REVISTA DE DIREITO INTERNACIONAL

BRAZILIAN JOURNAL OF INTERNATIONAL LAW

Editores responsáveis por essa edição:

Editores:

Nitish Monebhurrun

Ardyllis Alves Soares

Marcelo Dias Varella

Editora assistente

Naiara Cardoso Gomide da Costa Alamy

Editores convidados:

Fábia Fernandes Carvalho

George Galindo

João Roriz

ISSN 2237-1036

Revista de Direito Internacional Brazilian Journal of International Law	Brasília	v. 19	n. 3	p. 1-447	dez	2022

doi: 10.5102/rdi.v19i3.8434

A construção da cibersoberania na União Europeia: a cibersegurança e a integração do ciberespaço europeu*

Building the cybersovereignty in the European Union: cybersecurity in the integration of European cyberspace

Leonardo Rafael de Souza**

Cinthia Obladen de Almendra Freitas***

Resumo

No presente estudo, descritivo e analítico, estruturado sobre o método dedutivo, com base em levantamento bibliográfico e documental, analisou-se como o evolutivo rol de ações e estratégias em cibersegurança — no âmbito do ciberespaço europeu — tem levado a União Europeia à construção de uma cibersoberania compartilhada entre União e Estados-Membros, problemática que repensa como o ambiente digital poderá, novamente, trazer as premissas apresentadas pelo Tratado de Maastricht. Reflete-se, inicialmente, sobre como a atual tutela do ciberespaço se constitui como a nova razão de ser da União Europeia para, na sequência, avaliar de que forma a construção de uma nova soberania digital pode ocorrer no contexto do ciberespaço, destacando o papel fundamental que a cibersegurança tem alcançado como eixo de integração entre os Estados-Membros. Ao término, descrevem-se as novas ações e estratégias de cibersegurança que estruturam o plano de meta da União Europeia, chamado "Um Futuro Digital para a Europa". Como conclusão, as ações mais recentes no contexto europeu revelam que a cibersegurança está no centro das discussões sobre o desenvolvimento do ciberespaço, o que poderá levar a Europa a, novamente, tentar alcançar o seu desejado constitucionalismo multinível, porém, atualmente, em meio digital, de uma cibersoberania compartilhada e integrada para um ciberconsitucionalismo europeu.

Palavras-chave: sociedade informacional; Estado; cibersoberania; União Europeia; constitucionalismo.

Abstract

Structured on the deductive method from a bibliographical and documental review, this descriptive and analytical study analyzes how the increasingly expanded cybersecurity strategies within the European cyberspace has led the European Union to the construction of a shared cybersovereignty between the Union and Member States, problematic that rethinks how the digital context could renew the premises of the Maastricht Treaty. The article ini-

* Recebido em 05/04/2022
Aprovado em 13/10/2022

** Doutorando em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR), Brasil, com estágio de doutoramento no Laboratório de Segurança Informática e do Cibercrime (Lab UbiNET) do Instituto Politécnico de Beja (IPBeja), Portugal. Pesquisador bolsista no Programa de Mestrado e Doutorado Acadêmico para Inovação (MAI/DAI) do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), no Ministério da Ciência, Tecnologia, Inovações e Comunicações do Brasil.
Email: leonardo.rafael@pucpr.edu.br

*** Professora Titular e Coordenadora do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná (PUCPR), Brasil. Doutora em Informática pela Pontifícia Universidade Católica do Paraná (PUCPR).
Email: cinthia.freitas@pucpr.br

tially reflects on how the current protection of cyberspace constitutes the new *raison d'être* of the European Union to, subsequently, evaluate how the construction of a new digital sovereignty can occur in the context of cyberspace, highlighting the fundamental role that cybersecurity has achieved as an axis of integration between Member States. At the end, the new cybersecurity actions and strategies that structure the European Union's goal plan called "A Digital Future for Europe." In conclusion, the most recent actions in the European context have shown that cybersecurity is at the center of discussions on the development of cyberspace, which could lead Europe to once again try to promote its multilevel constitutionalism, but now digital, of a shared cybersovereignty and integrated for a European cyber-constitutionalism.

Keywords: information society; State; cyber sovereignty; European Union; constitutionalism.

1 Introdução

O avanço das tecnologias da informação e comunicação (TICs) e a consequente consolidação de um ciberespaço global, atualmente disseminado pela Internet e acelerado pelas experiências da Covid-19 sobre a integração remota dos indivíduos e sociedades, levaram os vários países a também refletirem sobre a sua soberania em meio digital numa realidade essencialmente transnacional e transfronteiriça. No contexto europeu, essa reflexão, embora melhor compreendida a partir da realidade multilateral da União Europeia, parece igualmente complexa na medida em que a própria razão de ser do bloco evoluiu para um complexo e ambicioso projeto de fortalecimento do papel econômico e político da Europa no sistema geopolítico mundial que supera, sem desconsiderá-la, a iniciativa original de paz e prosperidade dos seus Estados-Membros no ambiente pós-guerras.

Todavia, essa complexidade se mostrou mais desafiadora para uma ideia de plena integração quando, na busca pela defesa das Comunidades Europeias como desejado e proposto no Tratado de Maastricht de 1992, o bloco europeu enfrentou resistências às lógicas propostas de cooperação e integração de distintas soberanias, levando alguns de seus Estados-Membros a refutarem a fundante ideia de um constitucionalismo multinível estruturado na construção de uma cidadania e soberania europeias, transnacionais e de bases democráticas.

