presentemente, a única alternativa que se lhe coloca é a exclusão completa da Era Digital e de partes substanciais da vida em comunidade<sup>177</sup>. Realmente, basta pensar na digitalização dos procedimentos nos serviços públicos, no comércio exclusivamente eletrónico de certos bens ou até nas formas de pagamento totalmente digitais para compreendermos que a ubiquidade da

<sup>174</sup> ZUBOFF, Shoshana - *The Age of Surveillance Capitalism: The Fight for Humana Future and The New Frontier of Power*. London: Profile Books, 2019. p. 8.

<sup>175</sup> VESNIC-ALUJEVIC et. al., *The Future of Government 2030+ ...*, p. 16.

<sup>176</sup> STEHLING, Miriam; VESNIC-ALUJEVIC, Lucia; JORGE, Ana; MARÔPO, Lidia - *The Co-option of Audience Data and User-Generated Content: Empowerment and Exploitation Amidst Algorithms, Produsage and Crowdsourcing*. In DAS, R. & YTRE-ARNE, B. *The Future of Audiences: A Foresight Analysis of Interfaces and Engagement*. [s.l.]: Palgrave Macmillan, 2018. p. 80.

<sup>177</sup> Acompanhamos aqui CASTELLS – *A Galáxia da Internet...*, p. 8.: «A influência das redes baseadas na Internet vai além do número dos seus utilizadores: diz respeito também à qualidade do uso. Atividades económicas, sociais, políticas e culturais essenciais por todo o planeta estão a ser estruturadas pela Internet e em torno dela, como por outras redes de computadores. De facto, ser excluído dessas redes é sofrer uma das formas mais danosas de exclusão na nossa economia e na nossa cultura».

Era Digital tem como contrapartida a quase obrigatoriedade de pertença e acesso às redes e à posse de objetos “inteligentes”. Por seu turno, essa obrigatoriedade significa a alimentação ininterrupta de uma cadeia de recolha e processamento de dados e informações, muitas das quais sensíveis e dificilmente partilháveis noutros contextos. Hoje, estar no mundo significa estar também em e na rede. Essa certeza acarreta, diríamos, um efeito conformista, por via do qual os indivíduos aceitam as intrusões nas suas esferas enquanto um *trade-off* do conforto que a tecnologia lhes permite<sup>178</sup>. Mas não são apenas as questões relacionadas com a privacidade e a propriedade dos dados pessoais que aqui emergem. Como ensina CASTELLS, «*o poder é exercido antes de tudo em torno da produção e difusão de nós culturais e conteúdos de informação. O controlo sobre as redes de comunicação torna-se a alavanca através da qual interesses e valores são transformados em normas condutoras do comportamento humano*», para mais à frente acrescentar que «*a soberania do Estado sempre começou com o controlo da informação*»<sup>179</sup>. Parece, pois, ser admissível a conclusão de que quem controla a informação e os dados detém, também, uma parte substancial do *poder*, aqui entendido como compreendendo a capacidade de influência, moldagem e determinação das vontades, preferências, pensamentos e desejos de outrem<sup>180</sup>. Dificilmente se pode afirmar continuarem a ter os Estados democráticos *poder* para controlar a informação produzida na Era Digital, tendo-se esse poder deslocado para um grupo restrito de gigantes tecnológicas<sup>181</sup>, quase todas fora das fronteiras da UE (localizadas maioritariamente nos EUA), responsáveis pela recolha e tratamento dos dados de quem utiliza os serviços que oferecem. Mais do que isso, a análise dos dados recolhidos é feita em disciplinas híbridas que têm sempre por base a componente social e comportamental associada ao *big data*, sendo os serviços oferecidos pelas *big tech* desenhados de acordo com essa análise de dados, resultando desta interação um poder cada vez maior de «*influenciar, moldar e ajudar a determinar as vontades e os desejos dos indivíduos, uma vez estas organizações desempenham uma papel significativo na forma como os cidadãos adquirem informação, comunicam uns com*

<sup>178</sup> A ideia base é de STEHLING et. al., *The Co-Option of Audience Data...*, p. 81.

<sup>179</sup> CASTELLS, Manuel - *A Galáxia Internet - Reflexões sobre Internet, Negócios e Sociedade*. Lisboa: Fundação Calouste Gulbenkian, 2004. p. 135 e 146.

<sup>180</sup> Para uma conceptualização completa em torno das teorias do poder cfr. LUKES, Steven - *Power: A Radical View*. 2.<sup>a</sup> ed. London: Palgrave Macmillan, 2005.

<sup>181</sup> Sem que isso queira significar que os Estados não continuem a lutar por esse domínio, inclusive, com algum sucesso, os Estados democráticos, principalmente com a implementação de sistemas de vigilância em massa. Além da China, que tem provavelmente os sistemas mais acabados de vigilância e classificação dos seus cidadãos (ainda que permita um considerável grau de liberdade de expressão *online*, atuando sobretudo no momento da mobilização cidadã de modo a cercear a ação coletiva. Cfr. KING, Gary; PAN, Jennifer; ROBERTS, Margaret E. - *How Censorship in China Allows Government Criticism but Silences Collective Expression*. American Political Science Review. Vol. 107. (2013), é preciso também analisar o exemplo dos EUA por exemplo com o programa PRISM gerido pela Agência para a Segurança Nacional e exposto pelo denunciante Edward Snowden.

os outros, se relacionam com as autoridades, e se autorrepresentam»<sup>182</sup>. É importante notar que estas empresas prestadoras de serviços na *internet* detêm posições dominantes nos respetivos mercados, aproveitando quer o efeito de rede (quanto mais utilizadores estiverem em rede, mais valiosa ela se torna para todos), quer o efeito *lock-in* (quanto mais um utilizador integra um serviço digital no seu dia-a-dia, mais dependente dele se torna)<sup>183</sup>. Vários autores têm sugerido que mais do que o poder económico, estes intermediários da sociedade de informação detêm um enorme *poder cívico* que os distingue de outras multi ou transnacionais. Este poder cívico, já referido como o “quinto poder”<sup>184</sup>, traduz-se na capacidade de criação, disponibilização e modelação dos espaços digitais de que os cidadãos dependem. MARTIN MOORE reduz a seis os poderes que as gigantes tecnológicas exercem: «o poder de controlar a atenção, o poder de comunicar notícias, o poder de possibilitar a ação coletiva, o poder de dar a todos os indivíduos uma voz, o poder de influenciar eleições e o poder de responsabilizar os poderes públicos e privados»<sup>185</sup>. Estes poderes tanto podem servir para empoderar a participação cívica, como podem ser usados para influenciar e manipular os cidadãos<sup>186</sup>.

Por outro lado, as próprias administrações públicas dos Estados e grande parte do tecido económico dependem de um número reduzido de prestadores de serviços da *internet* para armazenar e processar toda a informação e dados que geram, o que implica uma certa sujeição relativamente a esses prestadores de serviços. Esta questão tem particular premência no caso da UE, onde grande parte do armazenamento e processamento de dados, quer em locais físicos, quer em nuvem (computação em nuvem<sup>187</sup>), é feita por empresas sediadas noutras jurisdições,

<sup>182</sup> MOORE, Martin - *Tech Giants and Civic Power*. London: Centre for the Study of Media, Communication and Power of The Policy Institute at King's College London, 2016. p. 23.

<sup>183</sup> Por exemplo, a «Google, na maioria dos países europeus, tem mais de 90% de quota de mercado dos motores de busca» (*Ibid*, p. 13). Saber se as *big tech* constituem monopólios (ainda que naturais) ou sequer se são monopólios especiais é assunto que não exploraremos, muito embora a questão surja amiúde na UE. As práticas concorrenciais das plataformas digitais são questionáveis, tendo a Comissão Europeia multado a Google em mais de 8 mil milhões de euros por 3 vezes no espaço de três anos por práticas anti-concorrenciais (Cfr. [https://ec.europa.eu/commission/presscorner/detail/pt/IP\\_19\\_1770](https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_1770). Consultado: 03/05/2020.) Já em junho de 2020, a Comissão anunciou ter lançado quatro investigações contra a Apple para avaliar se as regras que a empresa aplica à programação e distribuição de aplicações violam as regras de concorrência da UE (Vide [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1073](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073). Consultado em: 03/09/2020).

<sup>184</sup> DUTTON, W. - *The Fifth Estate Emerging through the Network of Networks*. Prometheus. Vol. 27. n.º 1 (2009).

<sup>185</sup> MOORE, *Tech Giants and Civic Power*, p. 24.

<sup>186</sup> Explica CASTELLS, A *Galáxia Internet*, p. 10, que a «a Internet foi deliberadamente projetada como uma tecnologia de comunicação livre. O que resultou desse projeto não é que sejamos finalmente livres graças à Internet [...]; tudo depende do contexto e do processo. Mas resultou disso que a Internet é uma tecnologia particularmente maleável, suscetível de ser profundamente alterada pela prática social e conducente a toda uma série de resultados sociais potenciais – a serem descobertos pela experiência, não proclamados de antemão».

<sup>187</sup> A computação em nuvem é um modelo que permite o acesso omnipresente, conveniente e *on-demand* a um agregado de recursos computacionais partilhados (v.g.: redes, servidores, armazenamento, aplicações, serviços) que podem ser disponibilizados rapidamente com um esforço mínimo por parte do prestador dos serviços.

sobretudo nos EUA<sup>188</sup>. De outro modo, uma parte significativa da infraestrutura digital de banda larga da UE, que permite o funcionamento das redes 3G e 4G, é fornecida por empresas chinesas, designadamente a *ZTE* e a *Huawei*, ambas estatalmente controladas. Perante este cenário, alguns autores referem a prevalência de um «*neocolonialismo digital (ou dependência tecno-oligopolística)*» da UE face às gigantes tecnológicas norte-americanas e às infraestruturas de origem chinesa<sup>189</sup>. Este contexto agrava-se pelos distintos modelos de *internet* defendidos pelas duas potências: os EUA procuram um modelo de «*Internet global gerida pelo setor privado*», sendo as próprias empresas tecnológicas responsáveis por definir as regras da *Internet*, ao passo que o modelo chinês dá prioridade ao controlo estatal através de uma série de ferramentas e tecnologias que bloqueiam, controlam, filtram ou manipulam o conteúdo que circula *online*<sup>190</sup>. A UE encontra-se no meio das duas potências, ora preocupada com a posição dominante dos EUA e a dependência que isso acarreta em termos de gestão de dados de origem europeia, ora receosa de um crescente domínio chinês nas infraestruturas digitais europeias e as consequências que daí derivam em termos de equilíbrio geopolítico. O caso do 5G é talvez o melhor exemplo desta tensão: elevado a prioridade política pela Comissão Europeia, que estabeleceu, em 2016, ambiciosas metas<sup>191</sup>, como parte de uma estratégia mais ampla no sentido da criação de um Mercado Único Digital na UE<sup>192</sup>, o 5G fará parte de uma «*sociedade europeia*

<sup>188</sup> Veja-se, a este propósito, a jurisprudência do TJUE relativa ao armazenamento e tratamento de dados de cidadãos europeus fora do território da UE, designadamente o Ac. TJUE de 08.04.2014, C-293/12 e C-594/12 (*Digital Rights Ireland Ltd*), n.º 68 («a diretiva não impõe que os dados em causa sejam conservados no território da União, pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.º, n.º 3, da Carta, do respeito das exigências de proteção e de segurança»), pelo qual a Diretiva 2006/24/CE foi declarada inválida, e, ainda, a jurisprudência “Schrems” que começou, em 2015, por declarar inválida a decisão da Comissão (Decisão 2000/520) da Comissão que criava um “porto seguro” para a transferência de dados da UE para os EUA precisamente por não estar garantido um nível adequado de proteção para os titulares desses dados (Ac. TJUE de 06.10.2015, C-362/14 (“*Schrems I*”), n.º 106). Mais recentemente, cfr. também o Ac. do TJUE de 25.01.2018, C-498/16 (“*Schrems II*”) e, ainda, a notícia de que M. Schrems processou, na Irlanda a Facebook Europa, querendo obriga-la a processar todos os dados aqui obtidos, o que já levou o Facebook a ameaçarem retirar os seus serviços do velho continente.

<sup>189</sup> KLEIN, Andrés Ortega - *The view from Spain: The EU's bid for digital sovereignty*. In HOBBS, C. *Europe's Digital Sovereignty: From Rulemaker To Superpower In The Age Of Us-China Rivalry*. [s.l.]: European Council on Foreign Relations, 2020. p. 35.

<sup>190</sup> PUDDEPHATT, Andrew - *Governing the internet: The makings of an EU model*. In HOBBS, C. *Europe's Digital Sovereignty: From Rulemaker To Superpower In The Age Of Us-China Rivalry*. [s.l.]: European Council on Foreign Relations, 2020. p. 17.

<sup>191</sup> Designadamente que, até 2025, todas as zonas urbanas e as principais vias de transporte terrestres tivessem cobertura ininterrupta de 5G. Cfr. COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. 5G para a Europa: um Plano de Ação*. COM (2016) 588 final. Bruxelas, 14.9.2016. p. 5.

<sup>192</sup> O MUD, cuja estratégia remonta a 2015, baseia-se em ações específicas em torno de três pilares: melhor acesso dos consumidores aos bens e serviços digitais em toda a Europa, criação de condições adequadas e de concorrência para o desenvolvimento de redes digitais e serviços inovadores e otimizar o potencial de crescimento da economia digital. De entre os atos adotados no âmbito do MUD está o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679 de 27.04.2016), o Regulamento que visa prevenir o bloqueio geográfico injustificado (Regulamento (UE) 2018/302 de 28.02.2018), o Programa “WiFi4EU”, o Regulamento relativo à

a gigabits, na qual a disponibilidade e a adesão às redes de capacidade muito elevada permitam a utilização generalizada de produtos, serviços e aplicações», sendo da máxima importância para assegurar a velocidade e capacidade da rede sem fios para vários setores, como a IoT, a telemedicina, os veículos conectados, a gestão inteligente da energia, cidades verdes e inteligentes, entre outros. O principal fornecedor que se perfilhou no mercado europeu para as infraestruturas de banda larga 5G foi a chinesa *Huawei*, o que fez soar os alarmes do outro lado do Atlântico com várias pressões por parte do governo norte-americano para limitar a utilização de tecnologias da *Huawei* na UE à conta de preocupações relacionadas com a cibersegurança, designadamente a possibilidade de acessos indevidos (mas ao abrigo daquela jurisdição)<sup>193</sup>. A Comissão começou por reconhecer que *«uma vez implantadas, as redes 5G constituirão a espinha dorsal de uma vasta gama de serviços essenciais ao funcionamento do mercado interno e à manutenção e funcionamento de funções vitais da sociedade e da economia — energia, transportes, banca e saúde, bem como sistemas de controlo industriais. Para a organização dos processos democráticos, como eleições, recorrer-se-á também cada vez mais às infraestruturas digitais e às redes 5G»*<sup>194</sup>, razão pela qual se encontram especialmente sujeitas a ciberataques que podem afetar todos os EM da UE (tendo até em conta a natureza interligada e transnacional das infraestruturas subjacentes ao ecossistema digital), recomendando que na avaliação que cada EM fizesse dos riscos da implementação da estratégia para o 5G deveria ponderar, entre outros, mas já a pensar na fornecedora chinesa, *«os riscos decorrentes do quadro jurídico e político a que os fornecedores de equipamentos de tecnologias da informação e das comunicação podem estar sujeitos em países terceiros»*<sup>195</sup>. A mensagem não ficou clara o suficiente, o que motivou o alerta do Conselho para a necessidade de diversificação dos fornecedores a fim de evitar uma excessiva dependência, aconselhando expressamente a que escolha desses fornecedores obedeça também a *«fatores não técnicos, como o enquadramento jurídico e político a que os fornecedores podem estar sujeitos em países terceiros»*, de modo a proteger a *«soberania tecnológica europeia»* e a promover, a nível mundial, *«a abordagem seguida pela UE em matéria de cibersegurança das futuras redes de comunicações*

---

portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno (Regulamento (UE) 2017/1128 de 14.06.2017), o fim do *roaming* (Regulamento (UE) 2015/2120 de 25.11.2015 que estabelece medidas respeitantes ao acesso à Internet aberta), a nova Diretiva dos Direitos de Autor (Diretiva (UE) 2019/790 de 17.04.2019), a nova Diretiva dos Serviços de Comunicação Social Audiovisual (Diretiva 2010/13/UE de 10.03.2010) e as novas obrigações em matéria de transparência para as plataformas em linha (Regulamento (UE) 2019/1150 de 20.06.2019).

<sup>193</sup> America's war on Huawei nears its endgame. "The Economist". (16 Jul 2020). Consultado em: 29/08/2020. Disponível em: <https://www.economist.com/briefing/2020/07/16/americas-war-on-huawei-nears-its-endgame>

<sup>194</sup> COMISSÃO EUROPEIA – *Recomendação da Comissão de 26 de março de 2019. Cibersegurança das redes 5G*. COM(2019) 2335 final. Estrasburgo, 26.3.2019. p. 1.

<sup>195</sup> *Ibid*, p. 7.

*eletrónicas*»<sup>196</sup>. Este apelo à *soberania digital* e à *soberania tecnológica* da União Europeia tem-se, neste e noutros contextos, repetido, sendo, no entanto, disputado o seu exato sentido: «*para uns, é sobretudo sobre estratégia económica, enquanto que outros analisam a soberania tecnológica do prisma dos valores, da história e do direito internacional público*»<sup>197</sup>. Assim, o debate em torno da *soberania digital e tecnológica* na UE deve-se a quatro razões: cultura, controlo, competitividade e cibersegurança<sup>198</sup>. Para alguns autores, num mundo interdependente com cadeias de abastecimento globais, a soberania e a autonomia face aos demais não é, simplesmente, possível<sup>199</sup>. Parece claro, no entanto, que a soberania digital deve ser avaliada sob um prisma particular, não tendo o mesmo alcance da soberania dita tradicional, na medida em que necessita de ser articulada com a própria natureza circulante e transnacional dos dados e das infraestruturas digitais. No entanto, quando se fala em soberania tecnológica quer-se sobretudo salientar a necessidade de diminuição da dependência tecnológica face ao exterior e a preservação de um espaço de soberania ou, talvez melhor, de autonomia, em que a UE seja capaz de atuar efetivamente num mundo interdependente (quer como potência reguladora, quer como potência económica), nem que isso possa significar o surgimento de três *internets*, «*uma internet dos EUA, onde as regras criadas pelas empresas tecnológicas oferecem uma governança de facto; uma internet chinesa que é controlada nacionalmente, servindo os interesses do Estado e facilitando uma vigilância digital compreensiva; e uma internet europeia em que a UE, em nome do interesse público, regula as operações do mercado e das empresas digitais*»<sup>200</sup>.

<sup>196</sup> CONSELHO DA UNIÃO EUROPEIA – *Conclusões do Conselho sobre a importância da tecnologia 5G para a economia europeia e a necessidade de atenuar os riscos de segurança a ela associados – Conclusões do Conselho (3 de dezembro de 2019)*. 14517/19. Bruxelas, 3.12.2019. Em consequência destas Conclusões, a Comissão adotou já em janeiro de 2020 uma Comunicação em que admite restrições e até a exclusão fornecedores considerados de alto risco. COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da UE*. COM(2020) 50 final. Bruxelas, 29.1.2020.

<sup>197</sup> BAUER, Matthias; ERIXON, Dredrik - *Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls*. [s.l.]: European Centre For International Political Economy, 2020. p. 4.

<sup>198</sup> *Ibid.*, p. 8. As razões culturais partem da perceção de que a UE protege de forma diferente de outros parceiros os seus valores, o que se manifesta por exemplo na regulação em torno da proteção dos direitos humanos e da privacidade. O controlo refere-se ao desejo político de conseguir controlar as plataformas digitais e tecnológicas que armazenam dados gerados na UE. A competitividade reflete o receio de decadência industrial da Europa, incapaz de acompanhar e de competir no mercado mundial com as principais potências tecnológicas, apontando-se a ausência de gigantes tecnológicos europeus como prova de que a UE enfrenta um dilema em que ou se entrega às regras do mercado livre e liberal ou protege os seus valores fundamentais. A cibersegurança reflete as preocupações em torno da segurança e proteção de dados num ambiente digital cada vez mais global.

<sup>199</sup> *Ibid.*, p. 6.

<sup>200</sup> PUDDEPHATT, *Governing the internet...*, p. 23.

### Secção III – Cibercrime e conteúdos digitais ilegais.

MANUEL CASTELLS, no final do último século, dava conta de que apesar de «*a prática do crime ser tão antiga quanto a própria humanidade*», a era da informação havia desencadeado o crime global ou transnacional, com a «*formação de redes entre poderosas organizações criminosas e seus associados, com atividades partilhadas em todo o planeta*» o que afetava «*profundamente a economia no âmbito internacional e nacional, a segurança e, em última análise, as sociedades em geral*»<sup>201</sup>. Naquele momento, todavia, a preocupação ainda se concentrava na forma como as TIC facilitavam a organização de redes transnacionais dedicadas a crimes como o tráfico de droga, de seres humanos e de armas, a lavagem de dinheiro, e, muito em breve, o terrorismo. Poucos anos depois, e já nos alvares da Era Digital, a preocupação deslocava-se para o cibercrime e para os conteúdos digitais ilegais. Uma advertência se faça para referir que, neste âmbito, a terminologia, além de muitas vezes técnica, é vasta e pouco precisa<sup>202</sup>.

Aquando da sua fundação, a *Internet* surgiu como um expoente libertário, estando os seus criadores empenhados em desenvolver um espaço imaginário *além do Estado*, em que todos os indivíduos se podiam expressar em absoluta liberdade. Ainda hoje persistem alguns traços daquilo que haveria de ficar conhecido como *ciberlibertarismo*, o qual defende que a *Internet* e os restantes *media* digitais devem ser espaços de afirmação das liberdades individuais, *maxime* a de expressão, sendo por isso de recusar qualquer ingerência por parte dos Estados ou das próprias empresas privadas<sup>203</sup>. Todavia, a visão libertária da *Internet* como um espaço radical de liberdade logo começou a perder adesão, principalmente em face do abuso da liberdade

<sup>201</sup> CASTELLS, Manuel - *A Era da Informação: Economia, Sociedade e Cultura*. 3.<sup>a</sup> ed. Lisboa: Fundação Calouste Gulbenkian, 2014. Vol. III - O Fim do Milénio. p. 207-8.

<sup>202</sup> A ENISA (Agência Europeia para a Cibersegurança) recorre frequentemente a termos como ciberespaço (o conjunto presente e futuro de ativos tangíveis ou intangíveis que armazenam e/ou transferem informação eletrónica), cibersegurança (conjunto de atividades necessárias para a proteção do ciberespaço e os seus utilizadores), ciberhigiene (conjunto de práticas que devem ser implementadas e realizadas periodicamente para proteção dos utilizadores e dos negócios *online*), ciberincidente (qualquer ocorrência que tenha um impacto em qualquer um dos componentes do ciberespaço ou no seu funcionamento, independentemente de ter origem natural ou humana, maliciosa ou não-maliciosa, deliberada, acidental ou devido a erro humano), ciber-acidente (qualquer ocorrência relacionada com o ciberespaço que causa um dano significativo nesse espaço ou em qualquer outro ativo ou que cause danos pessoais), ciber-investigação, ciberataque (conjunto de ciber-acidentes de origem maliciosa que causa danos, disfuncionalidades ou perturbações), ciberameaça (uma circunstância, um evento ou uma ação potenciais suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas<sup>202</sup>), ciber-risco (uma circunstância ou evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação), cibercrime (conjunto de crimes que ou são facilitados ou são praticados no contexto do ciberespaço), ciber-sabotagem (corresponde um tipo particular de cibercrime), ciberdefesa (conjunto de mecanismos defensivos que podem ser usados para mitigar ou responder a um ciberataque), ciberespionagem (referente à espionagem com origem estatal ou industrial) ou ciberguerra (conjunto de ações desenvolvidas por Estados, grupos ou organizações criminais que tenham como alvo outro Estado e que sejam facilitadas ou praticadas usando o ciberespaço). Vide EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – *ENISA overview of cybersecurity and related terminology* [Em linha]. [s.l.]: ENISA, 2017.

<sup>203</sup> DAHLBERG, Lincoln - *Cyberlibertarianism*. [s.l.]: Oxford University Press, 2017.