Mas, com o advento da Era Digital, notadamente em torno da tutela do ciberespaço, a discussão sobre a complementação da soberania tradicional (física, analógica) por uma soberania supranacional em meio digital trouxe nova centralidade à experiência europeia. Isso porque, com os avanços experimentados na Europa desde o Tratado de Lisboa de 2007, a integração do bloco, por meio do compartilhamento de competências entre Estados e União, passou a ser considerada como um diferencial na compreensão legal e política do ciberespaço, ambiente imaterial necessariamente transfronteiriço e integrativo. Outrossim, a construção dessa integração, baseada na confiança e na segurança dos cidadãos, organizações, mercado e Estados trouxe, para o centro das discussões, a cibersegurança, entendida como o conjunto de precauções e ações utilizadas para proteger o ciberespaço de ameaças.

Considerando-se esse contexto, o estudo tem caráter analítico e descritivo, estruturado com base no método dedutivo e no levantamento bibliográfico e documental, e analisa como o cada vez mais ampliado rol de ações e estratégias em cibersegurança, no âmbito do ciberespaço europeu, tem levado a União Europeia à construção de uma cibersoberania compartilhada entre União e Estados-Membros, repensando, assim, como o meio digital poderá, novamente, trazer as premissas apresentadas pelo Tratado de Maastricht e consolidada pelo Tratado de Lisboa. O artigo é resultado de estudos realizados no âmbito de projeto de pesquisa com financiamento do Programa de Mestrado e Doutorado Acadêmico para Inovação MAI/DAI do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq / NAI-DAI CP nº 12/2020) do Ministério da Ciência, Tecnologia, Inovações e Comunicações do Brasil (MCTIC), com integração de pesquisa entre a Pontifícia Universidade Católica do Paraná (PUCPR) e o Laboratório de Segurança Informática e Cibercrime (Lab UbiNET) do Instituto Politécnico de Beja (IPBeja - Portugal).

O artigo busca em seu primeiro tópico demonstrar como a tutela do ciberespaço vem se constituindo na nova *raison d'être* — admitindo aqui o termo como apresentada por Graínne De Burca — da União Europeia na Era da Informação. Em um segundo momento, avalia-se como a construção de uma nova soberania em meio digital pode ocorrer no contexto do ciberespaço, desta-

cando o papel fundamental que a cibersegurança vem alcançando na União Europeia como eixo de integração entre os Estados-Membros. Por fim, o artigo se dedica a descrever as novas ações e estratégias de cibersegurança que estruturam o plano de meta da União Europeia chamado "Um Futuro Digital para a Europa", bem como descreve como a Agência de Defesa Europeia (ADE) e Agência da União Europeia para a Cibersegurança (ENISA) têm fortemente atuado não apenas entre os Estados-Membros no atual ambiente de guerra, mas também nas organizações e empresas para fortalecer a confiança na economia digital e reforçar a resiliência das infraestruturas críticas dos Estado-Membros e os seus cidadãos seguros no plano digital.

Em conclusão, ainda que a tutela do ciberespaço na União Europeia esteja centrada no estabelecimento de leis e políticas comuns à União e seus Estados-Membros, iniciativas como o plano "Um Futuro Digital para a Europa", que inclui ações para uma Década Digital, e o fortalecimento da Agência da União Europeia para a Cibersegurança (ENISA), mostram-se como importantes frentes multidirecionais que dão à cibersegurança a necessária centralidade para o desenvolvimento do ciberespaço europeu. Se assim avançar, a Europa poderá ter uma nova oportunidade de alcançar o seu outrora desejado constitucionalismo multinível, porém a partir da construção de uma cibersoberania compartilhada e integrada que concilie as propostas fundadoras da União Europeia com a natureza supranacional e transfronteiriça do ciberespaço.

2 A tutela do ciberespaço como *raison d'être* da União Europeia na Era da Informação

Ao discutir a razão de ser (*raison d'être*) da União Europeia, Gráinne De Búrca assevera que, para além de um então projeto-piloto de integração econômica, voltado para a busca da paz e da prosperidade nos seus Estados-Membros, especialmente a partir da lógica do pós-guerra, a integração dos países europeus em torno da União Europeia (UE) evoluiu para um mais complexo e ambicioso projeto de fortalecimento do papel econômico e político da Europa no ambiente global. Isso, na prática atual — e sem desconsiderar a importância dos objetivos originais —, acabou por se traduzir na busca de um sistema político relativamente unificado que tem como razão reagir à influência de, e influenciar, outras potências globais.[1]

Em outros termos, apesar da constante luta econômica e das tensões constitucionais ocorridas entre os países da União Europeia, os fundamentos da articulação, ainda hoje defendidos na Europa, estão numa dupla razão de articulação que se complementam: o fortalecimento de uma relação transnacional entre UE, Estados-Membros e seus cidadãos; e o desenvolvimento de uma relevância global que considere, efetivamente, o papel da União Europeia no contexto global em constante transformação.[2]