*online*<sup>204</sup>. A UE, por seu turno, embora reconhecendo a sua importância social, educacional, cultural e económica, desde cedo salientou o potencial da *internet* para a difusão de conteúdos ilegais e para a facilitação do crime. De facto, as preocupações não foram em vão, sendo hoje o discurso criminal em torno do ciberespaço orientado em dois vetores: a disseminação de conteúdos ilegais *online* e uma área mais restrita do cibercrime focada na cibersegurança e nos ciberataques. Começando pelos últimos, são em grande número as ciberameaças identificadas na UE, acompanhando a tendência de contínuo desenvolvimento das técnicas que possibilitam o uso malicioso das redes, num permanente ciclo em que cada ajuste nos mecanismos de ciberdefesa dá lugar a mais avançados, coordenados, criativos e complexos ciberataques. Ora, atendendo à crescente dependência em relação às tecnologias digitais (e as previsões relativas à multiplicação dos objetos inteligentes no âmbito da IoT<sup>205</sup>), o grau de exposição e de risco – que é transversal a todos os níveis, desde o governamental, ao empresarial e ao individual – aumenta proporcionalmente. Além do mais, o impacto económico do cibercrime não deve ser ignorado, havendo estudos que sugerem que o mesmo possa ir, na economia global, até aos 608 mil milhões de dólares (o que equivale a cerca de 0,80% do PIB global), e que, no caso europeu, possa representar 0,89% do PIB<sup>206</sup>. A cibercriminalidade é hoje oferecida *online*, principalmente na *darkweb*, como um serviço pronto a ser usado (*cybercrime-as-a-service*), o que aponta para a crescente profissionalização e sofisticação dos atores envolvidos nestas práticas. A cibercriminalidade tanto pode ter origem em atores estatais como não estatais. Em todo o caso, e como reconhece a Comissão Europeia, «a ameaça criminosa é reforçada pela definição pouco clara do limite entre a cibercriminalidade e o crime “tradicional”, uma vez que os criminosos utilizam a Internet quer como forma de intensificarem as suas atividades, quer como uma fonte para encontrarem novos métodos e ferramentas para a prática de crimes»<sup>207</sup>. Neste contexto, a grande problemática é, possivelmente, a atribuição da responsabilidade, na medida em que se colocam enormes dificuldades na localização dos agentes, os quais recorrem frequentemente a técnicas como a encriptação, a anonimização e a

<sup>204</sup> O que obrigou os EUA a, logo nos anos 90, com o crescimento comercial da *internet*, a regular certos conteúdos *online*, designadamente em torno da “decência”, da segurança infantil e dos direitos de autor. Foi o caso do *Communications Decency Act* de 1996 que procurava proibir a transmissão e exibição de conteúdos pornográficos a menores, o qual acabou por ser declarado inconstitucional pela *Supreme Court* por violar a liberdade de expressão protegida ao abrigo da Primeira Emenda no caso *Renov. American Civil Liberties Union*.

<sup>205</sup> Que é, diga-se, uma das áreas mais vulneráveis, como prova o sucedido em 2016 com o *malware* Mirai que explorava vulnerabilidades em objetos da IoT para criar uma *botnet* (ou rede *bots*) destinada lançar um ataque *DDoS* que impediu o acesso dos utilizadores a plataformas como a Netflix, o Twitter ou a Amazon.

<sup>206</sup> LEWIS, James. – *Economic Impact of Cybercrime – No Slowing Down*. McAfee: [s.l.], 2018.

<sup>207</sup> COMISSÃO EUROPEIA e ALTA REPRESENTANTE DA UNIÃO PARA OS NEGÓCIOS ESTRANGEIROS E POLÍTICA DE SEGURANÇA – *Comunicação Conjunta ao Parlamento Europeu e ao Conselho. Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE*. JOIN(2017) 50 final. Bruxelas, 13.9.2017. p. 2.

atribuição do mesmo endereço de IP a múltiplos utilizadores, o que torna complexo não só o processo de identificação dos atores, como também a identificação da localização a partir da qual atuam (ou onde se encontra a infraestrutura criminosa ou, ainda, as provas eletrónicas), o que tem impactos no âmbito da competência jurisdicional para o prosseguimento da ação penal<sup>208</sup>. Por outro lado, é preciso ter em conta que a cibercriminalidade pode nunca chegar a ser detetada pelas vítimas, principalmente aquelas com poucas competências digitais, ou, então, pode ser detetada semanas ou meses após o lançamento dos ataques. Mais ainda: muitas vítimas, principalmente organizações que dependem da confiança e proteção dos dados pessoais dos seus consumidores, não reportam os ciberataques sofridos nem os danos por eles causados.

Entretanto, as ciberameaças e os cibercrimes são de variada ordem, sendo os mais comuns cometidos com recurso ao *malware*<sup>209</sup>. Outro ataque de alto impacto, principalmente para vítimas institucionais e organizações, consiste nas designadas (*Distributed*) *Denial of Services* (*DoS* ou *DDoS*), situação em que o agente procura fazer com que um sistema ou uma rede inteira fique temporária ou indefinidamente indisponível para os seus utilizadores. Com o grande número de objetos ligados à rede, têm crescido as preocupações em torno destes ataques, os quais podem potencialmente causar disrupções em sistemas críticos e perturbações transnacionais para as organizações e Estados. Um tipo específico de *malware* é o *ransomware* ou *software* de resgate, muito referido e temido, principalmente no seguimento de ataques de grande escala como o “WannaCry” (uma das vítimas foi o *NHS* britânico) e o “Petya”. O *ransomware*, ao infetar um computador ou uma rede, impossibilita (ora através do bloqueio, ora através da encriptação) que as vítimas acedam, total ou parcialmente, aos dados armazenados no sistema, sendo que para readquirem esse acesso as vítimas têm primeiro de pagar um resgate monetário (geralmente em criptomoeda). As vítimas, além de sofrerem uma perda financeira, sofrem também uma perda de credibilidade e confiança por parte do público. A maioria dos ciberataques tem como objetivo ou efeito uma violação de dados (*data breach*) dos sistemas infetados, que ora se perdem ou ficam comprometidos<sup>210</sup>. Os *data breaches* podem

<sup>208</sup> Os vários desafios que se colocam ao combate ao cibercrime estão bem identificados pelo Eurojust e pela Europol. Vide EUROPOL. EUROJUST – *Joint Report: Common challenges in combating cybercrime as identified by Eurojust and Europol* [Em linha]. [s.l.]: Europol and Eurojust Public Information, 2019.

<sup>209</sup> O *malware* corresponde a qualquer *software* malicioso criado intencionalmente para causar danos a um computador, servidor ou rede de computadores, por exemplo furtando ou apagando (*wiper*) dados ou impedindo o acesso dos utilizadores à rede. Alguns dos principais tipos de *malware* são os *Trojan* (*malware* que se apresenta como um *software* legítimo de modo a convencer a vítima a instalá-lo), os vírus (tipo de *malware* que se encontra “anexado” a um programa, ficheiro ou documento), os *worms* (um subtipo de vírus que se multiplica sem necessidade de intervenção humana) e os *spywares* (tipo de *malware* que espia a atividade da vítima sem o seu conhecimento ou consentimento, podendo registar dados relevantes, como palavras-passe). Vide ENISA – *ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends*.

<sup>210</sup> É possível definir uma violação de dados como um incidente que provoque, de modo acidental ou malicioso, a

também ocorrer por via da ciberespionagem levada a cabo por atores estatais ou empresariais e, ainda, provir de *leaks* intencionais ou não intencionais.

Do ponto de vista do Estado, a cibercriminalidade acarreta significativas perdas económicas, a que se podem somar perdas financeiras quando os próprios órgãos de governo ou de administração pública são as vítimas de ataques de *ransomware*. Todavia, mais do que as perdas económicas, a cibercriminalidade, até pela dificuldade de investigação, de atribuição e de prossecução da ação penal, erode a confiança dos cidadãos nas instituições. Por outro lado, os ciberataques podem ter efeitos mais diretos e disruptivos para a vida em comunidade, nomeadamente quando em causa está o ataque informático a infraestruturas críticas<sup>211</sup>. Estes ciberataques, ao contrário dos ataques a setores como o financeiro e o bancário, não têm como principal objetivo uma violação de dados, mas, antes, «*assumir o controlo da infraestrutura crítica para causar danos físicos*»<sup>212</sup>, podendo ter impactos disruptivos enormes tendo em conta a interligação e dependência transnacional destas redes na UE<sup>213</sup>, a que se soma o crescente número de redes e sistemas críticos inteligentes. Assim, um ciberataque em relevantes infraestruturas sociais pode muito facilmente colocar em causa serviços e funções essenciais (e soberanas) prestadas ou reguladas pelo Estado. Estas preocupações são ainda mais prementes quando se sabe que ao nível da União os Estados-Membro dispõem de capacidades tecnológicas distintas, principalmente no que diz respeito à implementação de ligações de banda larga à rede, a que se juntam as assimetrias internas entre regiões urbanas e rurais.

Mas a cibercriminalidade pode também deixar marcas no funcionamento do sistema democrático, principalmente se os ciberataques se concentrarem em períodos críticos, como é o caso dos eleitorais. Nesta sede, a ENISA identifica como ciberameaças a interseção de dados, os *leaks*, o *phishing*, o *malware* e os ataques *DDoS* a comissões eleitorais, a sistemas de partidos

---

destruição, a perda, a alteração, a divulgação ou o acesso de dados, incluindo informações sensíveis relacionadas com instituições e organizações ou simples dados pessoais de indivíduos (por exemplo, informação bancária, dados médicos, etc.). Um dos maiores *data breaches* dos últimos anos ocorreu em 2017, quando foram comprometidos os dados bancários de quase 147 milhões de norte-americanos e 15 milhões de cidadãos britânicos armazenados pela empresa *Equifax* e que deu origem a inúmeros casos de roubo de identidade.

<sup>211</sup> Definidas como «o elemento, sistema ou parte deste 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». São exemplos de infraestruturas críticas as redes e instalações de eletricidade e de gás natural, as refinarias, as barragens e os sistemas de transporte e distribuição de água, entre outras. Vide art.º 2.º, al. a) da Diretiva 2008/114/CE do Conselho de 8 de Dezembro de 2008 relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

<sup>212</sup> ONYEJI, Ijeoma; BAZILIAN, Morgan; BRONK, Chris - *Cyber Security and Critical Energy Infrastructure*. The Electricity Journal. Vol. 27. n.º 2 (2014). p. 54.

<sup>213</sup> Por exemplo, em 2006, um ocorreu um apagão elétrico que, tendo tido origem na Alemanha, afetou quinze milhões de residências em vários países europeus, incluindo Portugal, tendo inclusive chegado a Marrocos. Cfr. ONYEJI, et. al., *Cyber Security and Critical...*, p. 55.

e campanhas, ao registo de eleitores, aos sistemas de contagem de votos e de disseminação dos resultados, etc.<sup>214</sup>. Não obstante, e tendo em conta que a maioria dos EM da UE adiou ou descontinuou o voto eletrónico<sup>215</sup>, as grandes vulnerabilidades ocorrem durante as campanhas eleitorais em que agentes politicamente motivados podem distribuir *SPAM* ou *psinshing* através das redes sociais ou outros sistemas de comunicação, levando à introdução de *malwares* nos sistemas das campanhas com acesso a informações sensíveis e privadas e a sua posterior divulgação ou para difamação (*doxxing*) ou para uma tentativa de influência eleitoral<sup>216</sup>.

Olhando, agora, para a disseminação de conteúdos ilegais no ciberespaço, notamos que as primeiras preocupações foram dirigidas contra a produção, oferta, difusão, obtenção ou posse de pornografia infantil, como resulta da obrigação de criminalização destes comportamentos pelos Estados-parte da Convenção sobre o Cibercrime enquadrada no âmbito do Conselho da Europa e concluída em 2001 (art.º 9.º). No mesmo instrumento, dá-se também enfoque à criminalização da violação de direitos da propriedade intelectual, designadamente direitos de autor e direitos conexos e direitos de propriedade industrial, sendo certo que ainda hoje a pirataria e o *upload* ilegal de obras (principalmente musicais e audiovisuais) na *internet* permanece um problema sério sem solução óbvia, na medida em que as tecnologias digitais de reprodução, armazenamento e partilha de informação vieram facilitar desmesuradamente a difusão destes conteúdos, que se multiplicam na rede (*once in the Internet, always on the Internet*), com frequência carregados pelos utilizadores em plataformas digitais sem prévia autorização dos respetivos titulares dos direitos de autor<sup>217</sup>. Entretanto, e a acompanhar a “canibalização” do discurso *online*, cedo surgiram preocupações em torno da liberdade de expressão em linha, principalmente quando ela é usada para promover o discurso de ódio, a instigação à violência, o assédio, a difamação e, até, o recrutamento e a ação terrorista. Neste sentido, logo em 2003, foi concluído, no âmbito da Convenção sobre o Cibercrime, um Protocolo Adicional para a incriminação de atos de natureza racista e xenófoba praticados através dos sistemas informáticos, obrigando os Estados-parte a adotar medidas legislativas e outras destinadas a classificar como infração penal a distribuição e outras formas de disponibilização ao público de material daquela ordem, incluindo a ameaça e o insulto por

<sup>214</sup> EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – *Election Cybersecurity: challenges and opportunities*. [Em linha]. [s.l.]: ENISA, 2019.

<sup>215</sup> Exemplos de países que recorrem a tecnologias de voto eletrónico na UE são a Estónia e a Bélgica. *Ibid.* p. 7.

<sup>216</sup> BOSSETTA, *The Weaponization of social media...*, p. 99.

<sup>217</sup> A este respeito, foi repetidamente colocada em causa a posição das plataformas digitais que, atuando como intermediárias, se desresponsabilizavam quanto aos conteúdos partilhados pelos seus utilizadores, muito embora beneficiem dessa partilha. Recentemente, a UE veio exigir às plataformas digitais as necessárias autorizações através da concessão de licenças. Cfr. Diretiva (UE) 2019/790 de 17.04.2019 relativa aos direitos de autor e direitos conexos no mercado único digital.

motivos racistas e xenófobos. A par disto, o Protocolo Adicional previa também a criminalização da negação, minimização grosseira, aprovação ou justificação do genocídio e de outros crimes contra a humanidade conforme definidos no Estatuto de Roma do TPI, o que inclui, por exemplo, a negação do Holocausto. Este Protocolo é ainda anterior ao surgimento da maioria das plataformas digitais, sendo que até aí os conteúdos ilegais eram colocados essencialmente na blogosfera. Com o alvor das redes sociais, passou a ser mais fácil e mais comum, até pelo número de utilizadores, a difusão deste tipo de conteúdos em linha, ao mesmo tempo que diminuiu a capacidade de deteção e remoção. Apesar de as grandes plataformas digitais terem políticas de autorregulação que proíbem este tipo de conteúdos, existe uma rede paralela de fóruns e redes, que não se limitam aos espaços na *darkweb*, que advogam a liberdade de expressão total e facilitam a distribuição destes conteúdos<sup>218</sup>.

#### **Secção IV – Novas tecnologias disruptivas.**

A velocidade com que as inovações digitais se têm multiplicado no último par de décadas faz crer que os próximos anos conheçam novas tecnologias digitais, as quais terão, presumivelmente, as características seguintes: complexidade (devido à interação de um número crescente de componentes e atores digitais), opacidade (que se associa à complexidade e resulta num “efeito de caixa negra”, em que não é possível compreender o processo inerente à realização de uma tarefa), abertura (decorrente da contínua necessidade de atualizar as tecnologias digitais e da necessidade de interação com outros sistemas ou fontes de dados para que aquelas funcionem corretamente), autonomia (referente à desnecessidade de *inputs* humanos para que as tecnologias desempenhem tarefas devido à capacidade de alterarem os próprios algoritmos e auto-aprenderem a partir dos dados que recolhem), imprevisibilidade (associada à capacidade de identificar e classificar novos estímulos), *data-drivenness* (relacionada com dependência de informação externa não pré-instalada, mas antes comunicada através de sensores ou outras fontes exteriores) e vulnerabilidade (resultante das restantes características)<sup>219</sup>. A este respeito, e porque se tratam ainda de tecnologias em desenvolvimento que aguardam a penetração nos respetivos mercados, esta secção assume caráter especulativo

<sup>218</sup> Vide, a este propósito, um interessante estudo acerca da rede social *Gab*, semelhante ao Twitter, que afirma ser a “campeã da liberdade de expressão”. O estudo concluiu que ¼ do tráfego gerado nessa rede era discurso de ódio. MATHEW, Binny; GOYAL, Pawna; DUTT, Ritam; MUKHERJEE, Animesh - *Spread of Hate Speech in Online Social Media*. WebSci'19: Proceedings of the 10th ACM Conference on Web Science. (2019).

<sup>219</sup> EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES – NEW TECHNOLOGIES FORMATION - *Liability for Artificial Intelligence and other emerging digital technologies*. [s.l.]: Publications Office of the European Union, 2019. p. 32 e ss.

partindo da proposição de que, à luz da experiência passada, é razoável assumir que estas novas tecnologias serão disruptivas e terão impactos, muitos deles ainda imprevisíveis, para o Estado de Direito democrático.

A Comissão Europeia avança que, «*nos próximos 10 anos, 50 mil milhões de objetos, desde residências a automóveis e relógios, fiquem ligados a nível mundial, a grande maioria através tecnologias sem fios*»<sup>220</sup>. Num futuro próximo, deverá, pois, generalizar-se a IoT ou *Internet das Coisas*, além da computação de alto desempenho (ou computação quântica), a condução conectada e automatizada, as cirurgias à distância, etc. O desenvolvimento das redes 5G e 6G serão essenciais para dotar o ambiente digital das capacidades técnicas que permitirão o aproveitamento destas tecnologias. Esta generalização terá impactos significativos nos processos empresariais e nas interações sociais, acarretando preocupações crescentes devido ao volume de dados que será gerado e ao conhecimento que isso potencia dos utilizadores dessas tecnologias, o qual, associado ao aumento da capacidade de processamento, pode ser usado para a previsão comportamental e a manipulação das audiências, além da ainda insuficiente resposta ao problema da responsabilização destes sistemas. Por outro lado, a ligação em rede de um número crescente de objetos aumenta a suscetibilidade e os efeitos dos ciberataques, além de dilatar a dependência das sociedades das *big tech*, sem esquecer o potencial excludente destas tecnologias, que acumularão o fosso entre regiões e entre gerações. Todos estas tecnologias integram a categoria *catch-all* da Inteligência Artificial (IA), que pode ser definida como o conjunto de sistemas (*software* e *hardware*) «*criados por humanos e que, perante um objetivo complexo, agem no mundo físico ou na dimensão digital, compreendendo o ambiente que os rodeia através da aquisição de dados, interpretando os dados recolhidos (estruturados ou não), raciocinando no conhecimento adquirido ou processando a informação que resulta desses dados, e decidindo as melhores ações a tomar para atingir o objetivo determinado. Os sistemas de AI tanto podem usar regras simbólicas ou usar um modelo numérico, podendo também adaptar o seu comportamento analisando a forma como o ambiente é afetado pelas suas ações anteriores*»<sup>221</sup>. A IA, enquanto categoria lata (que combina dados, algoritmos e capacidade computacional), dá origem a disciplinas científicas específicas como “raciocínio e tomada de decisões”, “aprendizagem” (que inclui o *machine learning*, as redes neurais, o *deep learning*, as árvores de decisão, entre outras técnicas) e robótica (que corresponde à IA em ação

<sup>220</sup> COMISSÃO EUROPEIA – Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Conectividade para um Mercado Único Digital Concorrencial – Rumo a uma Sociedade Europeia a Gigabits. COM(2016) 587 final. Bruxelas, 14.9.2016. p. 2.

<sup>221</sup> HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE - A definition of AI: Main capabilities and scientific disciplines. Bruxelas: Comissão Europeia, 2019. p. 6.

no mundo físico). As tecnologias associadas à IA poderão agravar significativamente o problema da desinformação, por exemplo através do recurso ao *deep learning*. Estas técnicas (que dão origem às *deep fakes*) permitem manipular imagens e vídeos, ora alterando o comportamento das pessoas, ora criando pessoas falsas ou alterando a aparência do local onde um evento ocorreu, ao ponto de se tornar virtualmente impossível distinguir a versão manipulada da versão original. A utilização de vídeos e imagens representa, em termos de emotividade do discurso e de credibilidade, um passo em frente na eficácia da desinformação.

### CAPÍTULO III: O ESTADO DE DIREITO DEMOCRÁTICO EM RISCO.

Analizados os vários perigos associados às tecnologias e práticas da Era Digital, é tempo de concluirmos pelos riscos que eles podem representar para o Estado de Direito democrático, os quais serão analisados sob vetores como a liberdade de expressão, o pluralismo, a disrupção dos processos democráticos e a interferência em processos eleitorais, e, ainda, a destabilização da esfera pública necessária à democracia deliberativa e participativa. É relevante esclarecer que a nossa análise parte do pressuposto da mais-valia do modelo deliberativo e discursivo de democracia<sup>222</sup>, assente numa esfera pública “forte” onde os assuntos de interesse público são discutidos, entre cidadãos iguais, através de um processo normativo assente em argumentos racionais por forma a alcançar-se um consenso acerca do bem comum<sup>223</sup>. Essa argumentação tem lugar, por excelência, na *esfera pública*, conceito introduzido por HABERMAS e que se refere à arena comunicacional onde a «*sphere of private people come together as a public*» de modo a articularem «*the needs of society with the state*»<sup>224</sup>. Essa arena é constituída, por um lado, pelos meios de comunicação social e, por outro, pelos espaços em que os cidadãos ativamente

<sup>222</sup> Não é possível desenvolver aqui as tradições da teoria democrática e descrever em detalhe os modelos democráticos participativos, discursivos/deliberativos, liberais/representativos ou construtivista. Em todo o caso, sempre diremos que na teoria liberal/representativa o papel principal do cidadão é votar, estando a esfera pública reservada para os especialistas e as elites. Para as teorias participativas, é importante tornar os cidadãos parte ativa das decisões públicas que afetam a comunidade, num modelo que se aproxima da democracia direta. O enfoque das teorias discursivas está no processo deliberativo, o qual, em questões de relevo, deve ser alargado a atores que não se encontrem no centro do sistema político, designadamente à esfera pública onde a única força é a do melhor argumento. Finalmente, os construtivistas adotam uma visão mais pessimista, colocando ênfase no facto de os resultados do discurso público serem fruto das relações de poder pré-existentes na sociedade. Para mais, vide FERREE, Myra Marx; GAMSON, William A.; GERDARDS, Jürgen; RUCHT, Dieter - *Four models of the public sphere in modern democracies*. Theory and Society. Vol. 31. (2002).

<sup>223</sup> De notar que existem variantes quanto ao objetivo do processo deliberativo, o qual pode não ter como resultado o consenso. Seguimos, aqui, a posição de JOSHUA COHEN, para quem a deliberação ideal deve alcançar o consenso motivado pela razão na medida em que ao longo da discussão se avancem razões que sejam persuasivas para todos. No entanto, obviamente que o consenso nunca está garantido (embora, segundo HABERMAS, os participantes devem assumir que ele é possível), pelo que falhando deve ser adotada a regra da maioria. Vide COHEN - *Deliberation and Democratic Legitimacy*, p. 75.

<sup>224</sup> HABERMAS, Jürgen - *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Massachusetts: The MIT Press, 1991. p. 27 e 176.

comunicam entre si. Na concepção “burguesa” de HABERMAS<sup>225</sup>, esta segunda esfera pública não conhecia mediação (ou *gatekeeping*), sendo diretamente exercida em fóruns sociais públicos como cafés, salões e praças<sup>226</sup>. Para o que aqui nos interessa, entendemos que a esfera pública funciona, em sociedades pluralistas, enquanto um agregado dos fóruns temáticos interconectados em rede (sejam eles temáticos, locais, regionais, nacionais ou supranacionais), onde se discutem (idealmente recorrendo à argumentação racional, embora também haja espaço para a emoção) assuntos de interesse coletivo e, ao mesmo tempo, onde se desenrola a luta e o conflito político e a contestação social<sup>227</sup>, funcionando essa “esfera de esferas em rede” (a par de outros mecanismos como as eleições) como referencial da vontade coletiva e da noção partilhada de bem comum<sup>228</sup>. Independentemente do concreto modelo de democracia defendido, a existência de um espaço comunicativo que medeia entre os cidadãos e o poder é, num sentido muito abrangente, largamente aceite como requisito democrático<sup>229</sup>.