Essa percepção parece atualizar os fundamentos da União Europeia como apresentados em seu tratado base, o Tratado de Maastricht ou Tratado da União Europeia (TUE), os quais estão estruturados sobre a defesa das Comunidades Europeias em cooperação tanto para o seu pleno desenvolvimento econômico e social — propostos pelo ideal de Justiça e pela integração dos seus povos e assuntos internos — quanto para a proposição de políticas externas e de segurança comuns que amplifiquem a soberania e as possibilidades dos seus Estados-Membros. E, para a instrumentalização desses fundamentos, o referido Tratado, em seu artigo 2º, apresenta distintos objetivos como "a manutenção e o desenvolvimento da União enquanto espaço de liberdade, de segurança e de justiça", exercidos a partir da livre circulação de pessoas e/ou por medidas de prevenção e combate à criminalidade. Assim, confirmados os direitos sociais fundamentais da Carta Social Europeia de 1961.[3]

Portanto, a proposta de um sistema político relativamente unificado em reação à influência de outras potências globais pode ser compreendida, também, a partir da proposta comunitária de estabelecimento de uma política externa e de segurança comum, o que, na visão de

[1] BURCA, Gráinne de. Europe's raison d'être. *In:* KOCHENOV, Dimitry; AMTENBRINK, Fabian (ed.). *The European Union's shaping of the international legal order.* Cambridge: Cambridge University Press, 2014. p. 21-37. p. 21.

[2] BURCA, Gráinne de. Europe's raison d'être. *In:* KOCHENOV, Dimitry; AMTENBRINK, Fabian (ed.). *The European Union's shaping of the international legal order.* Cambridge: Cambridge University Press, 2014. p. 21-37. p. 31.

[3] PARLAMENTO EUROPEU. *Tratado da União Europeia (TUE).* 2021. Disponível em: https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/maastricht-treaty. Acesso em: 12 nov. 2021.

Vasco Vieira, pode ser entendido também sob a ótica de partilha da soberania. Na sua proposta, "os diversos Estados nacionais europeus articulam os seus poderes e os seus recursos de modo a formar um poder superior ao que qualquer Estado isolado teria possibilidade de conseguir."[4]

A estruturação da União Europeia se consolida com base na sua experiência de coordenar, internamente, os diferentes interesses dos Estados, sem ataque às suas respectivas soberanias nacionais, com vista a resolver problemas comuns. A questão central, no entanto, é que, cada vez mais, o bloco europeu tem procurado discutir temas (nem sempre tão comunitários) que a ratifiquem como um importante ator global, tal qual ocorre nas discussões sobre as alterações climáticas e a promoção da democracia, por exemplo. A questão é que o diferencial proposto pela União Europeia nesse contexto está na busca de soluções coletivas, coordenadas e multilaterais para problemas globais, o que não acontece quando enfrentados individualmente por grandes nações.[5]

Nesse aspecto, o novo paradigma econômico-social causado pelo signo digital, a partir da difusão da Internet já nos anos de 1990, atualmente entendido como a Quarta Revolução Industrial[6], trouxe, para a União Europeia, a percepção inicial de que, para o avanço do seu mercado no meio digital, a confiança nos produtos e serviços fornecidos na rede mundial de computadores, somada ao constante desenvolvimento de Tecnologias da Informação e Comunicação (TICs), seria fundamental para o desenvolvimento de políticas internas e externas voltadas ao crescimento e fortalecimento econômico do bloco[7], porém atualmente considerando a Era da Infomação, como definido por Manuel Castells. Nela a força e a influência da Europa estariam também ligadas à compreensão multilateral das transformações econômicas causadas pela centralidade da informação, potencializada pelo avanço das TICs conectadas à Internet. Isso é fundamental porque a compreensão sobre o processamento e a transmissão da informação não somente altera as formas de exercer o poder, mas redimensionam a própria relação entre Estado(s) e sociedade(s).[8]

Assim, a busca pela compreensão do ciberespaço passou a dominar também o contexto de análise desde uma perspectiva europeia. Segundo Pierre Lévy, o termo "ciberespaço" teve como origem a descrição de um espaço desterritorializado na obra de ficção científica de William Gibson intitulada "Neuromancer"[9]. Atualmente, o ciberespaço é compreendido como um espaço não material, portanto sem limitações geográficas, "composto por redes de computadores, telecomunicações, programas, interfaces e banco de dados em que as experiências se desmaterializam e passam a concretizar-se em bits."[10] Quer dizer, o ciberespaço é uma projeção do mundo real para uma realidade de interações virtuais, ou o contrário, marcada por uma não espacialidade que permite novas interações humanas, sociais e econômicas para além dos territórios físicos, incluindo os Estados como inicialmente imaginados, e nos quais "podemos movimentar, trabalhar, construir, criar, investir."[11] O ciberespaço, então, assim compreendido possui as características de imaterialidade, despersonalização, desterritorialização e atemporalidade.

Pela compreensão inicial do ciberespaço como um domínio comum e global inserido no ambiente informacional, muitos pensadores levaram a comparar a sua totalidade a algo imune de apropriação, o alto mar, o espaço aéreo internacional ou até mesmo a órbita espacial.[12] Para Pierre Lévy, por exemplo, o ciberespaço, desde uma proposição original, estaria essencialmente estruturado sobre uma base de afinidades sociais e econômicas na qual "a geografia, contingente, não é mais um ponto de partida, nem uma coerção."[13]

Essas novas formas de interação em rede trouxeram como resultado a igualmente relevante transformação dos riscos e da criminalidade para a realidade informa-

[4] VIEIRA, Vasco Rocha. A União Europeia de Maastricht a Nice: uma reflexão sobre o futuro. *Nação e Defesa,* v. 2, n. 100, p. 37-49, 2001. p. 41.