Com a *internet*, a esfera pública transformou-se e passou a incluir fóruns públicos *virtuais*, primeiro na blogosfera e, mais tarde, nas redes sociais e plataformas digitais, que se caracterizam pela sua horizontalidade (por oposição à verticalidade que persiste nos *media* tradicionais). Estas plataformas funcionam, pelo menos em teoria, como espaços abertos em que todos os cidadãos (com acesso) se podem expressar. Enquanto “rede de redes”, a *internet*

<sup>225</sup> Sujeita que está, evidentemente, a todo o criticismo, sintetizada nas seguintes palavras GOMES CANOTILHO, no prefácio ao livro “*Um Ensaio sobre a Constituição da Europa*”: «a construção habermasiana é criticada por muitos e acusada de ser uma «fantasmagoria» normativa própria de um espírito utópico».

<sup>226</sup> De forma sumária, a esfera pública habermasiana consiste em quatro elementos essenciais: (1) os cidadãos devem contribuir ativamente no processo político dos assuntos de interesse coletivo, (2) a esfera pública requer uma arena ou fórum com determinadas características estruturais, designadamente abertura (sendo acessível a todos quantos queiram participar), liberdade de partilha e troca de opiniões e ideias e independência quer do Estado quer de influências económicas, (3) o processo deliberativo na esfera pública deve obedecer às regras de um debate racional e crítico, o qual requer reciprocidade, (4) é necessária a existência de meios de comunicação social que funcionam como um fórum de debate em si mesmo e como guardiões da esfera pública, informando os seus participantes. Uma nota mais para acrescentar que o debate racional, normativamente ancorado, determina que os participantes cumpram certas regras ou condições discursivas, como, por exemplo, terem um interesse comum na verdade e existir igualdade formal e substancial, sendo a primeira apontada à ideia de que o processo deliberativo não exclui ninguém, dando a todos voz igual na decisão; a igualdade substancial traduz o facto de que «a distribuição de poder e recursos pré-existente não altera as oportunidades dos participantes em contribuir para a deliberação» (COHEN - *Deliberation and Democratic Legitimacy*, p. 74).

<sup>227</sup> De modo a incluir também as “teorias agnósticas” e do “pluralismo radical” associadas sobretudo a CHANTAL MOUFFE, e que têm, a nosso ver, a vantagem de serem modelos mais próximos da realidade, ao passo que o modelo deliberativo parte de uma base idealista e racional. Para os agnósticos, a premissa é a da «*instabilidade radical do social concebido primariamente como antagonista*», uma vez que os indivíduos se encontram «*profundamente embrenhados em comunidades distintas*», tendo um apego «*apaixonado*» às suas concepções de bem comum, as quais não estão dispostos a abandonar. Nunca sendo possível alcançar o consenso pleno, todos os «*acordos são contingentes e estratégicos*». Cfr. DAHLBERG, Lincoln; SIAPER, Eugenia - *Introduction: Tracing Radical Democracy and the Internet*. In DAHLBERG, L. & SIAPER, E. *Radical Democracy and the Internet*. London: Palgrave Macmillan, 2007. p. 9.

<sup>228</sup> KARPPINEN, Kari - *European Public Spheres and the Challenge of Radical Pluralism*. In MORING-SALOVAARA, I. *Manufacturing Europe: Spaces of Democracy, Diversity and Communication* Göthenburg: NORDICOM, 2009. p. 59.

<sup>229</sup> *Ibid.*, p. 57.

veio, por um lado, diminuir o limiar de participação, permitindo que mais pessoas (e pessoas que não acediam a outros fóruns) façam parte do debate e da opinião pública, aumentando, assim, a heterogeneidade dos participantes. Mas, ao mesmo tempo, a *internet* contribui para uma segmentação e diferenciação (ainda maior) da esfera pública, o que resulta dos muito distintos tópicos debatidos, estilos e participantes envolvidos em cada subgrupo ou sub-fórum<sup>230</sup>. Esta segmentação – diz-se – prejudica a coesão social dentro da comunidade política e a promoção de um conjunto mais ou menos partilhado de normas e valores<sup>231</sup> o que conduz à «*polarização dos debates, ao isolamento de grupos temáticos, à participação desigual, à falta de responsividade e respeito no debate, ao discurso não cívico e de ódio*»<sup>232</sup>. Por outro lado, a tendência *online* é de que nos debates não prevaleça a força do melhor argumento, uma vez que a falta de mediação e de presença física dos participantes (associada à anonimização) leva à prevalência das características privadas do discurso. Não obstante as potencialidades do *online* para alargar os horizontes da esfera pública, *maxime* a virtual, dando voz a indivíduos e grupos muitas vezes marginalizados pelos *media* tradicionais, a verdade é que a “abertura” e a ausência de “mediação” nas plataformas digitais deve ser olhada com cautelas, isto porque não é possível ignorar o carácter excludente das redes, às quais só acede quem tem as capacidades tecnológicas para tal (muito embora essa base pareça aumentar continuamente), ora pelo surgimento daquilo a que chamaríamos uma “mediação algorítmica discreta” que, baseada em interesses económicos, procede a uma curadoria do discurso por via da personalização e da filtragem de conteúdos e dos sistemas de recomendação, assim permitindo fenómenos como as “câmaras de eco” ou as *filter bubbles*. Na mesma lógica, as plataformas digitais, e apesar do seu aparente compromisso para com o pluralismo e a liberdade de expressão, podem ser facilmente utilizadas e manipuladas como armas de promoção de certos interesses políticos<sup>233</sup>. Aliás, as ferramentas tecnológicas que integram essas plataformas parecem frequentemente ter sido desenhadas de modo a facilitar a manipulação da opinião pública. A este propósito, as redes sociais têm aquilo que descreveríamos como um efeito igualitário no acesso e desigualitário na permanência, uma vez que se é verdade que a ausência de barreiras à entrada (v.g.: gratuidade, literacia, etc.) contribui para a inclusão popular, também não deixa de ser verdade que a lógica numérica e métrica das redes faz com que se transfira para o *online* as hierarquias sociais e as estruturas de

<sup>230</sup> RASMUSSEN, Terje - *Internet-based media, Europe and the political public sphere*. Media, Culture & Society. Vol. 35. n.º 1 (2013). p. 99.

<sup>231</sup> KARPPINEN, *European Public Spheres...*, p. 60.

<sup>232</sup> RASMUSSEN, *Internet-based media...*, p. 99.

<sup>233</sup> BAYER et. al., *Disinformation and propaganda...*, p. 52.

poder prevalentes no mundo *offline*<sup>234</sup>, sendo tudo medido em termos de alcance (amigos, comentários, partilhas, etc.), lógica essa de que depende o próprio modelo das redes.

Quando colocada a esfera pública e o processo democrático em confronto com os perigos identificados, um dos maiores riscos que cremos existir é o da autenticidade do próprio discurso e das conclusões (em termos de decisões coletivas, o que extravasa o momento eleitoral) que dessa esfera se pode extrair. Naturalmente, a questão da autenticidade não se coloca apenas no contexto digital, mas aqui aparece de forma acutilante, sobretudo graças à abertura popular das plataformas digitais. Assim, é crível que na esfera pública virtual alguns debates ou conteúdos dominantes e que apontam para um consenso ou uma maioria de participantes a apoiar certas opções discursivas não passe do resultado de processos de amplificação automática ou de manipulação, o que legitima que se questione de quem são as ideias que circulam na esfera pública virtual: são realmente dos utilizadores, de atores de desinformação, ou são o resultado de um processo de filtragem de conteúdos que exclui visões concorrentes? O discurso público *online*, para ser efetivo, tem de ser transparente, ainda que os seus participantes permaneçam anónimos, não devendo ser “assaltado” por mecanismos automáticos ou algoritmos, nem por atores que distorcem as mensagens e o verdadeiro alcance das propostas aí difundidas. Do mesmo modo, a utilização crescente de redes privadas e encriptadas, completamente opacas, conduz à fragmentação da esfera pública e à divisão da sociedade «*em várias plataformas que agregam os indivíduos com a mesma mundividência e que completamente alienam outros indivíduos com opiniões diferentes*»<sup>235</sup>. A fragmentação da esfera pública é ainda visível em redes sociais que conservam a característica da abertura, na medida em que a automação leve a uma refração total das narrativas sociais o que agrava a polarização, a qual, a partir de certo limiar, torna precário o consenso em torno de um conjunto mínimo de valores comuns da comunidade, como a própria democracia, o Estado de Direito e os direitos fundamentais. Outra preocupação é a circunstância de a “inundação” de conteúdos na esfera pública virtual originada pela cacofonia de “vozes artificiais e amplificadas” conduzir à completa supressão de participantes com menor capital social, assim diminuindo também a visibilidade das suas propostas<sup>236</sup> e afetando o pluralismo das sociedades. Em última análise, com os seus processos algorítmicos, as plataformas sociais digitais tomam decisões subjetivas sobre quais e a quem

<sup>234</sup> NEUDERT et. al., *Polarisation and the use of...*, p. 20. Refere-se aqui, muitas vezes, a prevalência do efeito «*rich get richer*» em que quem já dispõe de largas redes sociais *offline* acaba por, em proporção, beneficiar mais na socialização *online*, ou a situação em que um conjunto reduzido de vozes com vasto capital social é dado um desproporcional poder de influência sob o fluxo de informação, o que pode, em teoria, levar ao reforço das hierarquias, à centralização do poder à manutenção de desigualdades eleitorais (em que, por exemplo, os candidatos independentes e os partidos pequenos têm um reduzido alcance nas redes sociais).

<sup>235</sup> BAYER et. al., *Disinformation and propaganda...*, p. 55.

<sup>236</sup> *Ibid*, p. 64.

expor ou não expor determinados conteúdos, criando, por isso, sistemas que empoderam ou aniquilam a visibilidade dos cidadãos, não ficando assegurada a igualdade formal e substancial dos participantes no fórum. Estes processos de modelação do discurso público *online*, em que se criam e ajustam narrativas em massa e para as massas, alteram a distribuição do poder e aumentam o risco da manipulação do ciberespaço para a promoção de discursos que se lhe ajustam perfeitamente, como é o caso das técnicas de comunicação populistas, as quais representam um risco sério para a democracia liberal<sup>237</sup>.

Em contextos eleitorais, os perigos antes referidos são ainda mais evidentes. Em última instância, principalmente se houver suspeitas de ciberataques ou campanhas de desinformação e manipulação em grande escala, podem levar a que todo o processo eleitoral, *maxime* o seu resultado, seja colocado em causa e, conjuntamente com ele, o próprio carácter democrático do sistema, uma vez que como refere DAHLBERG et. al., o termo democracia «*tornou-se um sinónimo universal de legitimidade política*»<sup>238</sup>. Por outro prisma, «*sem um público informado acerca dos problemas prementes, as decisões políticas e sociais cruciais não podem, simplesmente, ser tomadas*»<sup>239</sup>, o que significa que os direitos de informação (e informação verdadeira, completa e elucidativa) e de consulta são essenciais à democracia, designadamente no modelo deliberativo, uma vez que sem eles os cidadãos são extirpados do direito a participarem efetivamente no debate político munidos do conhecimento necessário para avaliar as diferentes propostas de bem comum em confronto. Assim, quanto mais (bem) informado se encontrar o público, maior será a qualidade processual do resultado alcançado e maiores serão as resistências à desinformação e à manipulação. Pelo contrário, se os cidadãos não tiverem acesso à informação ou se os conteúdos desinformativos e manipulativos se sobrepuserem à própria informação legítima, a participação dos cidadãos no debate e o consequente voto pode estar equivocado, assim se violando o direito a eleições livres e imparciais (art.º 3.º do Protocolo Adicional à CEDH). Estas circunstâncias são especialmente evidentes no caso do *micro-targeting* e dos *dark ads* de conteúdo político, sendo possível imaginar cenários em que as forças políticas apenas revelam fragmentos dos seus programas a eleitores com determinado perfil, excluindo outros temas que sabem à partida que esses utilizadores não apoiarão. Na mesma linha de pensamento, tanto a personalização e filtragem de conteúdos, como o micro-

---

<sup>237</sup> Sem desmesurados rigores, definimos aqui populismo como uma «*ideologia fina que considera que a sociedade se encontra, em última análise, dividida em dois grupos homogéneos e antagónicos*», i.e., as elites e os cidadãos comuns, sendo que «*soberania última e irrestrita pertence ao povo*». Cfr. ERNST, Nicole; ENGESSER, Sven; BÜCHEL, Florin; BLASSNIG, Sina; ESSER, Frank - *Extreme parties and populism: an analysis of Facebook and Twitter across six countries*. Information, Communication & Society. Vol. 20. n.º 9 (2017).

<sup>238</sup> DAHLBERG et. al., *Introduction: Tracing Radical...*, p. 1.

<sup>239</sup> RAWLS - *The Idea of Public Reason Revisited*, p. 773.

direcionamento e os *dark ads* são contrários aos princípios estruturais da esfera pública, uma vez que os cidadãos que não recebem as mensagens ficam excluídos do processo comunicativo, impossibilitados de as criticar ou de propor visões alternativas. Para VILMER et. al., «*por vezes a manipulação informativa transforma uma convicção passiva numa convicção ativa – de forma similar ao processo de radicalização. O ato em questão pode ser um voto.*»<sup>240</sup>.

De outro ângulo, os perigos assinalados impactam negativamente os direitos fundamentais dos cidadãos, desde logo afetando a própria dignidade do ser humano (art.º 1.º CDFUE) nas suas várias projeções, tais como a autonomia e a não instrumentalização da pessoa, a privacidade (art.º 7.º CDFUE) e a proteção dos dados pessoais (art.º 8.º CDFUE) e a liberdade de expressão e informação (art.º 11.º CDFUE) em sociedades pluralistas. Focando-nos na liberdade de expressão e informação, importa referir que esta é recebida no DUE com o mesmo alcance e sentido ao correspondente direito garantido pela CEDH (*ex vi*, art.º 52.º, n.º 3 CDFUE). Nos termos do n.º 2 do art.º 10.º da CEDH, a liberdade de expressão implica «*deveres e responsabilidades*», pelo que pode ser restringida, condicionada ou sancionada quando esteja em causa, no âmbito de uma sociedade democrática, entre outros, a segurança nacional, a segurança pública, a defesa da ordem e a prevenção do crime, a proteção da honra ou dos direitos de outrem ou a confidencialidade da informação. Fora estes casos, a liberdade de expressão não pode ser restringida, o que desde logo significa que a desinformação, a mentira e as técnicas agressivas de persuasão e manipulação estão protegidas pela liberdade de expressão, a menos que sejam difamatórios ou que de outro modo violem uma disposição legal. Ora, a liberdade de expressão e de informação é necessária ao exercício de outros direitos e liberdades fundamentais, logo à cabeça o direito ao voto e à participação política. Conforme o TEDH já enfatizou na sua jurisprudência, não é possível haver democracia sem pluralismo, sendo por isso que a proteção conferida pelo art.º 10.º da CEDH é referente não apenas a informação ou as ideias que são recebidas favoravelmente ou consideradas inofensivas ou indiferentes, mas também as afirmações e ideias que ofendam, choquem ou perturbem<sup>241</sup>. Aliás, é «*da própria essência da democracia permitir que diversos programas políticos sejam propostos e debatidos, mesmo aqueles que coloquem em causa a forma como Estado é correntemente organizado, desde que eles não prejudiquem a democracia em si mesma*»<sup>242</sup>. Do mesmo modo, o TEDH reconhece também que a *internet* fornece uma plataforma sem precedentes para o exercício da liberdade de expressão<sup>243</sup>. No entanto, salienta que os riscos da

<sup>240</sup> VILMER et. al., *Information manipulation*, p. 25.

<sup>241</sup> Cfr., *inter alia*, caso *Partido Socialista e outros v. Turquia* (20/1997/804/1007), par. 41.

<sup>242</sup> Caso *Manole e outros v. Moldávia* (13936/02), 17/12/2009, par. 95 e 96.

<sup>243</sup> *Delfi AS v. Estonia* [GC], no. [64569/09](#), § 110, ECHR 2015

violação dos direitos e das liberdades consagradas na Convenção são maiores no contexto digital<sup>244</sup>. Realmente, a digitalização permite uma certa brutalização e canibalização do discurso público *online*, podendo representar a banalização da manipulação como mecanismo de radicalização da opinião pública e de atropelos à liberdade de expressão. Perante a multiplicação quer da desinformação, quer dos conteúdos ilegais *online*, um dos riscos mais salientes é a possibilidade de os Estados, adotando medidas mais militantes, coartarem e violarem, em nome da democracia e do pluralismo, as liberdades jusfundamentais dos seus cidadãos em transgressão dos seus próprios valores democráticos, o que levará a novas divisões sociais e ao enfraquecimento generalizado do Estado de Direito democrático<sup>245</sup>. Assim, e paradoxalmente, se o Estado decidir intervir pela via legislativa, proibindo, por exemplo, as plataformas digitais de albergarem conteúdos desinformativos ou obrigando-as à partilha dos dados pessoais dos autores desses conteúdos ou, ainda, bloquearem o acesso a determinados *websites* onde são partilhados vários conteúdos, podemos assistir à supressão, ou pelo menos ao escrutínio, de liberdades e direitos fundamentais sem respeito pelo princípio da proporcionalidade. Do mesmo molde, os critérios, regras e processos que as plataformas digitais adotam para eliminar ou bloquear os conteúdos que são contrários os termos e condições dos seus serviços, podem, sob pressão dos Estados e da sociedade na sequência de campanhas de desinformação, manipulação ou cibercriminais, ser endurecidos, traduzindo-se em violações da liberdade de expressão, o que já acontece amiúde no quadro de políticas pouco transparentes, arbitrárias ou demasiado complexas que não garantem aos utilizadores mecanismos de reação. Se é amplamente aceite que numa democracia saudável é necessário que os cidadãos sejam expostos a opiniões diversas, o que, no contexto das plataformas digitais, até tem efeitos positivos, nomeadamente para a moderação do discurso político<sup>246</sup>, é também preciso garantir que as várias ideias e propostas em competição na esfera pública tenham (idealmente) oportunidades semelhantes de ser expressas e criticadas, procurando-se evitar que uma ideia possa ser artificialmente amplificada a ponto de se tornar dominante (pelo menos *online*), caso que é a própria diversidade do ambiente mediático que é posta em causa e, isso sim, pode conduzir à violação da liberdade de expressão e informação, principalmente na sua vertente do direito a receber informação num quadro pluralista. A realidade é que, tal como colocado por HANNAH ARENDT, «a liberdade de opinião é uma farsa se a informação sobre os factos não estiver garantida e se não forem os próprios factos o objeto do debate»<sup>247</sup>, o que significa que

---

<sup>244</sup> *Ibid*, § 133.

<sup>245</sup> VILMER et. al., *Information Manipulation*, p. 25.

<sup>246</sup> MARTENS, et. al., *The digital transformation of news media...*, p. 27.

<sup>247</sup> ARENDT, *Entre o Passado e o Futuro*, p. 248.

a desinformação e a manipulação, ainda que protegida, enfraquece a liberdade de expressão, chegando-se, por esta via, ao paradoxo do pluralismo e da liberdade de expressão ilustrado por KARL POPPER: a informação falsa em si mesma e as ideias, propostas e projetos antidemocráticos gozam, em princípio, da proteção oferecida pela liberdade de expressão e informação. Mas quando o ambiente discursivo na esfera pública é não só ocupado, mas dominado, pela mentira, manipulação, distorção ou pelo populismo é o próprio propósito primário da liberdade de expressão e de informação que sai frustrado. Nestes termos, atualmente, o maior risco para a democracia é que através dos processos que fomos descrevendo, o poder seja (ainda que através de eleições) capturado por forças pouco empenhadas na defesa da democracia, do Estado de Direito e dos direitos fundamentais, o que pode significar [i.] o enfraquecimento ou violação dos princípios associados ao Estado de Direito, [ii.] uma violação dos direitos fundamentais dos cidadãos e/ou [iii.] uma deriva do regime vigente que se afasta do modelo da democracia liberal. Tendo em conta a interdependência que se estabelece entre democracia, Estado de Direito e direitos fundamentais, qualquer interferência no processo ou princípio democrático ou qualquer violação dos direitos fundamentais resulta no declínio automático dos restantes pilares.

## **PARTE II – AS OPORTUNIDADES DA «CONSTELAÇÃO DIGITAL» PARA A CONSTITUCIONALIZAÇÃO DA UNIÃO EUROPEIA.**

### **CAPÍTULO I – DOS RISCOS ÀS OPORTUNIDADES: OS RISCOS COMO IMPULSIONADORES DO «MOMENTO COSMOPOLITA» PARA AGIR.**

#### **Secção I – Conceptualizar a «constelação digital».**

Explica BECK que o *«risco constitui uma figura de reflexão, uma vez que pondera o proveito e o prejuízo, permitindo tomar, no presente, decisões relativas ao futuro»*<sup>248</sup>. Segundo o Autor, quando o risco é percebido como omnipresente nas sociedades, existem três reações possíveis: a negação, a apatia ou a transformação, dando esta última origem ao chamado *«“momento cosmopolita” da sociedade de risco mundial»*<sup>249</sup>. Os perigos levam à ação e ao recomeço,

<sup>248</sup> BECK, *A Sociedade de risco mundial...*, p. 49.

<sup>249</sup> *Ibid.*, p. 100. O cosmopolitismo deve ser aqui entendido como corrente que, nascendo da teoria do risco, nota que *«todos vivemos numa vizinhança direta com todos, portanto num mundo com outros que não podem ser excluídos»*, pelo que advoga uma obrigação cultural de inclusão do culturalmente outro, que se aplica a todos em todo o mundo, e que se distingue da exclusão hierárquica, do universalismo (que afirma a dissolução das diferenças), do nacionalismo (que unifica, ao mesmo tempo que delimita as diferenças através de contrastes nacionais) ou do multiculturalismo (entendido como monoculturalismo plural). Assim, para os cosmopolitas interessa sobretudo o reconhecimento da alteridade cultural, sem classificação hierárquica nem eliminação das diferenças, as quais são aceites como tal e até consideradas como positivas.

podendo, numa ambivalência já notada, surgir enquanto oportunidades de mudança. A reflexão em torno dos “riscos digitais mundiais” leva-nos, desde logo, a concluir pela sua dimensão essencialmente global ou transnacional, uma vez que eles «*não respeitam fronteiras nacionais*»<sup>250</sup>. A “revolução digital”, nas contrariedades próprias que lhe são inerentes, fez emergir novos perigos e riscos mundiais: ciberataques contra infraestruturas críticas dos Estados, contra governos e organizações privadas, e até contra hospitais e sistemas militares; dispersão do discurso de ódio e radical com incitamentos à violação; aproveitamento das ferramentas *online* por organizações terroristas; campanhas de desinformação e manipulação que minam a confiança no Estado de Direito e colocam em causa a legitimidade dos processos democráticos; a automação e datificação, que conduzem à vigilância em massa quer por parte de governos, quer pelas grandes empresas tecnológicas, em violação da privacidade e dos dados pessoais dos cidadãos de várias nações; a ciberespionagem e outras formas de cibercriminalidade usadas no contexto de “guerra híbrida” ou de interferência noutros Estados. A natureza destas atividades, permite que elas sejam conduzidas por uma multitude de agentes a partir de qualquer lugar e a qualquer momento, permanecendo por resolver, em muitos casos, o problema da atribuição da responsabilidade e da sua efetivação. De outro modo, os efeitos ou externalidades associadas aos riscos que daí decorrem podem fazer-se sentir mundialmente, ao passo que nenhum Estado consegue, isoladamente, tomar medidas suficientemente eficazes para erradicar ou limitar os riscos e perigos identificados. Assim, ao serem em grande parte incontrolláveis a partir dos esquemas do Estado-Nação, os riscos digitais tornam as fronteiras mais porosas, obrigando a repensar conceitos como a soberania enquanto poder supremo na ordem interna e alertando para a interdependência existente à escala global que a todos aproxima numa espécie de «*vizinhança globalizada*» criada graças às «*diferentes vulnerabilidades nas diferentes regiões do mundo*»<sup>251</sup>.