[5] BURCA, Gráinne de. Europe's raison d'être. *In:* KOCHENOV, Dimitry; AMTENBRINK, Fabian (ed.). *The European Union's shaping of the international legal order.* Cambridge: Cambridge University Press, 2014. p. 21-37. p. 36-37.

[6] SCHWAB, Klaus. *A quarta revolução industrial.* São Paulo: Edipro, 2016. p. 15-16.

[7] CHRISTOU, George. The EU's approach to cybersecurity. *University of Essex Paper Series*, 2017. p. 1-2.

[8] CASTELLS, Manuel. *A era da informação:* economia, sociedade e cultura. São Paulo: Paz e Terra, 2020.

[9] LÈVY, Pierre. *O que é virtual?* São Paulo: Ed. 34, 1996. p. 20.

[10] MAIAS, André; BRAVO, Rogério. *Geopolítica, geoestratégia e ciberespaço.* Lisboa: Academia, 2010. p. 3.

[11] MAIAS, André; BRAVO, Rogério. *Geopolítica, geoestratégia e ciberespaço.* Lisboa: Academia, 2010. p. 14.

[12] VON HEINEGG, Wolff Heintschel. Territorial sovereignty and neutrality in cyberspace. *International Law Studies US Naval War College*, v. 89, n. 1, p. 127-156, 2013. p. 125.

[13] LÈVY, Pierre. *O que é virtual?* São Paulo: Ed. 34, 1996. p. 21.

cional[14], ambos refletidos no aumento exponencial de ataques cibernéticos a indivíduos, empresas, Estados e infraestruturas críticas no ciberespaço desde o início dos anos 2000. Isso fez com que a visão, até então essencialmente econômica, de integração das novas tecnologias na União Europeia, passasse a ser refletida também sob a necessária confiança social nas tecnologias enquanto uma nova forma de compreensão de segurança comum no ambiente europeu, como pensado no Tratado de Maastricht. Em simples palavras, observou-se a profusão de debates voltados à reflexão sobre a adoção de políticas de cooperação e a garantia da segurança cibernética do ciberespaço desde uma perspectiva europeia.[15]

Isso porque, embora a noção de não espacialidade do ciberespaço torne difícil perceber e/ou gerenciar com precisão as suas mais diversas interações, há de se considerar que o mesmo não pode existir sem o apoio do mundo físico.[16] Quer dizer, a compreensão do ciberespaço não está, unicamente, ligada à lógica da realidade virtual, essencialmente digital, mas pode ser considerada, também, por meio das estruturas físicas que formam as suas vias de comunicação, formas estáticas cujo acesso "só é possível se se disponibilizar *hardware* (computadores, teclado, sinal, monitores) e *software* (programas, drives)."[17]

Assim, por requererem uma arquitetura física para existir, serem de propriedade de indivíduos, empresas e governos e estarem pelo menos ligado a alguma rede elétrica nacional, os componentes do ciberespaço não estão imunes à tutela de um determinado Estado. O exercício da jurisdição estatal sobre determinada infraestrutura cibernética, então, passou a ser determinada a partir da sua localização territorial, física, geográfica.[18] Mas, inclusive, em razão dessas estruturas estarem localizadas e serem mais facilmente desenvolvidas globalmente, a noção de integração pela segurança comum foi apresentada pelo Conselho da União Europeia como uma solução lógica e eficiente dado que o ciberespaço e as suas ameaças, assim como suas infraestruturas, não estão limitados pelas fronteiras nacionais, precisando, então, de uma ação integrada para melhor garantir a segurança cibernética.[19]

Por meio da Decisão-Quadro 2005/222, de 24 de fevereiro, e considerando-se o objetivo de garantir liberdade e segurança aos seus cidadãos pela adoção de ações comuns entre os Estados-Membros no domínio da cooperação policial e judiciária em matéria penal (artigo 29 do Tratado de Maastricht), o Conselho da União Europeia se propôs a, efetivamente, tutelar o ciberespaço desde o contexto de qualquer país do bloco em face de possíveis ataques contra os sistemas de informação localizados em seu território. E, para isso, a norma definiu tais sistemas estruturantes do ciberespaço (artigo 1º, a) como

> qualquer dispositivo ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, protecção e manutenção.[20]

Importante ponderar que, dentre as justificações para adotar a referida Decisão-Quadro, o Conselho da União Europeia considerou a crescente inquietação, já global à época, de possíveis ataques terroristas contra sistemas de informação que ameaçassem estruturas vitais dos Estados-Membros, o que poderia "comprometer a instauração de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia."[21] Como se percebe, propôs-se uma

[14] VIRGA, Joy Marie. International criminals and their virtual currencies: the need for an international effort in regulating virtual currencies and combating cyber crime. *Revista de Direito Internacional*, Brasília, v. 12, n. 2, p. 511-526, 2015. p. 515-518.

[15] CARRAPICO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. *European Politics and Society,* v. 19, n. 3, p. 299-303, 2018. p. 299-300.