Ao concretizar as consequências da globalização, que define enquanto processo caracterizado pela quantidade e intensidade das relações de troca, de comunicação e de trânsito para além das fronteiras nacionais, HABERMAS deixa claro que «*as funções do Estado Social só poderão continuar a ser levadas a cabo no mesmo nível se elas forem transferidas do Estado-Nação para entidades políticas mais latas que assumam de algum modo uma economia transnacional*»<sup>252</sup>, isto porque o processo de tomada de decisão de cada Estado é por natureza limitado ao espaço geográfico onde a sua ordem geográfica goza de validade, ao passo que os

<sup>250</sup> HABERMAS, Jürgen – *The Postnational Constellation: political essays*. Massachusetts: The MIT Press, 2001. p. 68.

<sup>251</sup> PERNICE, *Risk management in the digital constellation...*, p. 87.

<sup>252</sup> HABERMAS, *The Postnational Constellation...*, p. 52.

desafios e efeitos secundários colocados pelo fenómeno da globalização só podem ser mitigados através de respostas comuns, quer sob a forma de cooperação entre Estados, quer através da constituição ou do reforço dos poderes de organizações transnacionais ou internacionais. Neste âmbito, e HABERMAS cunha o termo “*constelação pós-nacional*” para descrever as circunstâncias em que o Estado-Nação é, fruto de fenómenos que estão *para além* do seu controlo, obrigado a abrir a sua democracia a formas de governança internacional<sup>253</sup>. Assim, «*temos de admitir como irreversível a dependência crescente dos Estados nacionais dos constrangimentos sistémicos de uma sociedade mundial cada vez mais interdependente*»<sup>254</sup>. Segundo o Autor, e perante uma margem de manobra cada vez mais limitada dos Estados<sup>255</sup>, impõe-se, no âmbito de uma *constelação pós-nacional*, a abertura das capacidades políticas de atuar além das fronteiras nacionais, o que em última análise «*resulta do próprio sentido normativo da democracia*»<sup>256</sup>. E não basta sequer que se tente compensar a perda de capacidade de ação com a ajuda de organizações internacionais, sendo antes necessária, por uma questão de legitimação democrática, que se centre nos cidadãos – e não nos Estados – uma «*constitucionalização do direito internacional*» para responder aos «*constrangimentos sistémicos de uma sociedade globalizada*» no quadro de uma democracia e de uma comunidade cosmopolita global, composta pelos «*cidadãos do mundo*», que não corresponderia a uma «*república mundial, mas sim a uma associação supraestatal de cidadãos e povos de Estados, de tal modo que os Estados-Membros preservariam a disposição – ainda que não o direito à livre disposição – sobre os meios de recurso legítimo à violência*»<sup>257</sup>. A representação dos *cidadãos do mundo* e dos Estados teria lugar numa assembleia geral (um «*Parlamento mundial*») quer permitiria que, simultaneamente, as perspetivas concorrentes acerca do bem comum global dos *cidadãos do mundo* e dos cidadãos dos Estados fossem tidas em conta. A esse Parlamento mundial competiria, além da garantia da concretização dos direitos fundamentais dos *cidadãos do mundo*, a elaboração de uma base normativa transnacional que regulasse e impusesse restrições comuns quanto aos assuntos mais relevantes da política interna mundial<sup>258</sup>, o que necessariamente incluiria a resposta aos riscos digitais mundiais.

INGOLF PERNICE, partindo da conceção da democracia cosmopolita, e caracterizando também os novos riscos digitais como ameaças transnacionais independentes de fronteiras e distâncias

---

<sup>253</sup> *Ibid*, p. 84.

<sup>254</sup> HABERMAS, Jürgen - *Um ensaio sobre a constituição da Europa*. Lisboa: Edições 70, 2012. p. 77.

<sup>255</sup> Há também quem se refira ao fenómeno da desterritorialização do poder, descrevendo aquela circunstância de o voto exercido numa certa circunscrição deixar de ser eficaz. SILVEIRA, et. al., *Do mercado interno...*, p. 14.

<sup>256</sup> *Ibid*, p. 76.

<sup>257</sup> *Ibid*, pp. 119. e ss.

<sup>258</sup> *Ibid*, pp. 121 e ss.

geográficas<sup>259</sup>, defende que a «*revolução digital e a internet permitem-nos pensar além dos limites daquilo que, tradicionalmente, constitui a presente ordem mundial, tendo em vista a constitucionalização democrática do fragmentado sistema de direito internacional e de governança global*»<sup>260</sup>. Realmente, é relativamente pacífico que os Estados nacionais não dispõem das capacidades necessárias para responder, por si, aos problemas criados pelos riscos digitais; de facto, as ferramentas constitucionais e legais vigentes no quadro nacional partem ainda de uma conceção tradicional da soberania, pelo que quando se deparam com fenómenos transnacionais, de origem obscura ou que ultrapassam as barreiras territoriais do Estado, quedam-se pelas proclamações mais ou menos vazias ou pela impotência em atuar que obriga a uma permanente corrida atrás do prejuízo. Todavia, e como referido, essa fragilidade do Estado nacional face a acontecimentos que o ultrapassam é também uma oportunidade para repensar as bases da governança global, a qual deve necessariamente incluir as tecnologias digitais. Face à contradição aparente que aqui se gera, visto que vimos expondo as deficiências de funcionamento que tornam o digital um risco para a democracia e o Estado de Direito, convém explicar que esse risco existe principalmente graças à incapacidade de se encontrar uma resposta global efetiva que ultrapasse quer o nível nacional, quer o nível supranacional. Ora, se essa resposta for encontrada, partindo de propostas como a de PERNICE, que *infra* desenvolveremos, e se for possível encontrar uma governança comum para o digital, que tenha como prioridade e fim efetivo a proteção dos indivíduos, das organizações e dos Estados, nada impede que a digitalização seja usada em prol de um reforço global da democracia, dos direitos humanos e do Estado de Direito. Alcançando-se esse estágio, a Era Digital emerge como uma *oportunidade* que deve ser aproveitada em todas as suas potencialidades. No entanto, enquanto essa concertação não for possível, sobretudo por razões de ordem política, então as ferramentas digitais devem ser encaradas com todas as cautelas, uma vez que muito facilmente podem ser usadas contra os cidadãos e os Estados, que permanecem sem capacidade de resposta adequada. Ao refletir os riscos na Era Digital, PERNICE vai um passo mais além que aquele que já havia sido dado por HABERMAS e introduz o conceito de «*constelação digital*», para expressar a ideia de que a digitalização, que é já um processo sem retorno, está a criar simultaneamente perigos e oportunidades e novos conceitos de governança que podem ser particularmente relevantes para a gestão do risco digital<sup>261</sup>. Quando concetualiza a *constelação digital*, PERNICE nota que existem essencialmente três grandes mudanças em relação à concetualização da *constelação*

<sup>259</sup> PERNICE, *Risk management in the digital constellation...I*, p. 85.

<sup>260</sup> PERNICE, Ingolf - *Global cybersecurity governance: A constitutionalist analysis*. Global Constitutionalism. Vol. 7. n.º 1 (2018). p. 113.

<sup>261</sup> PERNICE, *Risk management in the digital constellation...I*, p. 85.

*pós-nacional*<sup>262</sup>: (1) uma nova densidade comunicativa da sociedade global, (2) associada a novas oportunidades para os processos democráticos, que poderão permitir (3) o desenvolvimento de respostas globais para os novos riscos da digitalização. Essa nova densidade comunicativa traduz-se, essencialmente, na crescente proximidade existencial entre os membros da “aldeia global”, permitida pelos processos de globalização cultural que esbatem os particularismos locais e dão uma “voz ativa” aos cidadãos relativamente a problemas e assuntos que afetam pessoas de outros espaços no globo. Essa proximidade permite, na ótica do Autor, aprofundar, através das tecnologias, a esfera pública global, condição essencial para uma «nova democracia aberta e deliberativa também à escala global»<sup>263</sup>. As tecnologias digitais entram aqui em jogo ao permitirem um processo continuado, em tempo real e sem fronteiras de comunicação, o acesso ao conhecimento e à informação, o debate e a deliberação. Deste modo, «o termo “constelação digital” corresponde à sociedade digital, que, tal como a sociedade de risco, é também global. O conceito reflete um nível de relações sociais e comunicativas entre os indivíduos que é comparável àquelas relações nos níveis local, nacional e supranacional da sociedade, embora esse novo nível seja ainda mais informal. Os seus potenciais, contudo, incluem a formação de uma vontade política global [...] como parte fundamental de uma ordem global capaz de responder aos desafios globais através de regras e conceitos estabelecidos democraticamente. Entre esses desafios estão os novos riscos que necessitam de ser geridos a todos os níveis, incluindo globalmente»<sup>264</sup>. A proposta de PERNICE para a gestão dos novos riscos digitais num contexto global é a do “constitucionalismo global multinível”, visto que este garantiria uma capacidade de resposta adequada em todos os níveis de ação, desde o local ao mundial<sup>265</sup>. A gestão do risco, a ser assumida através desta estrutura multinível, envolveria os indivíduos, as empresas, a sociedade civil e as autoridades públicas a todos os níveis<sup>266</sup> e permitiria a criação de um sistema deliberativo global democraticamente legitimado associado a um esquema de regulação vinculativa quer para os Estados quer diretamente para os indivíduos e organizações, com regras para a sua execução, controlo judicial e proteção efetiva dos direitos fundamentais, tudo em respeito pelo princípio do Estado de Direito. Este modelo não corresponderia nem a um governo nem a um Estado mundial, mas antes a um nível adicional de coordenação e governança sem governo, centrado nos indivíduos enquanto fonte de soberania, os quais atribuem poderes a instituições nos respetivos níveis de

---

<sup>262</sup> *Ibid*, p. 89.

<sup>263</sup> *Ibid*, p. 90.

<sup>264</sup> *Ibid*.

<sup>265</sup> PERNICE, Ingolf - *Risk management in the digital constellation - a constitutional perspective (part II)*. Revista D'Internet, Dret i Política. n.º 27 (2018). p. 81.

<sup>266</sup> *Ibid*, p. 82.

ação política que os partilham e integram com outras instituições situadas noutros níveis, sempre com base no princípio da atribuição e da subsidiariedade, atuando todos os níveis num sistema de camadas entrelaçadas e interconectadas limitadas pelo Estado de Direito<sup>267</sup>. Note-se que governo e governança não se confundem, correspondendo a última, a nível global, «*ao exercício de autoridade além das fronteiras nacionais, bem como às normas e regras consensualizadas fora do Estado-nação, umas e outras justificadas com a referência a bens comuns e a problemas transnacionais*», através do envolvimento de uma pluralidade de atores sob várias formas (governo global, governança global com governos (v.g. ONU) e governança global sem governos)<sup>268</sup>. Para ilustrar o modo de funcionamento deste constitucionalismo global multinível, que entronca no campo mais lato do constitucionalismo ou democracia cosmopolita, que, reconhecendo o carácter «*complexo e interconectado do nosso mundo*», defende uma «*divisão de poderes e competências entre diferentes níveis de interação política*», ligados vertical e horizontalmente<sup>269</sup>, podemos usar o caso da cibersegurança. Relativamente à cibersegurança, a resposta mais comum dos Estados é o apelo ao reforço da soberania digital<sup>270</sup>. Este apelo, se até pode fazer algum sentido no que toca à dependência do fornecimento de equipamentos e infraestruturas digitais, não é uma solução viável, pelo menos enquanto se defender uma *internet* aberta, isto porque, «*não há nada que esteja mais longe das conceções tradicionais da soberania estadual que a internet*»<sup>271</sup>, a qual não é controlada nem pelos indivíduos, nem pelos Estados, nem mesmo pela comunidade internacional<sup>272</sup>. Num contexto

<sup>267</sup> *Ibid*, p. 86.

<sup>268</sup> ZÜRN, Michael - *A Theory of Global Governance: Authority, Legitimacy and Contestation*. Oxford: Oxford University Press, 2018. p. 3.

<sup>269</sup> HELD, David - *Globalization and cosmopolitan democracy*. Peace Review. Vol. 9. n.º 3 (1997). p. 310 e ss.

<sup>270</sup> E soberania aqui entendida de acordo com a noção tradicional de autoridade política suprema sobre um certo território. Cfr. BAUER et. al., *Europe's Quest for Technological...*, p. 5.

<sup>271</sup> PERNICE, *Global cybersecurity governance...*, p. 114.

<sup>272</sup> A governança da *internet* não pertence a nenhum ator específico, antes se encontrando globalmente distribuída por uma rede de organizações que provêm do setor privado, da sociedade civil, da academia, dos Estados e de organizações internacionais. Por exemplo, o sistema de nomes de domínio (*DNS*), essencial ao funcionamento da *internet*, é gerido pela ICANN (*International Corporation for Assigned Names and Numbers*), que corresponde a uma organização privada sem fins lucrativos que coordena a alocação e atribuição dos identificadores únicos da *internet*, como os IP's, funcionando num modelo descentralizado e aberto mundialmente aceite. Até 2016 a ICANN era "superentendida" pelo governo federal dos EUA, data em que entidade passou totalmente para o setor privado. A elaboração de *standards* para a *internet* está a cargo da IETF (*Internet Engineering Task Force*) e, num âmbito mais genérico, da ISO (*International Organization for Standardization*). A primeira é formada por voluntários, estando sob o auspício da *Sociedade da Internet*, uma organização sem fins lucrativos que se dedica à promoção do desenvolvimento da *internet* para todos. A ISO é também uma organização não-governamental e sem fins lucrativos. A ONU, partindo da Cimeira Mundial sobre a Sociedade de Informação de 2005, decidiu constituir o Fórum de Governança da Internet (IGF) que serve de plataforma de diálogo para que os vários *stakeholders* discutam aspetos sobre a governança da *internet*, mas sem a emissão de quaisquer orientações vinculativas. Entretanto, em 2014, teve também lugar o fórum NETmundial, no Brasil, que reuniu os vários interessados na discussão do futuro da *internet* e que produziu uma declaração não-vinculativa sobre os princípios de governança da *internet*, de onde se destaca o respeito *online* dos direitos humanos como a liberdade de expressão e de informação, de associação e reunião e a privacidade.

de *internet* aberta e sem fronteiras, as medidas legislativas adotadas a nível nacional são sempre insuficientes contra os ciberataques, sempre a evoluir em sofisticação e repercussões. Em substituição de abordagens nacionais ou até regionais (como é o caso da UE), o constitucionalismo multinível, ancorado num constitucionalismo global e numa democracia cosmopolita, pode ser a resposta para uma regulação global em assuntos de cibersegurança<sup>273</sup>. Essa resposta começaria ao nível mais básico do indivíduo, traduzindo-se aí em autoproteção, resiliência (que neste contexto significa robustez, flexibilidade e adaptação) e participação nos processos políticos a todos os níveis. Ao nível das empresas, as palavras de ordem são produtos seguros, sistemas de alerta, *standards* comuns de segurança e engenharia de segurança, tudo na base da autorregulação com o estabelecimento de códigos de conduta globalmente aplicáveis. Às autoridades públicas, quer sejam internacionais, supranacionais ou nacionais cabe a proteção dos direitos fundamentais e a promoção das melhores práticas, a aprovação de legislação e a constituição de agências para a cibersegurança, ciberinteligência, cooperação intergovernamental e cooperação dentro das organizações internacionais, sem esquecer a adoção de tratados internacionais. Do ponto de vista normativo e deliberativo, e porque se procura uma legitimação da ação coordenada aos vários níveis, o corpo fundamental de deliberação, que agregaria todos os *stakeholders*, seria o Fórum de Governança da Internet (IGF), onde seriam discutidos os assuntos centrais relativos à governança da *internet*, incluindo a cibersegurança. Ao IGF somar-se-iam fóruns regionais e nacionais. A necessidade de estabelecer princípios relativos a vários aspetos de cibersegurança seria satisfeita por um fórum que envolvesse os vários níveis, princípios esses depois sancionado pelo IGF. Com base nos princípios alcançados, elaborar-se-iam, ao nível da ONU, convenções internacionais que estabeleceriam obrigações concretas para os Estados, cujo cumprimento seria assegurado por organismos especiais a funcionar no seio da ONU, sempre com garantias processuais e possibilidade de controlo judicial.

## **Secção II – O mundo em rede necessita de respostas em rede: a gestão do risco digital na União Europeia.**

A União Europeia é, se assim se pode dizer, um laboratório ou estudo de caso no que diz respeito ao constitucionalismo e governança multinível e em rede. De facto, a UE tem procurado desenvolver soluções de gestão do risco digital baseadas em respostas verticais e horizontais implementadas ao nível das instituições e dos EM. Apesar de não existir, ainda,

---

<sup>273</sup> A proposta é de PERNICE, *Global cybersecurity governance*, p. 122 e ss.

uma política transversal, partilhada e compreensiva no que toca à gestão do risco digital, antes prevalecendo um conjunto de medidas setoriais algo dispersas, a verdade é que podemos encontrar na União vários exemplos que, ou são já a concretização dessa governança multinível e em rede, ou servem de inspiração quando pensamos nas *possibilidades e oportunidades* que os riscos digitais colocam à forma como pensamos a resposta a problemas globais.

Sem pretensões de exaustão, e apontando aqui apenas alguns exemplos significativos, a resposta da UE ao perigo da desinformação foi-se desenvolvendo em proporção à gravidade do problema. Em 2015, as preocupações estavam sobretudo centradas nas campanhas de desinformação promovidas pela Federação Russa no contexto do conflito com a Ucrânia<sup>274</sup>, o que veio a dar origem à criação da *East StratCom Task Force* com o objetivo de desenhar uma estratégia de comunicação e promoção das políticas da UE junto dos países do Leste Europeu vizinhos da UE, no âmbito da política de ação externa cuja finalidade é, entre outras, a consolidação e o apoio à democracia, ao Estado de Direito e aos direitos humanos (cfr. al. d) do n.º 2 do art.º 21.º TUE). Em 2018, o enfoque desloca-se para o interior da própria União, na sequência, *inter alia*, do referendo sobre a permanência do Reino Unido na UE, das eleições francesas e alemãs, da atuação do governo húngaro, da deriva política em Itália e do referendo pela independência na Catalunha<sup>275</sup>. À boleia das eleições para o Parlamento Europeu de 2019, matéria em que, além da «*dimensão europeia óbvia*»<sup>276</sup>, a UE dispõe de competências, ora não se tratasse das eleições para uma das suas instituições, muito embora a operacionalização do processo eleitoral caiba aos EM<sup>277</sup>, a Comissão propôs, no ano anterior, uma “estratégia europeia” para combater a desinformação em linha<sup>278</sup>, reconhecendo expressamente a dimensão transnacional do problema e a incapacidade dos Estados para, por si só, mitigar o fenómeno,

<sup>274</sup> Cfr. CONSELHO EUROPEU – *Reunião do Conselho Europeu (19 a 20 de março de 2015) – Conclusões*. EUCO 11/15. Bruxelas, 20.03.2015, p. 5.

<sup>275</sup> Apesar de estes eventos terem sido marcados por processos desinformativos, é com extrema cautela que devemos olhar a existência – ou não – de um nexo de causalidade entre a distribuição e amplificação da desinformação e as perceções, crenças, ideologias e comportamentos resultantes do consumo destes conteúdos. O impacto da desinformação nas opiniões políticas e no comportamento dos votantes não está científica e definitivamente provado, uma vez que as análises que vão sendo desenvolvidas sofrem várias limitações. Apesar das limitações apontadas, é possível medir e até quantificar o impacto da desinformação no ambiente e esfera pública digital, daí se extraindo consequências para a Democracia e o Estado de Direito. Cfr. BAYER et., al., *Disinformation and propaganda...*, p. 9; VILMER et. al., *Information Manipulation*, p. 24.

<sup>276</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Garantir eleições europeias livres e justas*. COM(2018) 637 final. Bruxelas, 12.9.2018.

<sup>277</sup> Vide a Decisão (UE, Euratom) 2018/994 do Conselho, de 13.07.2018, que altera o Ato relativo à eleição dos membros do PE por sufrágio universal direto, anexo à Decisão 76/787/CECA, CEE, Euratom do Conselho de 20.09.1976.

<sup>278</sup> COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Combater a desinformação em linha: uma estratégia europeia*. COM(2018) 236 final. Bruxelas, 26.4.2018.

pelo que, em respeito pelo princípio da subsidiariedade (n.º 3 do art.º 5.º do TUE), e porque em causa estão os próprios valores fundacionais da UE (art.º 2.º TUE), o respeito devido à CDFUE e à CEDH (art.º 6.º TUE e 51.º CDFUE), e a própria integridade e qualidade do espaço de liberdade, segurança e justiça (n.º 2 do art.º 3.º TUE e n.º 2 do art.º 67.º TFUE), torna-se necessário adotar «*uma abordagem europeia, a fim de garantir uma ação eficaz e coordenada e proteger a UE, os seus cidadãos, as suas políticas e as suas instituições*»<sup>279</sup>, principalmente num quadro em que, acrescentamos nós, a própria UE e a sua integridade é alvo preferencial das campanhas de desinformação e manipulação, muitas vezes com origens externas.

A pedra angular dessa estratégia foi a elaboração de um código de conduta que funcionaria como mecanismo de autorregulação das plataformas digitais a ser subscrito por estas numa base voluntária. A conclusão do Código de Conduta da UE sobre a Desinformação foi apoiada pela Comissão no âmbito de um fórum multilateral sobre a desinformação realizado em setembro de 2018 e que reuniu os principais *stakeholders*, entre representantes das plataformas digitais, dos meios tradicionais de imprensa, de verificadores de factos, de membros da academia e da sociedade civil. A esta data, o Código foi já subscrito por várias empresas tecnológicas e associações comerciais, designadamente a Google, o Facebook, o Twitter, a Mozilla, a Microsoft (em maio de 2019) e o TikTok (em junho de 2020)<sup>280</sup>, mas apenas quando prestem serviços no Espaço Económico Europeu. A elaboração e subscrição deste instrumento é um exemplo possível de uma gestão do risco digital multinível, assente num compromisso entre um nível superior e transnacional de legitimação política (a UE), em representação das suas instituições, dos EM e dos cidadãos da União, e o setor privado, responsável primário pela gestão das plataformas onde a desinformação é difundida. Em termos de objetivos, o Código de Conduta divide-se em cinco pilares essenciais: (1) controlo da colocação de anúncios; (2) no que respeita à propaganda política e publicidade temática, as *big tech* comprometem-se a aumentar o grau de transparência, distinguindo claramente todos os anúncios publicitários de conteúdos de outro tipo, além da divulgação pública da propaganda política, incluindo a identidade do patrocinador e o montante despendido; (3) para assegurar a integridade dos serviços, os signatários comprometeram-se a adotar políticas claras no que diz respeito à identidade e utilização de robôs automáticos, sem nunca serem proibidos de autorizar a utilização de contas e serviços anónimos ou pseudonimizados (aliás, em respeito pelo art.º 8.º da CEDH); (4) a capacitação dos utilizadores, que deve ser prioritária em relação à supressão

<sup>279</sup> *Ibid.*, p. 3.

<sup>280</sup> Vide <https://ec.europa.eu/digital-single-market/en/news/roadmaps-implement-code-practice-disinformation>.

ou bloqueio de conteúdos lícitos, ainda que falsos<sup>281</sup>, e que se consegue através de produtos, tecnologias e programas que ajudem os utilizadores a reconhecer informações potencialmente falsas, nomeadamente através de indicadores de fiabilidade<sup>282</sup>, e, também, através de tecnologias que deem prioridade a informações fidedignas nos *feeds* das redes sociais<sup>283</sup> e de sistemas que facilitem a localização de perspetivas diversas sobre temas de interesse público, além de desenvolver mecanismos que permitam que os utilizadores compreendam porque razão estão a ser alvo de determinado anúncio de propaganda política ou publicidade temática; (5) capacitação da comunidade de investigação e apoio às comunidades independentes de verificadores de factos. Apesar da importância simbólica, o Código de Conduta não estabelece uma abordagem comum para todos os signatários (que podem optar livremente pelos compromissos que pretendem subscrever), além de não prever nenhum compromisso significativo ou objetivo por parte das plataformas digitais, que se limitam a envidar “esforços comercialmente razoáveis”, o que acaba por resultar na impossibilidade de medir objetivamente os progressos alcançados, cujo único reflexo se traduz num relatório anual elaborado pelas plataformas. Os representantes dos *media*, da sociedade civil, dos verificadores de factos e da academia presentes no fórum multilateral sobre a desinformação afirmaram que o documento

<sup>281</sup> Nesta senda, os signatários do Código de Conduta recusam qualquer obrigação legal ou política de caráter voluntário que os obrigue a impedir o acesso a conteúdos lícitos «*apenas por se julgar que são “falsos”*». Apesar de se concordar com a abordagem, uma vez que também nós concordamos que a desinformação, quando não caia em nenhuma categoria de ilicitude, está protegida pela liberdade de expressão, a expressão utilizada («*por se julgar que são “falsos”*») revela que as plataformas também aderem ao relativismo que confunde factos com opiniões.