[16] SHEN, Yi. Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, v. 1, n. 1, p. 81-93, 2016.

[17] MAIAS, André; BRAVO, Rogério. *Geopolítica, geoestratégia e ciberespaço.* Lisboa: Academia, 2010. p. 6.

[18] VON HEINEGG, Wolff Heintschel. Territorial sovereignty and neutrality in cyberspace. *International Law Studies US Naval War College*, v. 89, n. 1, p. 127-156, 2013. p. 125.

[19] CARRAPICO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. *European Politics and Society,* v. 19, n. 3, p. 299-303, 2018. p. 299.

[20] CONSELHO DA UNIÃO EUROPEIA. *Decisão-Quadro n.º 205/222, de 24 de fevereiro de 2005*. Relativa a ataques contra os sistemas de informação. Bruxelas, 2005. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32005F0222&from=PT. Acesso em: 13 nov. 2021.

[21] CONSELHO DA UNIÃO EUROPEIA. *Decisão-Quadro n.º 205/222, de 24 de fevereiro de 2005*. Relativa a ataques contra os sistemas de informação. Bruxelas, 2005. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32005F0222&from=PT. Acesso em: 13 nov. 2021.

efetiva e integrada reação a demandas pensadas desde o contexto global.[22]

Não obstante isso, tem-se de concreto que a Decisão-Quadro de 2005, complementar à proposta inicial da Agência da União Europeia para a Cibersegurança (ENISA), criada no ano anterior, se mostrou como uma iniciativa relevante na tutela do ciberespaço por propor um ambiente europeu de partilha de conhecimento voltado à segurança digital dos Estados-Membros e seus cidadãos.[23] Ademais, tal iniciativa foi igualmente importante por reconhecer, de forma expressa[24], que os sistemas de informação — estruturantes à compreensão do ciberespaço — possuem uma natureza transnacional que evidencia a necessidade de estratégias transfronteiriças que facilitem a integração da União Europeia.

Ocorre que, apesar do reconhecimento dessa transnacionalidade, a tutela do ciberespaço passa pela compreensão de que a sua imaterialidade leva ao rompimento das fronteiras físicas que marcam os limites políticos e identitários de uma nação, espaços até então físicos, geográficos, nos quais a noção de soberania era bem compreendida desde a Paz de Westfália. E, na realidade europeia, compreender os limites da tutela do ciberespaço passa pela compreensão do próprio compartilhamento de soberania já proposto pelo bloco desde a sua criação até a proposição de um constitucionalismo multinível, cuja não implementação culminou com o Tratado do Lisboa. Além disso, é basilar compreender como a cibersegurança estabelece, no ambiente global, os eixos de segurança cibernética que orientam a proteção do ciberespaço também no ambiente europeu.

3 A soberania no ciberespaço europeu e o papel da cibersegurança para a integração dos países membros

Desde a sua concepção no Tratado de Maastricht, a União Europeia restou consolidada como uma comunidade de leis e valores em que o Estado de Direito, assentado nas premissas democráticas, aproximou os países a uma concepção política de valores constitucionais.[25] Isso porque, além de estabelecer os fundamentos necessários para uma lógica de desenvolvimento econômico, social, ambiental e político, Maastricht também instituiu a cidadania europeia comprometida com os direitos humanos desde de uma perspectiva funcionalmente constitucional. Quer dizer, consagrou-se na Europa a tentativa de superação das estruturas políticas nacionais tradicionais[26] para a concepção de um marco na busca por um constitucionalismo multinível que reconhecesse uma nova interpretação sobre a soberania.[27]

O constitucionalismo multinível proposto na União Europeia seria compreendido como um novo modelo constitucional que considerava não apenas determinado sistema constitucional nacional dentro do bloco, mas também um constitucionalismo de nível supranacional que estabeleceria um novo poder político legítimo. Entre esses sistemas constitucionais, porém, haveria uma integração por meio da influência recíproca e do estabelecimento de novas relações integradas que passariam a considerar também o contexto europeu, como a cidadania e a soberania.[28]

[22] Sobre o tema, também a leitura do Considerando 7 da Decisão-Quadro dá a exata noção dessa relevância global no combate ao ciberterrorismo: é necessário completar o trabalho realizado pelas organizações internacionais, especialmente ao nível do Conselho da Europa, no domínio da aproximação do direito penal e os trabalhos do G8 sobre cooperação transnacional no âmbito da criminalidade de alta tecnologia, propondo uma abordagem comum neste domínio ao nível da União Europeia. Este pedido foi desenvolvido na Comunicação que a Comissão dirigiu ao Conselho, ao Parlamento Europeu, ao Comité Económico reforçando a segurança das infraestruturas da informação e lutando contra a cibercriminalidade.

[23] CARRAPICO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. *European Politics and Society,* v. 19, n. 3, p. 299-303, 2018. p. 299.

[24] Vide Considerando 5 do CONSELHO DA UNIÃO EUROPEIA. *Decisão-Quadro n.º 205/222, de 24 de fevereiro de 2005*. Relativa a ataques contra os sistemas de informação. Bruxelas, 2005. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32005F0222&from=PT. Acesso em: 13 nov. 2021.

[25] KELEMEN, R. Daniel. The European Union's authoritarian equilibrium. *Journal of European Public Policy*, v. 27, n. 3, p. 481-499, 2020. p. 482.

[26] Mesmo diante do surgimento das Nações Unidas e a ideia de uma integração pós-guerra, o sistema prevalecente nas relações internacionais até a União Europeia eram aqueles introduzidos pela Paz de Westfália em 1648, ou seja, estabelecidos sob a lógica de igualdade e soberania dos Estados que não precisam reconhecer nenhuma autoridade superior na sua relação com outros Estados. Nesse sentido: HOEKSMA, Jaap; SCHOENMAKER, Dirk. The sovereign behind the Euro. *Duisenberg School of Finance Policy Paper*, n. 15, 2011. p. 3.

[27] VILLAR, Gregorio Cámara. Los derechos fundamentales en el proceso histórico de construcción de la Unión Europea y su valor en el Tratado Constitucional. *Revista de Derecho Constitucional Europeo,* n. 4, p. 9-42, 2005. p. 21-22.

[28] NATO, Alessandro; BIFULCO, Raffaele. *The concept of sovereignty in the EU:* past, present and the future. Reconnect Working Paper, 2020. p. 33.

Isso significa dizer que, além de buscar uma Comunidade de direito, baseada sobre um estatuto comum voltado à construção de uma nova identidade — a cidadania europeia —, a União Europeia se propôs a repensar a relação entre as autoridades nacionais também considerando uma autoridade supranacional, de soberania compartilhada em determinados temas. Para isso, estabeleceu-se a reorganização de determinadas competências com base na tolerância constitucional das autoridades nacionais dos Estados-Membros.[29]

As inovações de uma nova ordem constitucional supranacional pela União Europeia foram inovadoras porque os Estados-Membros, mesmo mantendo o monopólio do uso legítimo da força, aceitaram se subordinar, em determinadas competências, às leis supranacionais, compartilhando a sua soberania com os cidadãos da União.[30] Embora a busca de uma constituição europeia voltada a consolidar esse constitucionalismo multinível, assentado numa concepção política de valores constitucionais, tenha sido rejeitado pelos franceses e pelos holandeses em 2005, foi pela ratificação do Tratado de Lisboa pelos Estados-Membros que a União Europeia se transformou numa política democrática de Estados e cidadãos marcada pelo compartilhamento e união de diversas soberanias.[31]

Outrossim, com o Tratado de Lisboa[32] e a sua especificação normativa quanto a divisão de responsabilidades entre os Estados-Membros e a União, esse modelo único de soberania compartilhada tem levado o bloco ao constante avanço nas relações de poder entre os níveis nacional e supranacional[33], às vezes exercido com base em uma série de crises e polarizações[34], mas também pela bem sucedida integração dessas soberanias, como parece ser a evolução da sociedade informacional no contexto europeu de tutela do seu ciberespaço. Isso porque, na atual Era Digital, o desenvolvimento das tecnologias passou pela tensão existente no globo entre a autorregulação corporativa e a adequada regulamentação do ciberespaço em nome do interesse público, tensão que força as sociedades a repensarem a natureza da soberania na lógica digital. Quer dizer, o que está em jogo não é a substituição da soberania territorial, necessária, porém cada vez mais insuficiente, mas sim a sua complementação por uma soberania supranacional em meio digital, contemporânea, o que já é vivido na realidade europeia desde uma perspectiva analógica até o reconhecimento da soberania dos dados digitais, como ocorre no Regulamento Geral de Proteção de Dados.[35]

Isso ocorre porque, ao se expressar apenas num território virtualmente representado, no qual a fronteira com o real está limitada às telas dos computadores, no ciberespaço as distâncias e o limites geográficos não mais condicionam a ideia de soberania unicamente a partir das fronteiras políticas que delimitam um Estado, ou a identidade de uma nação, mas também por parâmetros relacionais que exigem um pensamento supranacional, integrado.[36]

Sendo assim, para além de uma ideia de jurisdição territorial onde os Estados têm o direito de regular as atividades cibernéticas que ocorrem em seu território (*ratione loci*), há a necessidade de um entendimento acordado, internacionalmente, no sentido de contestar a ação de Estados que não exerçam suas soberanias de modo a garantir o respeito mútuo pelas redes uns dos outros e pela defesa de uma internet mais ampla e segura (*ratione materiae*), o que se traduz no dever de cooperação

[29] NATO, Alessandro; BIFULCO, Raffaele. *The concept of sovereignty in the EU:* past, present and the future. Reconnect Working Paper, 2020. p. 33.

[30] HABERMAS, Jürgen. The crisis of the European Union in the light of a constitutionalization of international law. *European Journal of International Law*, v. 23, n. 2, p. 335-348, 2012. p. 339-340.

[31] HOEKSMA, Jaap; SCHOENMAKER, Dirk. The sovereign behind the Euro. *Duisenberg School of Finance Policy Paper*, n. 15, 2011. p. 4.

[32] Segundo o Parlamento Europeu, o Tratado de Lisboa é resultado de um projeto constitucional iniciado em 2001, com a declaração do Conselho Europeu sobre o futuro da União Europeia, porém reconduzido ante o resultado negativo de referendos realizados em 2005. Também conhecido como Tratado de Funcionamento da União Europeia, esse Tratado altera a forma como a União exerce os seus poderes com base no compartilhamento de competências, reforçando a participação e proteção dos cidadãos, criando um quadro institucional. É nesse Tratado que se estabelecem as competências exclusivas da União, as competências compartilhadas e as competências de apoio, ou seja, na qual o bloco adota medidas suporte às políticas dos seus Estados-Membros. Vide: https://www.europarl.europa.eu/factsheets/en/sheet/5/the-treaty-of-lisbon

[33] NATO, Alessandro; BIFULCO, Raffaele. *The concept of sovereignty in the EU:* past, present and the future. Reconnect Working Paper, 2020. p. 36.