<sup>282</sup> A utilização destes mecanismos tem levado a fortes críticas contra as plataformas digitais, essencialmente acusadas de interferência em eleições e de violação da liberdade de expressão dos seus utilizadores. É o caso do Twitter que em maio de 2020 colocou uma “etiqueta” num dos *tweets* do atual presidente norte-americano que sugeria aos utilizadores que “verificassem os factos” relativo àquele assunto, direcionando-os para uma página de verificação de factos. Entretanto, o CEO do Facebook também se juntou às críticas ao Twitter, referindo que o as redes sociais «*não devem ser árbitros da verdade*» online. Independentemente da interessante discussão que se possa ter acerca da atuação das plataformas sociais neste contexto, e que além das preocupações de interferência na esfera pública, podem também ter repercussões na esfera de responsabilidade das plataformas (uma vez que ao etiquetar uma notícia de acordo com a sua fiabilidade, as plataformas estão já a atuar enquanto editores de conteúdo e não como meros intermediários), a questão mais relevante parece estar do lado da eficácia destas medidas, uma vez que há estudos que apontam para o chamado “*backfire effect*” em que, quando expostos a factos que desacreditam uma notícia falsa, os indivíduos ainda ficam mais convencidos da sua veracidade – vide NYAN, Brendan; REIFLER, Jason - *When Corrections Fail: The Persistence of Political Misperceptions*. Polit Behav. Vol. 32. n.º 2 (2010). No sentido de esse efeito não ser prevalente, Cfr, WOOD, Thomas; PORTER, Ethan - *The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence*. Polit Behav. Vol. 41. (2018).

<sup>283</sup> Para que fique claro, com isto pretende-se uma reversão do algoritmo, que em vez de destacar a desinformação, classifica-a mais abaixo no *feed* de notícias, em benefício de informações que a plataforma reputa por autênticas. Temos as maiores reservas quanto a esta opção, a qual bem pode resultar num “mal inverso”, isto se se mantiver a opacidade no funcionamento dos algoritmos e se não forem conhecidos claramente os critérios e instrumentos usados pelas plataformas para aferir da veracidade e autenticidade de um conteúdo. De notar, que o Facebook não remove da plataforma conteúdos desinformativos, antes reduz «*significativamente a sua distribuição*», apresentando-os «*mais abaixo no Feed de Notícias*», o que demonstra que a rede, apesar de não se posicionar enquanto “árbitro da verdade”, posiciona-se, pelo menos, enquanto árbitro da visibilidade. Atendendo aos vieses de que podem sofrer os algoritmos, resta saber se, inadvertidamente, e a coberto de se tratar de categorias próximas da desinformação, não acabarão por ser cometidos atropelos à liberdade de expressão e de informação.

elaborado «*não é, de modo algum, autorregulatório, pelo que as Plataformas, apesar dos seus esforços, não criaram um Código de Conduta*»<sup>284</sup>, uma vez que lhe faltam pressupostos essenciais como auto-mecanismos de monitorização, cumprimento e imposição. Apesar de bem-intencionado, o Código de Conduta acaba por padecer das limitações resultantes da ausência de uma governança multinível global com uma legitimidade forte para conseguir vincular e obrigar as empresas privadas a irem para lá das declarações platónicas, além de não garantir critérios transparentes e independentes no que toca ao equilíbrio delicado que cumpre alcançar entre a preservação do direito fundamental à liberdade de expressão e do princípio democrático e uma *internet* aberta onde imperem esses princípios e a limitação do impacto dos conteúdos desinformativos e manipulativos, ainda que lícitos.

Sem prejuízo os limites apontados, é importante referir que a atuação da UE nesta matéria já se encontra largamente enformada por aquilo que seriam os hipotéticos princípios constitucionais globais sobre a liberdade de expressão na *internet*<sup>285</sup>, designadamente a ideia da limitação da responsabilidade dos intermediários da *internet* (categoria que aqui abrange todas plataformas digitais que, não produzindo conteúdos próprios, são usadas pelos seus utilizadores para nelas colocarem e partilharem conteúdos) pelos conteúdos de terceiros, limitação que encontra respaldo na “Diretiva sobre comércio eletrónico”<sup>286</sup> adotada em 2000 e que, desde essa data, não sofreu qualquer alteração, razão pela qual se encontra datada<sup>287</sup>. Esta Diretiva, adotada no âmbito das competências da União para o mercado interno, limita a responsabilidade dos prestadores intermediários de serviços pelos conteúdos criados por terceiros que estejam disponíveis nos seus serviços, exceto se [i.] o intermediário tenha conhecimento da atividade ou informação ilegal ou [ii.] o intermediário, a partir do momento em que tenha conhecimento da ilicitude, não atue com diligência no sentido de retirar ou impossibilitar o acesso às informações (art.º 14.º, n.º 1, al. a) e b) da Diretiva sobre comércio eletrónico). Mais importante do que esta exclusão de responsabilidade pelos atos de terceiros, a Diretiva estabelece um outro princípio: o da ausência de uma obrigação geral de vigilância a cargo dos intermediários, o que significa que os EM não podem impor aos intermediários uma obrigação de procurarem

<sup>284</sup> *The Sounding Board’s Unanimous Final Opinion on the So-Called Code of Practice*. 24/09/2018. Disponível em: [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=54456](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54456). Consultado em 12/09/2020.

<sup>285</sup> Cfr. Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda. United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression. Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media. Organization of American States (OAS) Special Rapporteur on Freedom of Expression. African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. 03.03.2017.

<sup>286</sup> Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno. JO L 178 17.7.2000.

<sup>287</sup> BAYER et. al., *Disinformation and propaganda...*, p. 81.

ativamente factos ou circunstâncias que indiciem ilicitudes (art.º 15.º, n.º 1 da mesma Diretiva). Ora, a combinação das regras de responsabilização dos intermediários (*maxime*, a obrigação de atuar diligentemente no sentido da remoção do conteúdo para evitar responsabilidade) com a regra da ausência de um dever de vigilância deram origem ao designado sistema «*notice-and-takedown*»<sup>288</sup>, em que após receber uma denúncia relativa à presença de um conteúdo ilegal, o intermediário remove de imediato o conteúdo, notificando o utilizador desse facto e das vias de recurso que tem (ou não) à sua disposição. Este sistema tem sido criticado por violar a liberdade de expressão (art.º 11.º CDFUE), por não respeitar o *due process* (uma vez que o utilizador não é notificado antes da ação ser tomada, não lhe sendo dada oportunidade de defesa, em violação do art.º 47.º CDFUE), por conduzir a que as plataformas, para evitar a responsabilização, removam todo o conteúdo sinalizado automaticamente e por ser suscetível a abusos através de denúncias falsas para obtenção de uma vantagem competitiva<sup>289</sup> ou para silenciar vozes dissidentes<sup>290</sup>, assim colocando em causa o ideal democrático participativo e deliberativo da UE (art.º 10.º e ss. TUE e art.º 15.º TFUE). Ora, as falhas deste sistema e daquela regulação só podem ser ultrapassadas se, no quadro europeu, os vários atores, em especial os EM e o PE, se colocarem de acordo quanto à necessidade de rever a Diretiva (o que, como foi anunciado em junho de 2020, deverá acontecer em breve, com o pacote legislativo sobre serviços digitais<sup>291</sup>) e responsabilizar os intermediários sempre que eles atuem além da sua vocação de meros *depositários*, o que acontece quando recorrem a processos algorítmicos e automáticos de amplificação e personalização de conteúdos, quando gerem os dados pessoais dos utilizadores, quando atuam enquanto plataformas publicitárias, entre outros<sup>292</sup>. Aliás, só uma responsabilização efetiva dos intermediários digitais associada a uma governança em rede e multinível democraticamente legitimada poderia permitir que, como tem acontecido até agora, os atores privados e comerciais que são as plataformas digitais desempenhem funções de

<sup>288</sup> Um sistema alternativo, em vigor no Reino Unido nos casos de difamação, é o do «*notice-and-notice*». De acordo com este sistema, quando um intermediário recebe uma denúncia da existência de conteúdo ilegal na plataforma que gere, reencaminha essa denúncia para quem esteja a disponibilizar esse conteúdo. Esse indivíduo ou organização terá de decidir se pretender entrar numa disputa legal ou remover o conteúdo. Se entender seguir a via da disputa legal, as informações de contacto do distribuidor do conteúdo são reencaminhadas para o denunciante. Se o intermediário não conhecer a identidade do distribuidor do conteúdo ou se este não responder no prazo fixado, o conteúdo é removido pelo intermediário. Vide BÁRD, Petra; BAYER, Judit - *A comparative analysis of media freedom and pluralism in the EU Member States*. Brussels: European Parliament 2016. p. 78.

<sup>289</sup> BAYER et. al., *Disinformation and propaganda...*, p. 84.

<sup>290</sup> BRADSHAW et. al., *Challenging Truth and Trust...*, p. 12.

<sup>291</sup> Cfr. COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Construir o futuro digital da Europa*. COM(2020) 67 final. Bruxelas, 19.2.2020.

<sup>292</sup> Assim, seria de equacionar a responsabilização das plataformas digitais naqueles casos em que, por exemplo, se prove os vieses em que incorreu um algoritmo, o que deu origem a discriminações injustificadas, ou numa situação em que seja direcionada para os utilizadores publicidade sem uma cabal identificação da natureza do conteúdo ou da razão porque foram selecionados para a visualizar.

moderação na esfera pública global, decidindo arbitrariamente sobre os limites da liberdade de expressão e informação nas arenas públicas que gerem. Não existe neste momento, a nosso ver, e tendo em conta a importância crescente que as tecnologias digitais assumem para a democracia, o Estado de Direito e os direitos fundamentais, as condições de legitimidade política e constitucional que permitam às *big tech* atuar como árbitros do discurso público, sobretudo num contexto em que as regras relativas à moderação de conteúdos criadas pelas próprias plataformas, assim como os concretos mecanismos técnicos para filtragem e remoção de conteúdos, muitas vezes com recurso a mecanismos automáticos ou semiautomáticos de moderação que usam algoritmos que rastreiam as plataformas em busca de conteúdos desinformativos ou ilegais que são depois automaticamente eliminados ou bloqueados, são caracterizadas pela opacidade e arbitrariedade, problema, aliás, que se estende aos próprios termos e condições de serviços das plataformas, que recorrem a linguagem vaga ou que envolve uma elevada margem de subjetividade. A este respeito, bem andou a UE ao publicar o Regulamento relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha, que abrange também as plataformas digitais<sup>293</sup>, ao exigir que as cláusulas contratuais gerais destes serviços sejam redigidas de forma simples e inteligível, sempre estabelecendo os motivos para tomar decisões relativas à suspensão, cessação ou imposição de qualquer outro tipo de restrição dos serviços, além de criar mecanismos processuais que regulam essa atuação dos prestadores de serviços de intermediação em linha (como o aviso prévio, a fundamentação da decisão, o direito ao contraditório, etc.). Deveria equacionar-se o alargamento deste Regulamento à relação que os intermediários estabelecem com os utilizadores não profissionais ou consumidores, numa espécie de regime semelhante ao dos contratos de adesão e às suas cláusulas abusivas<sup>294</sup>, propondo-se até que uma entidade independente e democraticamente legitimado no espaço europeu (senão global, lembrando as propostas que apresentámos *supra*) pudesse previamente controlar o conteúdo dos termos e condições de serviço das plataformas digitais que gozem de elevado “poder cívico”. Ao mesmo tempo, é indispensável uma regulação transnacional, que até pode partir de esquemas autorregulatórios, desde que concertados e vinculativos entre os vários intermediários, que estabelecessem regras e procedimentos comuns relativos ao respeito e interferência com direitos fundamentais, como a liberdade de expressão e a proteção de dados, designadamente os mecanismos de moderação de conteúdos e sua supressão, sempre tendo

---

<sup>293</sup> Regulamento (UE) 2019/1160 do PE e do Conselho de 20 de junho de 2019. JO L 186 de 11.7.2019.

<sup>294</sup> Cfr. Directiva 93/13/CEE do Conselho de 5 de abril de 1993 relativa às cláusulas abusivas nos contratos celebrados com os consumidores, na sua redação atual.

como horizonte o respeito do princípio do Estado de Direito, garantindo-se o *due process* e o direito de ação e de reação administrativa e judicial contra as decisões adotadas pelas plataformas digitais, decisões baseadas em regras comuns claras, previsíveis e acessíveis. De facto, o horizonte que nos deve guiar é integrar a *internet* nas regras, procedimentos e princípios próprios do Estado de Direito, da democracia e do respeito pelos direitos fundamentais, sem prejuízo de se reconhecerem as especificidades das realidades virtuais.

Em jeito de conclusão deste tema da desinformação, e ainda aproveitando o objetivo de proteção das eleições do Parlamento Europeu, a Comissão publicou, em 2018, uma Recomendação<sup>295</sup> onde salientava que as garantias eleitorais *offline*, como as regras aplicáveis às comunicações políticas durante os períodos eleitorais, a transparência e os limites das despesas eleitorais, o respeito pelos períodos de reflexão e a igualdade de tratamento dos candidatos, são igualmente aplicáveis *online*, principalmente os limites quanto à publicidade política noutros meios de comunicação, limites esses que deveriam ser estendidos ao ciberespaço. Adicionalmente, foram criadas redes de cooperação eleitoral multinível para garantir a partilha de informação rápida e segura.

No que toca ao cibercrime e à cibersegurança, a ação da UE tem sido mais coerente e eficaz, talvez graças à competência bem firmada no domínio do ELSJ (art.º 67.º, n.º 3 TFUE) e da PESG (art.º 21.º e ss. TUE), uma vez que está em causa a garantia da integridade e segurança das redes e sistemas informáticos em toda a União, muitas vezes contra ataques externos, sendo reconhecido por todos os EM a necessidade de uma atuação conjunta. Nestes termos, em 2016, foi criada a Rede Judicial Europeia de Cibercrime, uma rede de magistrados especializados no combate ao cibercrime e investigações no ciberespaço, além de se terem feito uma série de recomendações destinadas a melhorar a efetivação da responsabilidade criminal no espaço digital<sup>296</sup>. Já antes, a Diretiva relativa a ataques contra os sistemas de informação<sup>297</sup> havia estabelecido regras mínimas relativas à definição de infrações penais e das sanções no domínio dos ciberataques, num exemplo de regulação comum em matérias transnacionais. A UE empenhou-se, também, na criação de um quadro comum para garantir um nível mínimo de segurança das redes e da informação em toda o continente, o que veio a resultar na adoção da

<sup>295</sup> COMISSÃO EUROPEIA – *Recomendação da Comissão de 12.9.2018 sobre redes de cooperação eleitoral, a transparência em linha, a proteção contra os incidentes de cibersegurança e as campanhas de desinformação no âmbito das eleições para o Parlamento Europeu*. C(2018) 5949 final. Bruxelas, 12.9.2018.

<sup>296</sup> CONSELHO DA UNIÃO EUROPEIA - *Conclusões do Conselho da União Europeia sobre a Rede Judiciária europeia em matéria de cibercriminalidade*. Bruxelas, 9 de junho de 2016.

<sup>297</sup> Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013 relativa a ataques contra os sistemas de informação. JO L 218. 14.8.2013.

Diretiva SRI (segurança das redes de informação)<sup>298</sup>, impondo aos EM a designação das autoridades competentes em matéria de cibersegurança, criando equipas de resposta a incidentes de segurança informática (CSIRT), que funcionam a nível nacional e em rede com as equipas dos outros EM e com a equipa de resposta das instituições europeias (a CERT-UE), adotando estratégias nacionais de cibersegurança baseadas em princípios e orientações comuns, numa arquitetura em rede e multinível. Entretanto, em 2019, foi aprovado o Regulamento relativo à ENISA e à certificação da cibersegurança das tecnologias da informação e comunicação<sup>299</sup> com o objetivo de reforçar o mandato da ENISA e de apoiar a elaboração de uma política harmonizada ao nível da UE em matéria de certificação da cibersegurança dos produtos, serviços e processos de TIC. Finalmente, notar que, em 14 de maio de 2019, o Conselho da União Europeia adotou uma Decisão relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a UE e os seus EM<sup>300</sup>, que passam pelas restrições de movimentos e o congelamento de fundos dos responsáveis por ciberataques que tenham um efeito significativo na União. Em função desta Decisão, no passado dia 30 de julho de 2020, o Conselho impôs as primeiras medidas restritivas a seis cidadãos de nacionalidade chinesa e russa, a duas empresas, uma chinesa e outra norte-coreana, e, ainda, a um organismo das forças armadas russas, por alegadamente terem participado em ciberataques conhecidos tais como o “WannaCry” (*ransomware*), o “NotPetya” (*ransomware*), a “Operação Cloud Hopper” (*malware* empregue em ciber-espionagem) e o planeado ciberataque contra a Organização para a Prevenção de Armas Químicas<sup>301</sup>.

Quanto aos conteúdos ilegais *online*, e apesar de não haver uma harmonização do conceito ao nível da UE, pelo que este abrange um grande número de conteúdos distintos que vão sendo definidos, em complementaridade, ao nível nacional, europeu e internacional (v.g.: violação de direitos da propriedade intelectual, ao discurso de ódio, à pedopornografia e ao incitamento ao terrorismo), a UE tem procurado junto das plataformas digitais encontrar mecanismos comuns quanto à identificação e retirada destes conteúdos. Nesta senda, em 2016, e também por iniciativa da Comissão, o Facebook, a Microsoft, o Twitter e o Youtube (a que mais tarde se juntaram o Instagram, o Snapchat e o TikTok) foi subscrito um Código de Conduta para a Luta Contra a os Discursos Ilegais de Incitação ao Ódio em Linha, num projeto de autorregulação

<sup>298</sup> Diretiva (UE) 2016/1148 do PE e do Conselho de 16 de julho de 2016 relativa a medidas destinadas a garantir um nível comum de segurança das redes e da informação em toda a União. JO L 194. 19.7.2016.

<sup>299</sup> Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação. JO L 151/15. 7.6.2019.

<sup>300</sup> Decisão (PESC) 2019/797 do Conselho de 17 de maio de 2019 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros. JO L 129. 17.5.2019.

<sup>301</sup> Decisão (PESC) 2020/1127 do Conselho de 30 de julho de 2020. JO L 246. 30.7.2020.

multinível semelhante ao já referido a propósito da desinformação. Todavia, este Código de Conduta é ainda menos ambicioso em termos de compromissos que o Código de Conduta da UE sobre a desinformação, limitando-se as “empresas de tecnologias de informação” a comprometer-se no cumprimento das suas regras internas no que respeita à notificação, examinação e supressão destes conteúdos, nada se acrescentando quanto a um quadro comum ou ao recurso a mecanismos automáticos de filtragem e a obrigações de vigilância ativa. De notar que, para estes efeitos, a noção de discursos ilegais e de incitação ao ódio parte diretamente da Decisão-Quadro 2008/913/JAI do Conselho, de 28 de novembro de 2008, relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia, designadamente o discurso de ódio e os crimes de ódio.

No que toca à proteção da privacidade, a UE deu um passo fundamental ao adotar o Regulamento Geral de Proteção de Dados<sup>302</sup>, bebendo das competências no âmbito do mercado interno (art.º 4.º, n.º 2, al. a), 26.º, 27.º, 114.º e 115.º TFUE) para a criação do MUD. Esse Regulamento prevê um direito de oposição a decisões individuais automatizadas (art.º 21.º) e o direito de o titular de dados não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a perfilagem (art.º 22.º). Todavia, e a este respeito, a ordem jurídica europeia continua «*em construção no que toca à proteção dos seus cidadãos contra inferências totalmente automatizadas que sejam injustas e irrazoáveis*»<sup>303</sup>.

## **CAPÍTULO II – O CONSTITUCIONALISMO MULTINÍVEL NA UNIÃO E O PAPEL (POSSÍVEL) DA DEMOCRACIA DIGITAL.**

A maioria dos autores concorda que a União Europeia não é nem um Estado, nem uma federação ou confederação de Estados. Também não é uma simples organização internacional ou supranacional de âmbito regional. A UE é, até certo ponto, inexplicável, não se tendo encontrado ainda uma terminologia capaz de, consensualmente, descrever com exatidão a natureza jurídica da arquitetura europeia, pelo que se torna mais simples e menos comprometedor entender a União como entidade *sui generis* ou como «*objeto político não identificado*» nas palavras atribuídas a DELORS<sup>304</sup>. Ainda que seja difícil, perscrutando a história

<sup>302</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. JO L 119 4.5.2016

<sup>303</sup> VERONESE, Alexandre; SILVEIRA, Alexandra; LEMOS, Amanda Nunes Lopes Espiñeira - Artificial intelligence, Digital Single Market and the proposal of a right to fair and reasonable inferences: a legal issue between ethics and techniques. UNIO - EU Law Journal. Vol. 5. n.º 2 (2019). p. 77.

<sup>304</sup> ZILLER, Jacques - *The Nature of European Union Law*. In PÉREZ, J. M. B., GONZÁLEZ-ORÚS, J. M. & ATIENZA, B. B. Tratado de derecho y políticas de la Unión Europea. 2011. Vol. IV.

da integração europeia, encontrar um “momento constituinte” em que o *demos* (?) europeu tenha decidido exercer o seu poder constituinte, instituindo, desse modo, uma constituição<sup>305</sup>, é, hoje, mais ou menos consensual que a UE é governada por uma qualquer forma de direito constitucional, ainda que esse direito se tenha desenvolvido «*sem uma teoria constitucional*»<sup>306</sup>. Assim, o constitucionalismo europeu compreende-se melhor enquanto «*processo de constitucionalização, consistindo em atos discursivos constitucionais interligados*»<sup>307</sup> e provenientes de várias fontes, que vão desde o direito primário e secundário da União, à tutela jurisdicional oferecida pelo TJUE, e, ainda, aos próprios sistemas jurídicos nacionais.

Várias propostas alternativas têm sido apresentadas em torno de uma teoria constitucional para o DUE, sendo o “pluralismo constitucional”, talvez, uma das mais promissoras. Sinteticamente, o pluralismo constitucional analisa a UE como um espaço onde coexistem várias fontes constitucionais - a europeia e as nacionais -, sendo que cada uma dessas fontes reclama a *autoridade final* dentro do mesmo sistema legal (o da UE), o que potencia a existência de conflitos constitucionais que não podem ser resolvidos hierarquicamente (uma vez que as fontes dispõem de uma legitimidade equivalente nos respetivos espaços, organizando-se heteriarquicamente), mas antes através de uma “prática discursiva” entre os tribunais dos diferentes espaços<sup>308</sup>. Outro modo de explicar a arquitetura constitucional da UE reside no constitucionalismo multinível, conceito popularizado por INGOLF PERNICE na sequência do “debate alemão” que se iniciou no Acórdão Maastricht, momento que o Tribunal Constitucional Federal daquele EM, numa reafirmação da autoridade soberana do Estado, decidiu classificar a UE como uma *Staatenverbund*, o que traduzido para português dará qualquer coisa como “*compósito de Estados*”, ao passo que PERNICE a qualificava como “*compósito constitucional*”<sup>309</sup>, de modo a salientar o «*código genético constitucional*» da União<sup>310</sup>, o que viria a dar origem à ideia de que a UE dispõe de uma “constituição compósita”, “mármore” ou ainda um “sistema de constituições compósitas”. Como reconhece GRAÇA ENES, o «*constitucionalismo multinível é agora abordagem teórica sólida para explicar a natureza da*

<sup>305</sup> Sob este ponto de vista, e apesar das «*culturas constitucionais nacionais diferirem acerca do conceito de “constituição”, ele geralmente é concebido como uma entidade normativa unitária, instituída num momento temporal definido*». Os conceitos de chave de constituição são, portanto, «*momento constitucional*», «*demos*» e um «*pouvoir constituant*». Cfr. TUORI, Kaarlo – *The Many Constitutions of Europe*. [Em linha] Oxford: Oxford University Press, 2016.

<sup>306</sup> MADURO, Miguel Poiars – *Three Claims of Constitutional Pluralism*. In AVBELJ, Matej; KOMÁREK, Jan (ed.) - *Constitutional Pluralism in the European Union and Beyond*. London: Hart Publishing, 2012. p. 67-84.

<sup>307</sup> *Ibid.*

<sup>308</sup> MADURO, *Three Claims of Constitutional Pluralism...*

<sup>309</sup> PERNICE, Ingolf - *Multilevel Constitutionalism and the Crisis of Democracy in Europe*. *European Constitutional Law Review*. Vol. 11. (2015). p. 547.

<sup>310</sup> WALKER, Neil – *Multilevel Constitutionalism: Looking Beyond the German Debate*. LEQS Paper No. 08/2009. p. 3.

*relação política e legal da União Europeia e dos Estados-membro»*<sup>311</sup>, permitindo separar o Estado da Constituição, olhando para esta última *além do Estado* mas com ele interagindo<sup>312</sup>, partindo do reconhecimento base de que «*onde quer que haja poder tem de haver limites constitucionais*»<sup>313</sup>. O constitucionalismo multinível, enquanto teoria normativa, não centra a sua visão no Estado ou na soberania, mas antes na «*soberania individual de cada ser humano*»<sup>314</sup>. Assim, PERNICE propõe que se olhe para a UE não como uma «*criatura de Estados, mas de cidadãos agindo através dos seus governos nacionais que atuam em [em seu] nome e por [sua] conta*». Esta visão permite ultrapassar o escolho da legitimação constitucional da UE, visto que ela não é instituída diretamente pelos cidadãos da União, mas antes pelos Estados-membro, que permanecem sendo os “Mestres dos Tratados”. Não obstante, e precisamente porque os EM atuam em nome e em representação dos seus nacionais, a legitimação constituinte e democrática europeia é, pelo menos, sempre dupla, pertencendo tanto aos Estados-membro como aos seus povos que decidem, com a adesão, tornar-se, adicionalmente, cidadãos da União<sup>315</sup>. Mas PERNICE vai mais longe, defendendo que em última instância são os próprios cidadãos os únicos “Mestres dos Tratados”, uma vez que os governos nacionais, quando ratificam tratados internacionais, fazem-no segundo o mandato que lhes é conferido pelos cidadãos, muitas vezes através de referendos<sup>316</sup>. Desta feita, o constitucionalismo multinível parte da assunção de que são os cidadãos o repositório de toda a soberania, podendo estes atribuir ou partilhar parte dos seus poderes com instituições que, para responder a desafios comuns a várias comunidades semelhantes, se localizam noutros níveis de ação política. Assim, uma vez criada a estrutura, os vários níveis, que não estão organizados numa pirâmide hierárquica, antes «*se justapondo*»<sup>317</sup>, interagem em interdependências enquanto componentes de um «*tecido entrelaçado*»<sup>318</sup>. De facto, já CASTELLS reconhecia que a UE «*é essencialmente organizada como uma rede que envolve mais a concentração e a partilha de soberania que a sua transferência para um nível mais alto*», pressupondo um «*pluralidade*

<sup>311</sup> ENES, *Digital platforms and European Union law...*, p. 36

<sup>312</sup> *Ibid.* De facto, é possível (e até necessário) existir constitucionalismo e constituição «*para além do Estado*», essencialmente enquanto «*método*» e «*ethos*» de organização dos atores supranacionais e internacionais. Vide WALKER, Neil - *Taking Constitutionalism Beyond the State*. Political Studies. Vol. 56. n.º 3 (2008). p. 519-543.

<sup>313</sup> MADURO, *Three Claims of Constitutional Pluralism...*

<sup>314</sup> PERNICE, *Risk management ... II*, p. 86.

<sup>315</sup> Essa dupla legitimação retira-se do art.º 10.º TUE, nos termos do qual a representatividade democrática pertence «*diretamente aos cidadãos, ao nível da União, no Parlamento Europeu*» e, indiretamente, através dos EM que estão «*representados no Conselho Europeu pelo respetivo Chefe de Estado ou de Governo e no Conselho pelos respetivos Governos, eles próprios democraticamente responsáveis, quer perante os respetivos Parlamentos nacionais, quer perante os seus cidadãos*».

<sup>316</sup> PERNICE, *Risk management...II*, p. 87.

<sup>317</sup> PERNICE, *Multilevel constitutionalism and the crisis...* p. 545.

<sup>318</sup> ENES, *Digital platforms...*, p. 36.

*de poderes entrelaçados», atrevendo-se até a classificar a UE como um «Estado em rede, caracterizado pela partilha de autoridade numa rede. Rede, por definição, tem nós, e não um centro. Os nós podem ser de tamanhos diferentes e estar ligados por relações assimétricas na rede, de tal forma que o Estado em rede não impede a existência de desigualdades políticas entre os seus membros. [...] Entretanto, não obstante essas assimetrias, os vários nós do Estado europeu em rede são interdependentes, de forma que nenhum nó, nem o mais poderoso, pode ignorar os outros, nem mesmo os menores, no processo decisório. Se alguns nós políticos o fizerem, todo o sistema é questionado»<sup>319</sup>. Deste modo, os diferentes níveis, que também podem ser entendidos como diferentes nós numa rede, não se encontram necessariamente em pé de igualdade, antes detendo as capacidades e atribuições necessárias para enfrentar os desafios do nível político em que operam. No entanto, é importante notar que o constitucionalismo multinível, enquanto sistema de geometria variável, e enquanto resposta à transnacionalização de um grande número de problemas que deixam de ter solução dentro das estruturas do Estado-nação, só sobrevive na interação e respeito constante pelos vários níveis de ação, até porque esta teoria normativa baseia-se quer no princípio da atribuição (art.º 5.º, n.º 2 TUE), segundo a qual, e no caso do nível europeu, a UE só goza das atribuições que lhe tenham expressamente sido conferidas pelos tratados, quer no princípio da subsidiariedade (art.º 5.º, n.º 2 TUE), que, enquanto limite de ação dentro das atribuições, impõe que a UE apenas intervenha no seu nível de ação política quando os níveis imediatamente inferiores não conseguirem alcançar atuação semelhante ou superior. Contrariamente ao pluralismo constitucional, cuja visão parte da existência de múltiplos sítios constitucionais em competição, o constitucionalismo multinível assume que um nível se constrói em complementaridade com os restantes níveis, até porque cada um é criado com objetivos e propósitos diferentes. Como sintetiza PERNICE, «o direito constitucional europeu não está separado das constituições nacionais, antes assentando nessas constituições: os direitos constitucionais europeu e nacional estão entrelaçados e são interdependentes de muitas formas; eles formam um único sistema de direito, uma unidade em substância que produz, idealmente, uma única solução para cada caso particular»<sup>320</sup>.*

Além de se tratar de uma teoria normativa, o constitucionalismo multinível pode ser usado, empiricamente, como ferramenta de regulação de realidades complexas e fragmentadas que fogem ao controlo das fronteiras nacionais. É, arguimos nós, também o caso da gestão do risco digital, que só pode ser verdadeiramente alcançado através de uma abordagem multinível em distintos campos de ação política, que vão desde o local ao global, passando, também,

<sup>319</sup> CASTELLS, Manuel - *A Era da Informação...*, Vol. III, p. 453-4.

<sup>320</sup> PERNICE, *Multilevel Constitutionalism and the Crisis...*, p. 545.

necessariamente, pelo europeu, e envolvendo diferentes atores, desde os públicos aos privados. Se na Secção II do último Capítulo tentamos criar um referencial para as respostas e abordagens comuns que a UE e os seus EM se encontram a implementar, é necessário compreender que essas abordagens não são, ainda, parte de uma política comum e multisetorial de gestão do risco digital, antes partindo de estratégias fragmentadas e sobrepostas para lidar com problemas específicos como a proteção dos dados pessoais, a integridade das eleições, a desinformação ou a automação. Sob esse ponto de vista, e compreendendo que estes fenómenos se encontram em interligação, partilhando causas e efeitos, uma só política digital compreensiva e multinível que explorasse as competências dos vários nós da rede europeia poderia granjear maior eficácia. Mas ainda que isso fosse possível não seria suficiente, pelo menos enquanto se partir de uma perspectiva eurocêntrica que ignora que os problemas com dimensão global têm de ser igualmente abordados nessa escala. Aí, a UE poderia realmente ter um papel relevante, uma vez que tem a experiência necessária à criação de estruturas de “governança sem governo” em vários níveis. Neste domínio, uma iniciativa do tipo “*fórum digital global*” poderia constituir o ponto de partida para uma regulação conjunta do setor digital à escala global, regulação essa assente num sistema de princípios acordado pelos vários atores relevantes através de um processo de deliberação aberto e democraticamente legitimado pelos cidadãos dos vários espaços globais, sem esquecer a criação de mecanismos de execução, acompanhamento e coerção sucessivamente delegados em níveis inferiores. Aliás, suspeitamos que uma estrutura deste tipo, cujo escopo se limitasse à gestão do risco digital, não traduziria uma intrusão dilacerante na soberania estadual, isto porque a própria *internet*, que funciona abertamente e sem fronteiras na maioria dos países, é já uma pedra na engrenagem dessa soberania, não podendo os Estados alegar que estariam a perder poderes sobre uma realidade relativamente à qual o seu escopo de ação foi até hoje extremamente limitado, dependendo, em grande medida, da colaboração das empresas privadas que atuam no setor, que, por força do seu poderio e magnitude, estão quase sempre para além dos mecanismos de coerção tradicionais, o que, julgamos, só poderá ser verdadeiramente ultrapassado através de uma concertação global em torno da publicização de aspetos críticos dos estatutos destas gigantes tecnológicas, o que envolveria a gestão do risco digital em matérias como a proteção de dados, a cibersegurança, a gestão da esfera pública digital e a moderação de conteúdos. Assim, uma cooperação multisetorial nestes domínios poderia até ter o efeito inverso de capacitar os Estados (e a própria UE) com competências que até aqui não lhes pertenciam ou que não podiam verdadeiramente exercer. Mas a UE dispõe ainda de um outro tipo de experiência, talvez mais relevante, situado

no domínio da regulação, o que já resultou em epítetos como o de “Estado regulador”<sup>321</sup> ou “superpotência reguladora”<sup>322</sup>, partindo do “poder normativo europeu” ou do «efeito bruxelas»<sup>323</sup>, que traduz, no contexto da globalização, a capacidade normativa que a União tem de exportar padrões além das suas fronteiras, estabelecendo-se enquanto *standard* global e definindo o *normal* nas relações internacionais.

O constitucionalismo multinível, que se insere no âmbito mais lato do constitucionalismo global e da democracia cosmopolita, não abdica dos quadros fundamentais da democracia deliberativa e participativa. Todavia, facilmente se depreende que a organização do processo político em vários níveis sucessivamente mais abrangentes cria dificuldades exponenciais à participação dos cidadãos nesses diferentes níveis, uma vez que competem com um número crescente de atores. Sob este ponto de vista, e se a esfera pública estadual já é muitas vezes complexa, somando-se dificuldades e exclusões à participação, a inserção de novas esferas ainda mais complexas só vem diminuir as probabilidades e a qualidade dessa participação. A este respeito, a UE oferece-nos um campo empírico para a avaliação da possibilidade de uma esfera pública transnacional, muito embora não se deva cair no erro de, sem mais, transferir as conceções nacionais da esfera pública para o nível europeu. Existem, *grosso modo*, três grandes modelos para a esfera pública europeia: o modelo pan-europeu de esfera pública, quase sempre rejeitado graças à ausência de uma língua, identidade, imprensa e sociedade civil comum aos cidadãos europeus<sup>324</sup>, o modelo da europeização das esferas públicas nacionais<sup>325</sup>, baseado na ideia de que a esfera pública transnacional não tem necessariamente de se assemelhar à nacional, desde que cumpra a função de controlo democrático<sup>326</sup>, todavia para concluir que a esfera pública europeia assim entendida é altamente segmentada e elitista, e o modelo em rede, advogando, no presente, uma esfera pública europeia mais ativa e menos elitista presente já não nos *mass media*, mas na *internet*, sobretudo nas redes sociais<sup>327</sup>. Esta esfera europeia digital é concetualizada como uma rede abundante de assuntos, vozes, linguagens e interpretações

---

<sup>321</sup> JOERGES, Christian – *Unity in Diversity as Europe’s Vocation and Conflicts Law as Europe’s Constitutional Form*. p. 15.

<sup>322</sup> KLEIN, *The view from Spain...*, p. 37.

<sup>323</sup> BRADFORD, Anu – *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.

<sup>324</sup> MÖRÄ, Tuomo – *The European Union and Ideals of the Public Sphere*. In MORING-SALOVAARA, I. *Manufacturing Europe: ...*. Gøthenburg: NORDICOM, 2009. p. 81.

<sup>325</sup> HENNEN, Leonhard – *E-Democracy and the European Public Sphere*. In HENNEN, L., KEULEN, I. V., KORTHAGEN, I., AICHHOLZER, G., LINDNER, R. & NIELSEN, R. O. - *European E-Democracy in Practice*. [s.l.]: Springer, 2020. p. 58 e ss.

<sup>326</sup> Este modelo insiste sobretudo no papel dos *media* tradicionais para disponibilizar, a nível nacional, informação sobre as instituições europeias (“europeização vertical”) para efeitos de controlo democrático e sobre os outros EM (“europeização horizontal”) para criar um certo sentido de comunidade e identidade.

<sup>327</sup> HENNEN, *E-Democracy and the European...*, p. 66 e ss.

culturais em diversos canais comunicativos<sup>328</sup>, em que os vários atores interagem porque os assuntos europeus os unem, ainda que com laços mais fracos que ao nível nacional. Não obstante, e porque a «*internet tem o potencial quer para criar espaços públicos, quer para enfraquecer a esfera pública em geral*»<sup>329</sup>, é ainda necessário aguardar por mais estudos quanto à possibilidade, existência e efetividade dessa esfera pública europeia em rede. Não obstante, e apesar das muitas questões que a esfera pública enfrenta, as tecnologias digitais podem ser encaradas como uma oportunidade, não como contribuindo para a fragmentação da discussão pública, mas antes, e idealmente, como veículo para a sobreposição de várias discussões a vários níveis e sobre múltiplos temas. Neste contexto, poderia ser interessante explorar as possibilidades de introdução nos vários níveis de modelos como o da “democracia líquida”, que combina a participação direta com formas altamente flexíveis de participação indireta, podendo os cidadãos ou escolher em que políticas ou níveis querem votar e participar diretamente ou em que querem ser representados por terceiros a quem confiam os seus votos<sup>330</sup>. Ou ainda a “wikidemocracia”, que advoga, em síntese, uma “colaboração” ativa, permanente e diferenciada dos cidadãos nos processos de decisão coletiva e de elaboração de políticas públicas, tudo com recurso às tecnologias digitais capazes de estabelecer mecanismos de conexão e troca de informações, conhecimentos e debate a larga escala e com baixos custos<sup>331</sup>. Ora, as potencialidades das tecnologias digitais para permitirem uma discussão coletiva são conhecidas, recordando-se aqui os poderes cívicos das plataformas digitais, designadamente o poder de controlar a atenção de milhões de utilizadores e de a direcionar para determinados acontecimentos, como geralmente sucede depois de ataques terroristas e desastres naturais<sup>332</sup>, o que demonstra que o digital pode ser plataforma para “discussões globais”. Por outra via, e apesar de as redes se terem tornado «*primariamente esferas de auto-publicação para a obtenção instantânea de gratificação em lugar de espaços de deliberação e de construção de uma identidade social e política*»<sup>333</sup>, a verdade é que as tecnologias digitais vieram permitir e potenciar a organização da ação coletiva, coadjuvando os meios tradicionais, mas, também, fazendo surgir novas formas de organização e associação coletiva *online*. A este respeito, o

<sup>328</sup> RASMUSSEN, *Internet-based media...*, p. 102.

<sup>329</sup> HENNEN, *E-Democracy and the European...*, p. 67.

<sup>330</sup> BLUM, Christian; ZUBER, Christina Isabel - *Liquid Democracy: Potentials, Problems, and Perspectives*. The Journal of Political Philosophy. Vol. 24. n.º 2 (2016). p. 162-182.

<sup>331</sup> NOVECK, Beth Simone - *Wiki government: how technology can make government better, democracy stronger, and citizens more powerful*. Washington, D.C.: Brooking Institution Press, 2009.

<sup>332</sup> MOORE, *Tech Giants and Civic Power*, p. 27.

<sup>333</sup> KLEUT, Jelena; PAVLÍČKOVÁ, Tereza; PICONE, Ike; RIDDER, Sander De; ROMIC, Bojana; HARTLEY, Jannie Møller - *Emerging Trends in Small Acts of Audience Engagement and Interruptions of Content Flows*. In DAS, R. & YTRE-ARNE, B. *The Future of Audiences: A Foresight Analysis of Interfaces and Engagement*. [s.l.]: Palgrave Macmillan, 2018. p. 125.

Movimento “15-M”, dos “Indignados” e o PPF (“*Put People First*”), a Primavera Árabe, o Movimento “*Occupy Wall Street*” ou, mais recentemente, os protestos “*Euromaidan*” na Ucrânia, o movimento independentista catalão<sup>334</sup>, os protestos pró-democracia em Hong Kong, as “greves” e “marchas climáticas”, o movimento “*#MeToo*” ou o movimento dos “*Gilets Jaunes*”, todos fazem ou fizeram uso das plataformas digitais, das redes sociais ou, mais genericamente, da *internet* como meios não só de divulgação das suas lutas e reivindicações, mas também, senão sobretudo, como instrumentos de mobilização e organização coletiva<sup>335</sup>. Não obstante, vários autores notam que o ativismo *online* é diferente do ativismo *offline*<sup>336</sup>, sendo o primeiro, principalmente no tocante a movimentos recentes, «*mais impactante e imprevisível*»<sup>337</sup>, com novas ações, causas e atores, havendo mesmo quem distinga entre “ação coletiva” e “ação conetiva”<sup>338</sup>, correspondendo esta última a uma lógica de ação em rede que recorre às plataformas digitais para assegurar o envolvimento do público através de temas e mensagens simples, adaptáveis, pessoais, personalizáveis e ressonantes junto da maioria das pessoas (dando origem à “*digitally networked action*”)<sup>339</sup>. A “ação conetiva”, por comparação à “ação coletiva”, requer pouca ou nenhuma coordenação e estrutura organizativa (numa espécie de “organização sem organizações”), nem requer a construção de uma única identidade coletiva, sendo a ação individual pública ou o contributo para uma causa comum um ato de expressão pessoal, de reconhecimento ou de auto-validação. Em sentido contrário, a “ação coletiva” necessita de um maior envolvimento dos participantes (e uma dificuldade acrescida de mobilização), uma estrutura formal de organização e coordenação coletiva mais complexa (com um plano de ação bem delineado e acordado pela maioria) e a mobilização de mais meios e recursos (ainda que o surgimento do digital tenha feito descer transversalmente os custos de organização)<sup>340</sup>. Tendo em conta a facilidade do envolvimento *online*, há quem entenda que o

<sup>334</sup> Ilustrando a influência das plataformas digitais na organização coletiva em torno da independência catalã, vide as notícias que dão conta da criação de uma aplicação móvel e de uma plataforma na *internet* que dirige os manifestantes para locais estratégicos por forma a maximizar o efeito da rebelião: <https://tinyurl.com/y6zntmas> Consultado em 25/07/2020.

<sup>335</sup> Não é incontestado o sucesso das plataformas digitais e das redes sociais quando usadas no âmbito de protestos políticos e da ação coletiva, com vários autores a apontarem para uma possível hipervalorização do digital em detrimento das estruturas organizativas tradicionais *offline* (ou da importância da combinação dos vários modelos), além de destacarem quer o resultado desses movimentos (v.g., no caso da Primavera Árabe, que ficou para a história como as primeiras “Revoluções Facebook”), quer a reverso da medalha com a vigilância das plataformas digitais pelos governos e Estados para suprimir a dissidência, o que faz com que, nestes contextos, o digital corresponde a uma «*double-edged sword*». Cfr., *inter alia*, MOROZOV, Evgeny - *The internet is a tyrant's friend*.

<sup>336</sup> VESNIC-ALUJEVIC et. al., *The Future of Government 2030+...*, p. 22.

<sup>337</sup> *Ibid.*, p. 16.

<sup>338</sup> BENNETT, W. Lance; SEGERBERG, Alexandra - *The Logic of Connective Action: digital media and the personalization of contentious politics*. Information, Communication & Society. Vol. 15. n.º 5 (2012).

<sup>339</sup> Destacam os autores que o enquadramento da “ação conetiva” requer muito pouco do ponto de vista da persuasão, da razão e da reconciliação de diferentes perspetivas face a um problema comum, visto que a ação conetiva é inclusiva. BENNETT et. al., *The Logic of Connective Action...*, p. 742.

<sup>340</sup> *Ibid.*, p. 756.

ativismo *online* é ativismo “fraco”, na medida em que o envolvimento dos participantes se resume «na participação em manifestações, na assinatura de petições, na alteração da foto de perfil», pelo que previamente outras pessoas terão desenvolvido o trabalho de reflexão e problematização em torno de um problema comum, planeando as formas de ação, o que, por sua vez, corresponde ao ativismo “forte”<sup>341</sup>. Do ponto de vista crítico, recorre-se com frequência às expressões “*clicktivism*” e “*slacktivism*” para descrever um ativismo fácil e “preguiçoso” de recompensa imediata que se traduz no apoio *online* através de atos públicos nas redes sociais com pouco impacto real<sup>342</sup>. Por outra, o aproveitamento das tecnologias digitais para a organização coletiva é transversal a todo o espectro político, não obstante as evidências que apontam para um uso intenso das tecnologias digitais pelas forças políticas conotadas com a extrema-direita no âmbito das designadas «*revoltas populistas*»<sup>343</sup> da segunda metade da última década em diante e, ainda, pelos vários regimes de feição autoritária, onde a *internet* serviu genericamente como forma de fortalecimento do poder (como é o caso da China, v.g.). Assim, é possível concluir que, a uma primeira fase em que a *internet* é vista com grande otimismo, sucedeu uma segunda fase (a atual) em que a mesma *internet* é já vista com pessimismo. Daqui se retira que a Era Digital não tem nenhum apelo libertador fundamental, sem que isso signifique que não a podemos encarar enquanto mecanismo que pode potenciar uma maior democratização das sociedades sob as circunstâncias certas.

A organização, mobilização e ação cívica e política através dos meios digitais é uma das dimensões da “democracia digital” ou “e-democracia”. A perceção de que as TIC podem ter um potencial tremendo para «*transformar as práticas de comunicação política existentes e os próprios sistemas políticos*» remonta à década de 60 do século passado, acompanhando, pois, os alvares da *internet*<sup>344</sup>. Neste contexto, a democracia digital pode ser definida como «*a prática democrática que recorre ao apoio ou suporte dos media digitais na comunicação e participação política*», ao passo que a “e-participação” «*engloba todas as formas de participação política que façam uso dos media digitais, incluindo quer os mecanismos*

<sup>341</sup> ZUCKERMAN, Ethan - *New Media, New Civics?*. Policy and Internet. Vol. 6. n.º 2 (2014). p. 158.

<sup>342</sup> Vide MOROZOV, *The Net Delusion...*, p. 190. O Autor ilustra esta problemática com o exemplo de uma campanha organizada no Facebook para «*salvar as crianças africanas*» através da recolha de donativos. A campanha foi apoiada publicamente por mais de 1,7 milhões de utilizadores, mas conseguiu reunir 12 mil dólares.

<sup>343</sup> DAHLGREN, Peter - *Media, Knowledge and Trust: The Deepening Epistemic Crisis of Democracy*. Javnost - The Public. Vol. 15. n.º 1-2 (2018). p. 20-27. (p. 24). São exemplos desta deriva a eleição de Donald Trump, Jair Bolsonaro, Rodrigo Duterte e ainda a presença no espaço público e expressão eleitoral de partidos como o Movimento 5 Estrelas, a Aurora Dourada, o Vox, o Podemos, a Frente Nacional, o PiS e o UKIP.

<sup>344</sup> LINDNER, Ralf; AICHHOLZER, Georg - *E-Democracy: Conceptual Foundations and Recent Trends*. In HENNEN, L., KEULEN, I. V., KORTHAGEN, I., AICHHOLZER, G., LINDNER, R. & NIELSEN, R. O. *European E-Democracy in Practice*. [s.l.]: Springer, 2020. p. 15.