[34] Como exemplo dessas crises que desafiam a União Europeia, há a crise política e democrática vivenciada na Polônia e Hungria, bem como a crise social, econômica e sanitária provocada pela Pandemia de Covid-19.

[35] FLORIDI, Luciano. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. *Philosophy & Technology,* v. 33, n. 3, p. 369-378, 2020. p. 372-374.

[36] MEZZAPELLE, Daniele; ZARRILLI, Luca. Border and cyberspace: some reflections of political geography. *Romanian Review on Political Geography,* n. 2, p. 133-139, 2009. p. 137-138.

para a proteção do ciberespaço.[37] Em outras palavras, a noção de cibersoberania considera o seu compartilhamento supranacional; contudo, esse compartilhamento depende da eleição — pelos Estados — dos elementos dessa soberania que deverão permanecer exclusivos ou serão transferíveis, as quais podem ser vistas desde a infraestrutura do ciberespaço até a busca de uma padronização global.[38]

No âmbito da União Europeia, esse compartilhamento da soberania cibernética, iniciada já em 2005 com a Decisão-Quadro 2005/222, ganhou contornos ainda mais relevantes após a ratificação do Tratado de Lisboa e o delineamento das competências da União e seus Estados-Membros. O desafio do bloco, na oportunidade, passou a ser a de proporcionar a busca integrada por uma agenda digital que fosse além da cooperação policial e judiciária no combate aos crimes cibernéticos (apesar da crescente importância deste) para também explicar e analisar sua economia, os seus desafios sociais e as deficiências da União Europeia, entre outros.[39]

Em outras palavras, se o desenvolvimento de uma sociedade informacional na Europa estava relegado a uma questão secundária, a aproximação dos anos 2010 marcou uma constante apresentação de diretivas e regulamentos relacionados com questões cibernéticas, voltadas a estabelecer, em nível supranacional, o desenvolvimento econômico e social dos cidadãos europeus, e também à construção de um ciberespaço seguro, aberto e protegido.[40] Dessa forma, fundada na lógica de segurança e disponibilidade do ciberespaço, a União Europeia buscou responder, com coerência institucional e política, os desafios cibernéticos enfrentados pela Europa, fazendo-o a partir do avanço de distintas áreas como a construção de marcos normativos, proteção de infraestruturas críticas, combate ao cibercrime e defesa[41], ou seja, por estratégias de cibersegurança, entendidas como o conjunto de ações destinado a proteger o ciberespaço, seus sistemas informáticos e os dados neles contidos.[42]

Ponto de partida dessa efetiva integração do bloco na defesa do ciberespaço foi a apresentação, em 2013, pela alto representação da União Europeia, da comunicação conjunta chamada Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido.[43] Nesse documento, além de se reconhecer que o mundo digital não é controlado por uma única entidade e está sob constante ameaça, é pelo desenvolvimento de ações de cibersegurança[44] que a União Europeia preserva o ambiente *online* com garantia de "maior liberdade e segurança possível", promovendo, assim, os valores fundamentais da União Europeia e garantido a sua integração nas relações internas e na política externa e de segurança comum. Outrossim, declara que, apesar de caber preponderantemente aos Estados-Membros a segurança do seu respectivo ciberespaço, suas dimensões transfronteiriças exigem ações específicas supranacionais por meio de "ações, de curto e de longo prazos, que incluem uma variedade de ferramentas políticas e envolvem diferentes tipos de atores — desde as instituições da UE aos Estados-Membros ou à indústria."[45]

Consequência dessa estratégia, e que ratifica a cibersegurança como eixo de integração da União Europeia na compreensão de um ciberespaço de soberania compartilhada, é a edição da Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, voltada a "garantir um elevado nível comum de segurança das redes e da informação em toda a União."[46]

[37] VON HEINEGG, Wolff Heintschel. Territorial sovereignty and neutrality in cyberspace. *International Law Studies US Naval War College*, v. 89, n. 1, p. 127-156, 2013. p. 155-156.

[38] YELI, Hao. A three-perspective theory of cyber sovereignty. *Prism*, v. 7, n. 2, p. 108-115, 2017. p. 112.

[39] KOVACS, László. Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review*, v. 23, n. 1, p. 16-24, 2018. p. 17.

[40] CAVELTY, Myriam Dunn. A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers,* v. 23, 2013. p. 4.

[41] CARRAPICO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. *European Politics and Society,* v. 19, n. 3, p. 299-303, 2018. p. 300.

[42] CRAIGEN, Dan; DIAKUN-THIBAULT, Nadia; PURSE, Randy. Defining cybersecurity. *Technology Innovation Management Review*, v. 4, n. 10, 2014. p. 17.

[43] GERALDES, Sofia Martins. A estratégia de cibersegurança da União Europeia: catastrofista, realista e/ou otimista? *Nação e Defesa*, 2019. p. 102.