*formalmente institucionalizados, quer o envolvimento cívico de carácter informal*»<sup>345</sup>. HACKER et. al., na definição de democracia digital proposta no início deste século, destacava que as TIC diluíam as limitações de «*tempo, espaço e outras condicionantes físicas*»<sup>346</sup> das práticas democráticas, aumentando a escala e a velocidade do acesso e distribuição de informação, assim contribuindo para a «*criação de cidadãos mais informados*», facilitando a participação política através da atenuação de obstáculos como a apatia e a timidez, entre outros, e, no domínio da ação coletiva, através da redução significativa dos custos de organização e mobilização<sup>347</sup>. Por outro lado, o recurso aos *media* digitais contribui para uma crescente horizontalidade e imediação da comunicação política associada a uma reforçada “voz” da cidadania em torno da definição das agendas políticas<sup>348</sup>. Desta associação entre e-democracia e reforço da participação através de meios digitais resulta a ideia de que a democracia digital tem mais potencial nos modelos democráticos participativos e deliberativos em lugar do modelo liberal, onde se resume a uma incrementação no acesso à informação<sup>349</sup>. Talvez a conceptualização mais compreensiva sobre os princípios, objetivos e orientações da e-democracia seja a do Conselho da Europa cujo Comité de Ministros adotou, em 2009, uma Recomendação sobre a democracia eletrónica, reconhecendo, desde logo, que as TIC têm «*progressivamente facilitado a disseminação de informações e o debate sobre questões políticas, permitido uma participação democrática mais ampla de indivíduos e grupos, garantido maior transparência e responsabilização nas instituições e processos democráticos, funcionando, assim, em benefício da democracia e da sociedade*», mas não deixando de alertar para os riscos decorrentes, por exemplo, «*da falta de acesso às TIC e às inadequadas capacidades de e-literacia*»<sup>350</sup>. Nessa recomendação, é avançada uma longa lista de 80 princípios e 102 orientações para a implementação da e-democracia, com destaque para a ideia de que a democracia digital serve sobretudo para apoiar e fortalecer o processo democrático, assumindo, por isso, um carácter «*adicional, complementar e interconectado com os processos democráticos tradicionais*»<sup>351</sup>,

<sup>345</sup> *Ibid.*, p. 18.

<sup>346</sup> HACKER, Kenneth L.; DIJK, Jan van - *What is Digital Democracy?*. In HACKER, K. L. & DIJK, J. V. *Digital Democracy: Issues of theory and practice*. London: Sage, 2000. p. 1.

<sup>347</sup> *Ibid.*, p. 4.

<sup>348</sup> De facto, no seu Relatório de 2016 sobre o “e-governo”, a ONU salienta que os «*avanços em torno da e-participação são motivados mais pelo ativismo cívico de indivíduos que buscam ter maior controlo sobre a sua própria vida do que pela disponibilidade de recursos financeiros ou tecnologias dispendiosas. Vários países em desenvolvimento, incluindo alguns países menos desenvolvidos, geram inúmeras boas práticas usando soluções de baixo custo (com código aberto) prontas a utilizar que se baseiam na colaboração entre os cidadãos*». Cfr. UNITED NATIONS – *E-Government Survey 2016. E-Government in Support of Sustainable Development*. New York: United Nations, 2016. p. 3.

<sup>349</sup> LINDNER et. al, *E-Democracy: conceptual Foundations...*, p. 13 e ss.

<sup>350</sup> COUNCIL OF EUROPE – *Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy)*. 18.02.2009. p. 1.

<sup>351</sup> *Ibid.*, p. 4.

baseando-se, antes de mais, no respeito pelos direitos humanos, incluindo o direito à privacidade e à proteção dos dados pessoais e promovendo os valores democráticos e culturais da sociedade em que é implementada. A democracia digital é um fenómeno multifacetado e multidimensional<sup>352</sup>, podendo assumir múltiplas e diferentes formas em função do contexto em que seja utilizada. AICHHOLZER et. al. distingue essencialmente três dimensões ou funções da e-democracia, quando perspectivada do ângulo da e-participação<sup>353</sup>: [i.] a monitorização e controlo do processo político e democrático através, por exemplo, do acesso eletrónico dos cidadãos às informações de interesse público (“e-informação”), da deliberação e discussão *online* (“e-deliberação”), da apresentação de reclamações, questões e queixas (“e-queixa”), entre outros; [ii.] a definição da agenda política através, entre outros, da formulação eletrónica de protestos e recomendações a instituições democráticas (“e-petições”), da formulação por meios *online* de propostas políticas (“e-iniciativas”) e da mobilização coletiva digital em torno de causas e objetivos específicos, eleitorais ou não (“e-campanhas”); [iii.] e a efetiva tomada de decisões recorrendo, designadamente, aos sistemas eletrónicos de voto (“e-voto”)<sup>354</sup>, à recolha digital de opiniões de especialistas ou do público em geral relativas a um determinado tópico político (v.g.: uma proposta de lei) de modo a informar e, possivelmente, influenciar (mas sem que exista um carácter vinculativo) o responsável pela decisão final (“e-consulta”), e, ainda, à definição de prioridades na determinação de gastos e investimentos orçamentais públicos (“orçamentos e-participativos”). Das três dimensões apontadas, é a primeira aquela que regista maiores desenvolvimentos, atendendo à quantidade apreciável de informação política, governamental e administrativa que se encontra hoje à disposição dos cidadãos através da *internet*. Todavia, os autores que, na década de 80 e 90, viram na e-democracia um instrumento que traria de volta a democracia direta ao estilo ateniense estarão por certo

<sup>352</sup> Por exemplo, o Conselho da Europa, na aludida Recomendação, refere que e-democracia engloba os seguintes setores: «*e-parlamento, e-legislação, e-justiça, e-mediação, e-ambiente, e-eleição, e-referendo, e-iniciativa, e-voto, e-consulta, e-petição, e-campanha, e-votação e e-sondagem, fazendo uso da e-participação, da e-deliberação e dos e-fóruns*» (p. 7). Nesta conceção, o e-parlamento, que se encontra intimamente ligado a outras dimensões da democracia digital, permite uma melhoria qualitativa no princípio da representação, decorrente de um maior envolvimento dos cidadãos com os seus representantes, facilitando, além do mais, o surgimento de assembleias deliberativas no nível local, regional, nacional, supranacional e internacional.

<sup>353</sup> AICHHOLZER, Georg; ROSE, Gloria - *Experience with Digital Tools in Different Types of e-Participation*. In HENNEN, L., KEULEN, I. V., KORTHAGEN, I., AICHHOLZER, G., LINDNER, R. & NIELSEN, R. K. *European E-Democracy in Practice*. [s.l.]: Springer, 2020.

<sup>354</sup> O “e-voto” é, porventura, a mais crítica dimensão da democracia digital e, consequentemente, aquela que vai conhecendo maior resistência. Realmente, as eleições são um dos pilares e uma das condições necessárias a uma democracia efetiva, sendo que a legitimidade do resultado depende da transparência, confiança e segurança de todo o processo. Daí que, na UE, só a Estónia recorra ao voto via *internet* para todos os tipos de eleições. É que se as eleições têm necessariamente de ser universais, iguais, secretas, diretas e livres, a verdade é que a observância destes princípios através dos meios digitais representa grandes desafios técnicos. A este propósito, vide Recomendação REC(2004)11 do Comité de Ministros do Conselho da Europa para os estados-membro sobre os *standards* legais, operacionais e técnicos para o e-voto, adotada em 30/09/2004, acessível em <https://tinyurl.com/y44jkkgl>.

dececionados, na medida em que a e-participação «*permanece largamente confinada aos estágios iniciais e finais do ciclo político (definição da agenda, preparação e avaliação de políticas), raramente permitindo aos cidadãos a entrada nos estágios centrais da tomada de decisões e da execução das políticas*»<sup>355</sup>. Aliás, e tomando como pano de fundo os instrumentos da “propaganda computacional”, AICHHOLZER et. al. nota que o envolvimento político digital pode estar a transformar a «*natureza contratual da relação de representação política entre eleitos e eleitores*», uma vez que a opinião pública surge como uma «*bússola através da qual os representantes vão alinhando o exercício do seu mandato*», pelo que o contrato, cujos termos estão definidos nos programas eleitorais, é substituído por uma «*relação em permanente fluxo, com os políticos a serem constantemente desafiados a determinarem as suas posições vis-à-vis com a opinião pública*»<sup>356</sup>.

Apesar de a democracia digital, que «*consiste numa mudança cultural*»<sup>357</sup>, poder contribuir decisivamente para atenuar o percecionado “défice democrático” da UE, nomeadamente através da participação e do envolvimento dos cidadãos europeus nos processos de formação e execução das políticas europeias, aumentando a confiança nas instituições e o sentido de representação, a verdade é que a UE se tem focado sobretudo na dimensão do “e-governo”<sup>358</sup>, procurando sistematicamente retirar potencialidades, em termos de eficiência e de redução de custos burocráticos para os cidadãos e para as empresas no âmbito do mercado interno, da digitalização das administrações públicas nacionais. Não obstante, já no início do século se reconhecia a necessidade de aproximar e conectar as instituições e os seus representantes com os cidadãos da Europa, cada vez mais «*desencantados e com questões fundamentais relativas ao futuro da Europa*»<sup>359</sup>, o que se propunha que se fizesse através de uma estratégia de comunicação e de participação mais intensa recorrendo às TIC para a criação de um «*”espaço”*»

<sup>355</sup> AICHHOLZER et. al., *Experience with Digital Tools...*, p. 94.

<sup>356</sup> *Ibid.*, p. 102.

<sup>357</sup> SILVEIRA, et. al., *Do mercado interno à cidadania de direitos...*, p. 16.

<sup>358</sup> A CE adotou, desde 2006, três planos de ação (2006-2010, 2011-2015 e 2016-2020) com o objetivo de avançar com a modernização das administrações públicas em toda a União Europeia. Esses esforços da Comissão foram sendo secundados pelos ministros encarregues das políticas de “e-governo” dos Estados que integram a UE e a EFTA, primeiro através da Declaração de Malmö (2009) e, mais recentemente, através da Declaração de Tallinn (2017). Note-se que a política em torno do “e-governo” obedece, essencialmente, aos seguintes princípios: “*digital by default*” (os serviços públicos devem ser prestados preferencialmente por meios digitais, ainda que se mantenham outras vias para quem se encontre desconectado), “princípio uma-só-vez e uma-só-paragem” (os cidadãos só precisam de fornecer a mesma informação uma vez para todos os serviços, os quais devem, preferencialmente, estar concentrados numa só plataforma), inclusão e acessibilidade, abertura e transparência, interoperabilidade por predefinição, confiança e segurança. Cfr. COMISSÃO EUROPEIA – *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Plano de ação europeu (2016-2020) para a administração pública em linha. Acelerar a transformação digital da administração pública*. COM(2016) 179 final. Bruxelas, 18.4.2016. p. 4.

<sup>359</sup> COMMISSION OF THE EUROPEAN COMMUNITIES – *European Governance: a White Paper*. COM(2001) 428. Brussels, 25.7.2001, p. 6.

*transnacional onde os cidadãos dos diferentes países possam discutir aquilo que percebem como sendo os desafios que se colocam à União»*<sup>360</sup>. Essa estratégia deveria garantir um maior envolvimento dos níveis locais e regionais na definição das políticas da UE numa estrutura multinível, além de promover a participação da sociedade civil. Nesta senda, o Tratado de Lisboa «veio atribuir especial ênfase ao fortalecimento dos elementos democráticos na UE»<sup>361</sup>, através, por exemplo, da introdução da Iniciativa de Cidadania Europeia (art.º 11.º, n.º 4 TUE e art.º 24.º TFUE). Ademais, o Tratado prevê, entre outros, uma visão democrática centrada no cidadão (art.º 10.º, n.º 3 TUE e art.º 15.º TFUE), o diálogo horizontal (art.º 11.º, n.º 1 TUE) e vertical (*idem*, n.º 2) com a sociedade civil, além de assegurar que a CE procede a amplas consultas (as quais, são, atualmente, “e-consultas”)<sup>362</sup> e de garantir aos cidadãos o direito de petição (e “e-petição”)<sup>363</sup>. Assiste-se, portanto, a uma preocupação crescente quanto ao papel da participação pública e do envolvimento dos cidadãos na governança da União. Esta preocupação não é, com certeza, alheia, do ponto de vista da constitucionalização da UE, à ausência de um *demos* europeu, pelo menos no sentido germânico do *Volk*<sup>364</sup>. Ora, porque a «*democracia não existe num vacuum*»<sup>365</sup>, tendo como premissa indispensável a existência de uma comunidade de membros por quem e para quem o discurso democrático tem lugar, se não há *demos*, também não pode existir constituição<sup>366</sup>. Todavia, como reconhece HABERMAS, «*as nações, como todas as outras grandezas comparáveis, não são factos naturais*», pelo que o *demos* parte sempre de uma construção imaginária, uma unidade sociológica que faz com que os indivíduos de um dado espaço tomem consciência de uma pertença abstrata a uma determinada comunidade. Sem prejuízo, é possível, senão desejável, imaginar a construção de um *demos* europeu sob uma outra base que não a identidade cultural ou a identificação nacional, antes ancorada numa decisão racional e num compromisso em torno do respeito de valores partilhados e, ainda, de um entendimento comum quanto aos direitos e deveres sociais. A nosso ver, o *demos* da UE pode ser construído em torno de uma comunidade valorativa historicamente ancorada e politicamente motivada, que partilha uma cultura intelectual e racional que transcende as diferenças subjetivas e orgânicas. Sob este ponto de vista, a instituição de uma cidadania europeia (art.º 20.º e ss. TFUE) é um passo importante, mas insuficiente, para a percepção de uma pertença comum, até porque a cidadania europeia não correspondeu à intenção

<sup>360</sup> *Ibid*, p. 10.

<sup>361</sup> LINDNER et. al., *E-Democracy: Conceptual...*, p. 24.

<sup>362</sup> Art.º 11.º, n.º 3 TUE

<sup>363</sup> Art.º 24.º TFUE e art.º 44.º CDFUE.

<sup>364</sup> Cfr., *inter alia*, WEILER, Joseph H. H. – *Does Europe Need a Constitution? Demos, Telos and the German Maastricht Decision*. European Law Journal. Vol. 1. n.º 3 (1995).

<sup>365</sup> *Ibid*, p. 2.

<sup>366</sup> HABERMAS, *Um ensaio sobre a constituição da Europa*, p. 66.

de criar uma «*cidadania nova, autónoma em relação à cidadania nacional*» que, por isso, fizesse supor o nascimento, em sentido jurídico, de «*cidadãos europeus, no sentido de povo europeu*»<sup>367</sup>. Não obstante, a cidadania da UE pode ser vista como um «*status de possibilidades*»<sup>368</sup> sujeito ao princípio da realização e definição progressiva, dependente do curso do processo de integração (cfr. art.º 25.º TFUE), sendo, simultaneamente, um sinal de que é possível pensar a pertença política e o exercício de direitos além do Estado num contexto transnacional ou global. Neste quadro, a “*cidadania digital*”, enquanto «*capacidade para um envolvimento positivo, crítico e capacitado no ambiente digital*»<sup>369</sup>, pode ter potenciais extraordinários para quem advogue uma autonomização da cidadania da UE<sup>370</sup>. Como questiona VESNIC-ALUJEVIC et. al., «*na Era das tecnologias digitais, dos estados supranacionais e da hiperconectividade além das fronteiras, pode a cidadania estar limitada à pertença a uma comunidade política específica de um único Estado com o qual nos podemos identificar?*»<sup>371</sup>. De facto, num mundo globalizado em permanente troca digital, as diferenças identitárias tendem a esbater-se, aproximando-se os povos num gradual processo de aculturação por parte das potências e vozes que estabelecem as narrativas dominantes. Esse processo tem lugar privilegiado no *online*. Nestes termos, não é difícil encontrar cidadãos em cuja vida política se «*sobrepõem várias lealdades às quais cada um atribui uma importância completamente diferente*»<sup>372</sup>, desde o nível local, ao nacional, ao europeu e ao global. Em face disto, é possível, também no quadro de um constitucionalismo multinível global, prefigurar uma situação em que um indivíduo dispõe de direitos e obrigações em cada nível, razão pela qual em cada nível lhe é atribuído um *status civitas* próprio e autónomo, cujos critérios de aquisição podem variar<sup>373</sup>. Essa autonomização e sobreposição de múltiplos estatutos poderia servir para fomentar uma ligação mais direta e imediata dos cidadãos às suas distintas esferas de cidadania, uma vez que todas essas esferas seriam colocadas horizontalmente em posição de igualdade (funcionando apenas como sítios distintos de exercício de direitos e deveres),

<sup>367</sup> QUADROS, Fausto de - *Direito da União Europeia: direito constitucional e administrativo da União Europeia*. Coimbra: Almedina, 2004. p. 560-1.

<sup>368</sup> GORJÃO-HENRIQUES, Miguel - *Direito da União: história, direito, cidadania, mercado interno e concorrência*. 6.ª ed. Coimbra: Almedina, 2010. p. 561.

<sup>369</sup> Vide a Declaração Ministerial da Reunião dos Ministros da Educação de 26.11.2019 em Paris: “*Citizenship education in the digital era*”.

<sup>370</sup> Cfr., *inter alia*, GARNER, Oliver - *The Existential Crisis of Citizenship of the European Union: The Argument for an Autonomous Status*. *Cambridge Yearbook of European Legal Studies*. n.º 20 (2018).

<sup>371</sup> VESNIC-ALUJEVIC et. al., *The Future of Government 2030+ ...*, p. 20.

<sup>372</sup> HABERMAS, *Um ensaio sobre a constituição da europa*, p. 108.

<sup>373</sup> I.e., admitimos que os critérios de aquisição da cidadania nacional podem exigir uma ligação genuína e forte àquela comunidade em detrimento de outras, mantendo-se esse estatuto inalterado; já no nível da UE, a cidadania poderia prever um critério de aquisição baseado na permanência ou residência na UE por determinado lapso de tempo considerado suficiente para a criação de uma ligação genuína com a UE; a cidadania global seria inerente e inextricável do estatuto de pessoa humana.

requerendo do cidadão semelhante grau de atenção e relacionamento, o qual se alcançaria através do pleno aproveitamento das ferramentas tecnológicas e da democracia digital, que potenciam uma participação além das barreiras do espaço e do tempo e a emergência de distintas e sobrepostas legitimidades e arenas discursivas e deliberativas em níveis muito diferentes de ação política.

## CONCLUSÃO

Os riscos associados à Era Digital são indisputados, o que inclusive levou o Fórum Económico Mundial a cunhar, em 2013, a expressão “*digital wildfires*”, alertando para um «*mundo hiperconectado*» onde as redes sociais servem para difundir desinformação, ao passo que a forma como esses conteúdos podem influenciar o comportamento humano permanecem por descortinar completamente<sup>374</sup>. Estar no mundo, para o *homo digitalis*, significa estar *em* e *na* rede, sendo o processo de digitalização das sociedades, em permanente aprofundamento, irreversível. É segura a conclusão de que o aparato tecnológico digital, nas suas mais variadas formas, alterou fundamentalmente o modo como os cidadãos comunicam, acedem à informação e colaboram entre si. Em 2019, e só na UE (a 27), cerca de 77% dos cidadãos admite aceder todos ou quase todos os dias à *internet*, sendo certo que mais de metade (54%) o fazem para navegar e interagir nas redes sociais<sup>375</sup>. Os processos políticos estão, também, em processo de transformação. Os limites do Estado-nação deixaram de ter significado na arena virtual global, a qual não conhece barreiras físicas, temporais, sociais, económicas ou linguísticas. Fenómenos como a desinformação, a modelação da esfera pública virtual segundo critérios opacos e nunca neutrais, a cibercriminalidade e os ciberataques, expõem a perda de capacidades de ação dos Estados nacionais, incapazes de, a partir de dentro das suas fronteiras, combater realidades transnacionais que ferem os princípios estruturais do Estado de Direito e da democracia.

As plataformas digitais atuam, no alvor desta transição, enquanto *sítios* de imensos poderes incontrolados, influenciando e determinando as conversas globais e a própria forma como os cidadãos comunicam (ou não) entre si e se autorrepresentam. Actualmente, a política já não se faz sem o recurso às ferramentas digitais, surgindo em cada rede um novo fórum ou arena que constitui uma de muitas esferas públicas sobrepostas em rede. Por outro lado, as redes sociais podem funcionar enquanto “silos digitais”, onde cada pessoa se encontra presa ouvindo apenas

<sup>374</sup> WORLD ECONOMIC FORUM - *Global Risks 2013*. 18.ª ed. Geneva, 2013.

<sup>375</sup> Dados do EUROSTAT, disponíveis no separador temático “*Digital Economy and Society*” em <https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables>. Consultado em 26/08/2020.

ecos da sua própria voz. Em contraponto, os crescentes “poderes cívicos” das plataformas digitais, que atuam enquanto árbitros da verdade e da visibilidade, não sujeitas a estatutos editoriais semelhantes aos dos restantes meios de comunicação social, não estão acompanhados de processos que garantam a sua legitimação e responsabilização democrática. Pelo contrário, a persistência no ambiente digital da desinformação, da propaganda computacional e dos algoritmos opacos que personalizam a experiência do utilizador *online* demonstra que o caminho ainda é longo para quem procura uma esfera pública virtual realmente igualitária e democrática não só no acesso, mas também na permanência.

Como fomos destacando ao longo destas páginas, o digital não contém em si mesmo nenhum apelo libertador fundamental, tanto servindo para emancipar e empoderar como para monetizar, manipular, controlar e oprimir. Os determinantes dos usos das tecnologias digitais sempre estarão dependentes dos seus agentes e respetivas intenções e, também, do modelo de governança e controlo escolhido para prevenir os riscos digitais. Até este momento, e porque a ideia de uma *internet* aberta continua a ser preponderante, a existência de uma estratégia global para a gestão do risco digital é uma miragem, ainda que na União Europeia se procurem dar os primeiros passos. Estamos em crer que as tecnologias digitais são componentes essenciais das várias revoluções que se avizinham, desde a transição energética à revolução do mercado de trabalho, como ficou evidente nos acontecimentos mais recentes. Todavia, a dependência face às novas tecnologias, cada vez mais intrusivas e físicas, tem de ser acompanhada de mecanismos eficazes que garantam a segurança dos utilizadores e o respeito e a promoção de sociedades democráticas abertas, racionais e transparentes. Sem prejuízo, esses mecanismos não podem ser de tal ordem que representem eles mesmos, por excesso de militância ou escrutínio, um ataque direto à democracia, ao Estado de Direito e aos direitos fundamentais. Antes, e porque a natureza transnacional e global destes riscos impede uma ação nacional, torna-se necessário alargar as nossas conceções para além daquilo que, tradicionalmente, constitui a ordem mundial, tendo em vista, por exemplo, um constitucionalismo global multinível, especialmente apto, na nossa ótica, na gestão do risco digital. Só através de modelos que vão além do Estado nação e das próprias regiões do globo, podem as forças políticas tradicionais sequer imaginar recuperar capacidades de ação que se encontram, hoje, nas mãos de um conjunto restrito de atores não estatais. Estar a favor do Estado de Direito significa, atualmente, ambicionar que as instituições políticas e o poder, onde quer que ele se encontre, esteja rigorosamente ao serviço da democracia, dos cidadãos e dos seus direitos fundamentais.

## BIBLIOGRAFIA

- AICHHOLZER, Georg; ROSE, Gloria - *Experience with Digital Tools in Different Types of e-Participation*. In HENNEN, L., KEULEN, I. V., KORTHAGEN, I., AICHHOLZER, G., LINDNER, R. & NIELSEN, R. K. *European E-Democracy in Practice*. [s.l.]: Springer, 2020.
- ALLCOTT, Hunt; GENTZKOW, Matthew - *Social Media and Fake News in the 2016 Election*. *Journal of Economic Perspectives*. Vol. 31. n.º 2 (2017). p. 211-236.
- ALMAGOR-COHEN, Raphael - *Internet History*. *International Journal of Technoethics*. n.º 2 (2011). p. 45-64.
- AMARAL, Inês; SANTOS, Sofia José - *Algoritmos e redes sociais: a propagação de fake news na era da pós-verdade*. In FIGUEIRA, J.; SANTOS, S. - *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Coimbra: Imprensa da Universidade de Coimbra, 2019.
- ANDERSON, Paul - *What is Web 2.0? Ideas, technologies and implications for education*. [s.l.]: JISC Technology and Standards Watch, 2007.
- ARENDT, Hannah - *Entre o Passado e o Futuro*. Lisboa: Relógio D'Água, 2006.
- BÁRD, Petra; BAYER, Judit - *A comparative analysis of media freedom and pluralism in the EU Member States*. Brussels: European Parliament 2016.
- BAUER, Matthias; ERIXON, Dredrik - *Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls*. [s.l.]: European Centre For International Political Economy, 2020.
- BAYER, Judit; BITIUKOAVA, Natalija; BÁRD, Petra; SZAKÁCS, Judit; ALEMANN, Alberto; USZKIEWICZ, Erik - *Disinformation and propaganda - impact on the functioning of the rule of law in the EU and its Member States*. Brussels: European Parliament, 2019.
- BECK, Ulrich - *Critical Theory of World Risk Society: A Cosmopolitan Vision*. *Constellations*. Vol. 16. n.º 1 (2009). 3-22.
- BECK, Ulrich - *Sociedade de risco mundial: em busca da segurança perdida*. Lisboa: EDIÇÕES 70, 2016.
- BENNETT, W. Lance; SEGERBERG, Alexandra - *The Logic of Connective Action: digital media and the personalization of contentious politics*. *Information, Communication & Society*. Vol. 15. n.º 5 (2012). p. 739-768.
- BINGHAM, Tom - *The Rule of Law*. London: Penguin Books Ltd, 2011.
- BLUM, Christian; ZUBER, Christina Isabel - *Liquid Democracy: Potentials, Problems, and Perspectives*. *The Journal of Political Philosophy*. Vol. 24. n.º 2 (2016). p. 162-182.
- BOSSETTA, Michael - *The Weaponization Of Social Media: Spear Phishing And Cyberattacks On Democracy*. *Journal of International Affairs*. Vol. 71. n.º 1.5 (2018). p. 97-106.
- BRADFORD, Anu - *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.
- BRADSHAW, Samantha; HOWARD, Philip N. - *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. The Computational Propaganda Project, 2018.
- CARRERA, Sergio; GUILD, Elspeth; HERNANZ, Nicholas - *The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU: Towards an EU Copenhagen Mechanism*. [s.l.]: Centre for European Policy Studies, 2013.
- CASTELLS, Manuel - *A Galáxia Internet - Reflexões sobre Internet, Negócios e Sociedade*. Lisboa: Fundação Calouste Gulbenkian, 2004.
- CASTELLS, Manuel - *A Era da Informação: Economia, Sociedade e Cultura*. 3.ª ed. Lisboa: Fundação Calouste Gulbenkian, 2007. Vol. I – A Sociedade em Rede.
- CASTELLS, Manuel - *A Era da Informação: Economia, Sociedade e Cultura*. 3.ª ed. Lisboa: Fundação Calouste Gulbenkian, 2014. Vol. III - O Fim do Milénio.
- CERF, Vinton G. - *Computer Networking: Global Infrastructure for the 21st Century*. [Em linha] [s.l.]: [s.n.], 1995. [Consult. 17/11/2019] Disponível em: [shorturl.at/dvDHT](http://shorturl.at/dvDHT)

CHEN, Adrian – *The Agency*. The New York Times. (02 junho 2015). Disponível em: <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>.

CHOUDHURY, Nupur - *World Wide Web and Its Journey from Web 1.0 to Web 4.0*. International Journal of Computer Science and Information Technologies. Vol. 5, n.º 6 (2014). 8096-8100.

COHEN, Joshua - *Deliberation and Democratic Legitimacy*. In BOHMAN, J.; REHG, W. - *Deliberative Democracy: Essays on Reason and Politics*. Massachusetts: The MIT Press, 1997.

CRAIG, Paul - *The Rule of Law*. [Em linha] London: House of Parliament, 2007. [Consult. 27/05/2020] Disponível em: [shorturl.at/kwD59](http://shorturl.at/kwD59)

DAHLBERG, Lincoln - *Cyberlibertarianism*. [s.l.]: Oxford University Press, 2017.

DAHLBERG, Lincoln; SIAPERA, Eugenia - *Introduction: Tracing Radical Democracy and the Internet*. In DAHLBERG, L. & SIAPERA, E. - *Radical Democracy and the Internet*. London: Palgrave Macmillan, 2007.

DAHLGREN, Peter - *Media, Knowledge and Trust: The Deepening Epistemic Crisis of Democracy*. Javnost - The Public. Vol. 15. n.º 1-2 (2018).

DUTTON, William H. - *The Fifth Estate Emerging through the Network of Networks*. Prometheus. Vol. 27. n.º 1 (2009). p. 1-15.

DWORKIN, Ronald - *Levando os direitos a sério*. São Paulo: Martins Fontes, 2002.

ENES, Graça – *Digital platforms and European Union Law – challenges from a perspective of multilevel constitutionalism*. UNIO – EU Law Journal, Vol. 5, n.º 1, 2019. 16-39.

ERNST, Nicole; ENGESSER, Sven; BÜCHEL, Florin; BLASSNIG, Sina; ESSER, Frank - *Extreme parties and populism: an analysis of Facebook and Twitter across six countries*. Information, Communication & Society. Vol. 20. n.º 9 (2017). p. 1347-1364.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH THE LAW (VENICE COMMISSION) - *Report on the Rule of Law*. Strasburg: Council of Europe, 2011.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – *Election Cybersecurity: challenges and opportunities*. [Em linha]. [s.l.]: ENISA, 2019. [Consult. 08/09/2020] Disponível em: <https://tinyurl.com/y62khddy>.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – *ENISA overview of cybersecurity and related terminology* [Em linha]. [s.l.]: ENISA, 2017. [Consult. 07/09/2020]. Disponível em: [shorturl.at/hsFQT](http://shorturl.at/hsFQT)

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY – *ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends*. [Em linha]. [s.l.]: ENISA, 2019. [Consult. 07/09/2020] Disponível em: <https://tinyurl.com/y48r2z2b>.

EUROPOL. EUROJUST – *Joint Report: Common challenges in combating cybercrime as identified by Eurojust and Europol* [Em linha]. [s.l.]: Europol and Eurojust Public Information, 2019. [Consult. 07/09/2020] Disponível em: [www.eurojust.europa.eu/doclibrary](http://www.eurojust.europa.eu/doclibrary).

EVANGELIDIS, Basil - *Landmarks in the History of Science: Great Scientific Discoveries from a Global-Historical Perspective*. Delaware: Vernon Press, 2019.

EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES – *NEW TECHNOLOGIES FORMATION - Liability for Artificial Intelligence and other emerging digital technologies*. [s.l.]: Publications Office of the European Union, 2019.

FERREE, Myra Marx; GAMSON, William A.; GERDHARDS, Jürgen; RUCHT, Dieter - *Four models of the public sphere in modern democracies*. Theory and Society. Vol. 31. (2002). p. 289-324.

FRANKENBERG, Günter - *Democracy*. In ROSENFELD, M.; SAJÓ, A. - *The Oxford Handbook of Comparative Constitutional Law*. Oxford: Oxford University Press, 2012.

GARNER, Oliver - *The Existential Crisis of Citizenship of the European Union: The Argument for an Autonomous Status*. Cambridge Yearbook of European Legal Studies. n.º 20 (2018). p. 116-146.

GILES, Keir - *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016.

- GORJÃO-HENRIQUES, Miguel - *Direito da União: história, direito, cidadania, mercado interno e concorrência*. 6.<sup>a</sup> ed. Coimbra: Almedina, 2010.
- GORWA, Robert; GUILBEAULT, Douglas - *Understanding Bots for Policy and Research: Challenges, Methods, and Solutions*. [Em linha] [s.l.]: [s.n.], 2018. [Consult. 09/06/2020]. Disponível em: <https://arxiv.org/pdf/1801.06863v1.pdf>.
- HABERMAS, Jürgen - *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Massachusetts: The MIT Press, 1991.
- HABERMAS, Jürgen - *The Postnational Constellation: political essays*. Massachusetts: The MIT Press, 2001.
- HABERMAS, Jürgen - *Um ensaio sobre a constituição da Europa*. Lisboa: Edições 70, 2012.
- HACKER, Kenneth L.; DIJK, Jan van - *What is Digital Democracy?*. In HACKER, K. L. & DIJK, J. V. - *Digital Democracy: Issues of theory and practice*. London: Sage, 2000.
- HEADRICK, DANIEL R. - *Technology: A World History*. New York: Oxford University Press, Inc., 2009.
- HELD, David - *Globalization and cosmopolitan democracy*. Peace Review. Vol. 9. n.º 3 (1997). p. 309-314.
- HENDRICKS, Vincent F.; VESTARGAARD, Mads - *Reality Lost: Markets of Attention, Misinformation and Manipulation*. [s.l.]: Springer, 2019.
- HENNEN, Leonhard - *E-Democracy and the European Public Sphere*. In HENNEN, L., KEULEN, I. V., KORTHAGEN, I., AICHHOLZER, G., LINDNER, R. & NIELSEN, R. O. - *European E-Democracy in Practice*. [s.l.]: Springer, 2020. p. 47-91.
- HIGH LEVEL GROUP ON FAKE NEWS AND ONLINE DISINFORMATION - *A multi-dimensional approach to disinformation*. Brussels: European Commission, 2018.
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE - *A definition of AI: Main capabilities and scientific disciplines*. Brussels: European Commission, 2019.
- HOUSE OF COMMONS. Digital, Culture, Media and Sport Committee. *Disinformation and 'fake news': Interim Report*. [Em linha] London: [s.n.], 2018. [Consult. 20/04/2020]. Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/363/363.pdf>
- HOUSE OF COMMONS. Digital, Culture, Media and Sport Committee. *Disinformation and 'fake news': Final Report*. [Em linha] London: [s.n.], 2019. [Consult. em 20/04/2020] Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmums/1791/1791.pdf>
- HOWARD, Philip N.; WOOLLEY, Samuel; CALO, Ryan - *Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration*. Journal of Information Technology & Politics. Vol. 15. n.º 2 (2018). p. 81-93.
- INTERNATIONAL TELECOMMUNICATION UNION - *Measuring digital development: Facts and figures*. Geneva: ITU Publications, 2019.
- JOERGES, Christian - *Unity in Diversity as Europe's Vocation and Conflicts Law as Europe's Constitutional Form*. [Em linha]. LEQS Papel No. 28/2010. [Consult. 20/09/2020] Disponível em: [shorturl.at/GHU06](http://shorturl.at/GHU06)
- JOWETT, Garth S.; O'DONNELL, Victoria - *Propaganda and persuasion*. 5<sup>a</sup> ed. Washington DC: SAGE, 2012.
- KARPPINEN, Kari - *European Public Spheres and the Challenge of Radical Pluralism*. In MORING-SALOVARA, I. - *Manufacturing Europe: Spaces of Democracy, Diversity and Communication*. Göteborg: NORDICOM, 2009.
- KEYES, Ralph - *The Post-Truth Era*. New York: St. Martin's Press, 2004.
- KING, Gary; PAN, Jennifer; ROBERTS, Margaret E. - *How Censorship in China Allows Government Criticism but Silences Collective Expression*. American Political Science Review. Vol. 107. (2013). p. 1-18

KLEIN, Andrés Ortega - *The view from Spain: The EU's bid for digital sovereignty*. In HOBBS, C. - *Europe's Digital Sovereignty: From Rulemaker To Superpower In The Age Of Us-China Rivalry*. [s.l.]: European Council on Foreign Relations, 2020.

KRANZBERG, Melvin - *Technology and History: "Kranzberg's Laws"*. *Technology and Culture*. Vol. 27. n.º 3 (1986). p. 544-560.

LAMBIOTTE, Renaud; KOSINSKI, Michal - *Tracking the Digital Footprints of Personality*. *Proceedings of the IEEE*. Vol. 102, n.º 12 (2014). p. 1934-1939.

LEWANDOWSKY, Stephan; ECKER, Ullrich; COOK, John - *Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era*. *Journal of Applied Research in Memory and Cognition*. Vol. 6. n.º 4 (2017). p. 353-369.

LEWIS, James. - *Economic Impact of Cybercrime – No Slowing Down*. McAfee: [s.l.], 2018.

LINDNER, Ralf; AICHHOLZER, Georg - *E-Democracy: Conceptual Foundations and Recent Trends*. In HENNEN, L., KEULEN, I. V., KORTHAGEN, I., AICHHOLZER, G., LINDNER, R. & NIELSEN, R. O. - *European E-Democracy in Practice*. [s.l.]: Springer, 2020.

LOEWENSTEIN, Karl - *Militant Democracy and Fundamental Rights, I*. *The American Political Science Review*. Vol. 31. n.º 3 (1937). p. 417-432.

LUHMANN, Niklas - *Risk: a sociological theory*. New York: Routledge, 2002.

LUKES, Steven - *Power: A Radical View*. 2.<sup>a</sup> ed. London: Palgrave Macmillan, 2005.

MADURO, Miguel Poiars - *Three Claims of Constitutional Pluralism*. In AVBELJ, Matej; KOMÁREK, J. - *Constitutional Pluralism in the European Union and Beyond*. London: Hart Publishing, 2012. p. 67-84.

MARTENS, Bertin; AGUIAR, Luis; HERRERA-GOMEZ, Estrella; MUELLER-LANGER, Frank - *The digital transformation of news media and the rise of disinformation and fake news*. Seville: European Commission, 2018.

MATHEW, Binny; GOYAL, Pawna; DUTT, Ritam; MUKHERJEE, Animesh - *Spread of Hate Speech in Online Social Media*. WebSci'19: Proceedings of the 10th ACM Conference on Web Science. (2019). p. 173-182.

MIRANDA, Jorge - *Manual de Direito Constitucional*. 4.<sup>a</sup> ed. (rev. e atual.) Coimbra: Coimbra Editora, 2008. Tomo IV – Direitos Fundamentais.

MITTELSTADT, Brent - *Auditing for Transparency in Content Personalization Systems*. *International Journal of Communication*. Vol. 10. (2016). p. 4991-5002.

MOLLEN, Anne; DHAENENS, Frederik - *The Co-option of Audience Data and User-Generated Content: Empowerment and Exploitation Amidst Algorithms, Produsage and Crowdsourcing*. In DAS, R. & YTRE-ARNE, B. - *The Future of Audiences: A Foresight Analysis of Interfaces and Engagement*. [s.l.]: Palgrave Macmillan, 2018.

MOORE, Martin - *Tech Giants and Civic Power*. London: Centre for the Study of Media, Communication and Power of The Policy Institute at King's College London, 2016.

MÖRÄ, Tuomo - *The European Union and Ideals of the Public Sphere*. In MORING-SALOVAARA, I. - *Manufacturing Europe: Spaces of Democracy, Diversity and Communication*. Göteborg: NORDICOM, 2009.

MOROZOV, Evgeny - *The internet is a tyrant's friend*. *NewScientist*. (02 março 2011). Disponível em <https://www.newscientist.com/article/mg20928026-100-the-internet-is-a-tyrants-friend/>.

MOROZOV, Evgeny - *The Net Delusion: how not to liberate the world*. London: Penguin Books, 2011.

MURTHY, Dhiraj; POWELL, Alison B.; TINATI, Ramine; ANSTEAD, Nick; CARR, Leslie; HALFORD, Susan J. ; WAL, Mark - *Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital*. *International Journal of Communication*. Vol. 10. (2016). p. 4952-4971.

NEUDERT, Lisa Maria; MARCHAL, Nahema - *Polarisation and the use of technology in political campaigns and communication*. Brussels: European Parliamentary Research Service, 2019.

- NIELSEN, Rasmus Kleis - *Reuters Institute Digital News Report 2020*. [s.l.]: Reuters Institute for the Study of Journalism, 2020.
- NOVECK, Beth Simone - *Wiki government: how technology can make government better, democracy stronger, and citizens more powerful*. Washington, D.C.: Brooking Institution Press, 2009.
- NYAN, Brendan; REIFLER, Jason - *When Corrections Fail: The Persistence of Political Misperceptions*. Polit Behav. Vol. 32. n.º 2 (2010). p. 303-330.
- ONYEJI, Ijeoma; BAZILIAN, Morgan; BRONK, Chris - *Cyber Security and Critical Energy Infrastructure*. The Electricity Journal. Vol. 27. n.º 2 (2014). p. 52-60.
- PAUL, Christopher; MATTHEWS, Miriam - *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND Corporation, 2016.
- PECH, Laurent - *The Rule of Law as a Constitutional Principle of the European Union*. New York: NYU School of Law, 2009.
- PECH, Laurent - *Rule of Law as a Guiding Principle of the European Union's External Action*. Hague: Centre for the Law of EU External Relations, 2012.
- PERNICE, Ingolf - *Multilevel Constitutionalism and the Crisis of Democracy in Europe*. European Constitutional Law Review. Vol. 11. (2015). p. 547.
- PERNICE, Ingolf - *Global cybersecurity governance: A constitutionalist analysis*. Global Constitutionalism. Vol. 7. n.º 1 (2018). p. 112-141.
- PERNICE, Ingolf - *Risk management in the digital constellation - a constitutional perspective (part I)*. Revista D'Internet, Dret i Política. n.º 26 (2018). 83-94.
- PERNICE, Ingolf - *Risk management in the digital constellation - a constitutional perspective (parte II)*. Revista D'Internet, Dret i Política. n.º 27 (2018). p. 79-95.
- PLÍNIO, O VELHO; BOSTOCK, John; RILEY, Henry T; MAYHOFF, Karl Friedrich Theodor - *Pliny the Elder, The Natural History*.
- PRIOR, Helder - *Em nome do povo: populismo e o novo ecossistema mediático*. In FIGUEIRA, J.; SANTOS, S. - *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Coimbra: Imprensa da Universidade de Coimbra, 2019.
- PUDDEPHATT, Andrew - *Governing the internet: The makings of an EU model*. In HOBBS, C. - *Europe's Digital Sovereignty: From Rulemaker To Superpower In The Age Of Us-China Rivalry*. [s.l.]: European Council on Foreign Relations, 2020.
- QUADROS, Fausto de - *Direito da União Europeia: direito constitucional e administrativo da União Europeia*. Coimbra: Almedina, 2004.
- RASMUSSEN, Terje - *Internet-based media, Europe and the political public sphere*. Media, Culture & Society. Vol. 35. n.º 1 (2013). p. 97-104.
- RAWLS, John - *The Idea of Public Reason Revisited*. The University Of Chicago Law Review. Vol. 64. n.º 3 (1997). p. 765-807.
- RINI, Regina - *Fake news and partisan epistemology*. Kennedy Institute of Ethics Journal. Vol. 2. n.º 2 (2017). p. 43-64.
- ROCHLIN, Nick - *Fake news: belief in post-truth*. Library Hi Tech. Vol. 35. n.º 3 (2017). p. 386-392.
- RUDMAN, Riaan; BRUWER, Rikus - *Defining Web 3.0: opportunities and challenges*. The Electronic Library. Vol. 34. n.º 1 (2016). p. 132-154.
- SÁ, Alexandre Franco de - *Pré-verdade, verdade e pós-verdade: um percurso rumo à política contemporânea*. In FIGUEIRA, J.; SANTOS, S. - *As fake news e a nova ordem (des)informativa na era da pós-verdade*. Coimbra: Imprensa da Universidade de Coimbra, 2019. p. 101-122.
- SCANNELL, Josh - *What Can an Algorithm Do?* DISMAGAZINE. [Em linha] [sn.]: [sl.], 2015. [Consult. 12/08/2020] Disponível em: <http://dismagazine.com/discussion/72975/josh-scannell-what-can-an-algorithm-do/>
- SHAHIN, Jamal - *A European history of the Internet*. Science and Public Policy. Vol. 33. n.º 9 (2006). 681-693

SHOREY, Samantha; HOWARD, Philip N. - *Automation, Big Data, and Politics: A Research Review*. International Journal of Communication. Vol. 10. (2016). p. 5032-5055.

SILVEIRA, Alexandra; FROUFE, Pedro - Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. UNIO - EU Law Journal. Vol. 4. n.º 2 (2018). p. 4-20.

STEHLLING, Miriam; VESNIC-ALUJEVIC, Lucia; JORGE, Ana; MARÔPO, Lidia - *The Co-option of Audience Data and User-Generated Content: Empowerment and Exploitation Amidst Algorithms, Producers and Crowdsourcing*. In DAS, R. & YTRE-ARNE, B. - *The Future of Audiences: A Foresight Analysis of Interfaces and Engagement*. [s.l.]: Palgrave Macmillan, 2018.

STREITFELD, David - *The Internet Is Broken*. The New York Times. (20 Mai. 2017). [Consult. em 08/03/2020]. Disponível em: <https://www.nytimes.com/2017/05/20/technology/evan-williams-medium-twitter-internet.html>.

TAMBINI, Damian - *How advertising fuels fake news*. Media@LSE blog. [Em linha] (2017). [Consult. 09/03/2020] Disponível em: [shorturl.at/qLPVZ](http://shorturl.at/qLPVZ)

TUORI, Kaarlo – *The Many Constitutions of Europe*. [Em linha] Oxford: Oxford University Press, 2016. [Consult. 12/09/2020] Disponível em: [shorturl.at/pE238](http://shorturl.at/pE238).

UNITED NATIONS – *E-Government Survey 2016. E-Government in Support of Sustainable Development*. New York: United Nations, 2016.

VERONESE, Alexandre; SILVEIRA, Alexandra; LEMOS, Amanda Nunes Lopes Espiñeira - Artificial intelligence, Digital Single Market and the proposal of a right to fair and reasonable inferences: a legal issue between ethics and techniques. UNIO - EU Law Journal. Vol. 5. n.º 2 (2019). p. 75-91.

VESNIC-ALUJEVIC, Lucia; STOERMER, Eckhard; RUDKIN, Jennifer-Ellen; SCAPOLO, Fabiana; KIMBELL, Lucy - *The Future of Government 2030+: A Citizen-Centric Perspective on New Government Models*. Luxemburgo: Publications Office of the European Union, 2019.

VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan - *The spread of true and false news online*. Science. Vol. 359. n.º 6380 (2018). p. 1146-1151.

WALKER, Neil - *Taking Constitutionalism Beyond the State*. Political Studies. Vol. 56. n.º 3 (2008). p. 519-543.

WALKER, Neil – *Multilevel Constitutionalism: Looking Beyond the German Debate*. [Em linha] LEQS Paper No. 08/2009. [Consult. 12/09/2020] Disponível em: [shorturl.at/chAB5](http://shorturl.at/chAB5)

WARDLE, Claire - *Fake news. It's complicated*. First Draft. [Em linha] [Consult. em 12/03/2020]. Disponível em: <https://firstdraftnews.org/latest/fake-news-complicated/>

WARDLE, Claire; DERAKHSHAN, Hossein - *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Strasbourg: Council of Europe, 2017.

WEILER, Joseph H. H. – *Does Europe Need a Constitution? Demos, Telos and the German Maastricht Decision*. European Law Journal. Vol. 1. n.º 3 (1995). p. 219-258.

WILLIAMS, Robin; EDGE, David - *The Social Shaping of Technology*. Research Policy. Vol. 25. (1996). p. 856-899.

WOOD, Thomas; PORTER, Ethan - *The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence*. Polit Behav. Vol. 41. (2018). p. 135-163.

WORLD ECONOMIC FORUM - *Global Risks 2013*. 18.ª ed. Geneva: World Economic Forum, 2013. Consult. em 09/02/2020. Disponível em: [shorturl.at/rEO49](http://shorturl.at/rEO49)

ZILLER, Jacques - *The Nature of European Union Law*. In PÉREZ, J. M. B., GONZÁLEZ-ORÚS, J. M. & ATIENZA, B. B. Tratado de derecho y políticas de la Unión Europea. 2011. Vol. IV.

ZUBOFF, Shoshana - *The Age of Surveillance Capitalism: The Fight for Humana Future and The New Frontier of Power*. London: Profile Books, 2019.

ZUCKERMAN, Ethan - *New Media, New Civics?*. Policy and Internet. Vol. 6. n.º 2 (2014). p. 151-168.

ZÜRN, Michael - *A Theory of Global Governance: Authority, Legitimacy and Contestation*. Oxford: Oxford University Press, 2018.