[44] Importante destacar que nesse documento um conceito de cibersegurança é apresentado, o qual também revela a ideia de proteção do ciberespaço tanto a partir da logica civil como militar, de defesa: o termo cibersegurança refere-se, geralmente, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade das redes e infraestruturas, e a confidencialidade das informações nelas contidas.

[45] COMISSÃO EUROPEIA. *Cybersecurity strategy of the European Union, an open, safe and secure cyberspace.* Bruxelas, 2013. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52013JC0001&from=PT. Acesso em: 16 nov. 2021.

[46] CONSELHO DA UNIÃO EUROPEIA. *Diretiva (UE) n.º 2016/222, de 06 de julho de 2016*. Relativa a medidas destina-

Nos considerandos dessa diretiva, destaque à compreensão normativa de que, diante da natureza transnacional das redes e sistemas de informação, que integram o ciberespaço, "as perturbações significativas desses sistemas, intencionais ou não, e independentemente do local onde ocorram, podem afetar os Estados-Membros, individualmente considerados, e a União no seu conjunto" (Considerando 3), motivo pelo qual a resposta mais eficaz é "uma abordagem global a nível da União, que abranja os requisitos mínimos comuns" (Considerando 6), porém, "sem prejuízo da possibilidade de cada Estado-Membro tomar as medidas necessárias para garantir a proteção dos interesses essenciais da sua própria segurança" (Considerando 8).[47]

Como se percebe, para entender a cibersegurança no contexto de integração da União Europeia, devem se considerar, na visão de Carrapico e Barrinha, duas categorias distintas, quais sejam: (i) cooperação institucional e (ii) compreensão compartilhada de segurança. Enquanto a primeira considera uma abordagem comum para a cibersegurança desde uma visão público-privada que integra o mercado e autoridades nacionais como a ENISA e as CERTs (*Computer Emergency Response Teams*), a segunda categoria tem por base uma compreensão compartilhada de segurança que está efetivamente vinculada à ideia da cibersegurança como expressão de uma cibersoberania compartilhada pelos Estados-Membros por ser compreendida como uma nova arma de potencial econômico, político e militar.[48] Além de, também, potencial ambiental.

Seja então na lógica da atuação livre das organizações ou da defesa da soberania de um Estado no ciberespaço, a segurança e a consequente proteção das informações e dos ativos que as armazenam, processam e transmitem são condições fundamentais de cooperação entre as nações para a sua tutela. Boas práticas focadas em normas técnicas nacionais e internacionais, certificações na gestão da Segurança da Informação e o desenvolvimento de técnicas de defesa cibernética têm se mostrado fundamentais tanto para a segurança das atividades econômicas quanto para a manutenção da soberania no ambiente virtual do ciberespaço.[49]

Em outras palavras, por estar vinculada a distintas visões sobre o eixo da segurança comum, a cibersegurança tem se mostrado um elo essencial na integração da União Europeia da atualidade também com base nas perspectivas político-democráticas de Estados que, nesse caso, compartilham e unem a sua soberania cibernética. Por isso, a evolução normativa do ciberespaço, sob distintas dimensões, como tratado a seguir.

4 Um futuro digital para a Europa e a cibersegurança como pilar de integração à promoção e defesa do seu ciberespaço

A cibersegurança se transformou, nos últimos anos, como uma das prioridades políticas e institucionais da União Europeia, promovendo a integração do bloco para além das soberanias dos Estados-Membros por meio de uma arquitetura institucional que se desenvolve constantemente desde 2004, quando da criação da Agência da União Europeia para a Cibersegurança (ENISA) e do Centro Europeu de Crimes Cibernéticos (EC3), vinculado à Europol. De igual forma, a Diretiva (UE) 2016/1148, também conhecida como Diretiva NIS, foi essencial para a promoção de uma integração horizontal e vertical entre os Estados-Membros, a Comissão Europeia e a ENISA com novas atribuições, propiciando novos grupos de cooperação voltadas à promoção da segurança da informação na Europa.[50]

Prova dessa integração relativa à cibersegurança foi que para além de admitir, de forma integrada, o controle a novas ameaças digitais, como a desinformação, a Diretiva NIS estabeleceu os fundamentos para a implementação de sistemas de segurança em todos os Estados-Membros, determinando, ainda, ser obrigação

das a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L1148. Acesso em: 16 nov. 2021.

[47] CONSELHO DA UNIÃO EUROPEIA. *Diretiva (UE) n.º 2016/222, de 06 de julho de 2016*. Relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L1148. Acesso em: 16 nov. 2021.

[48] CARRAPICO, Helena; BARRINHA, André. The EU as a coherent (cyber) security actor? *JCMS:* Journal of Common Market Studies, v. 55, n. 6, p. 1254-1272, 2017. p. 1261.

[49] MARTINS, José Carlos Lourenço. *Gestão de segurança da informação e cibersegurança nas organizações:* sistema e método. Faro: Sílabas e Desafios, 2021. p. 45.

[50] CARRAPICO, Helena; BARRINHA, André. The EU as a coherent (cyber) security actor? *JCMS:* Journal of Common Market Studies, v. 55, n. 6, p. 1254-1272, 2017. p. 1263-1264.

destes introduzir estratégias nacionais de segurança cibernética, estruturados, inclusive, para incluir funções e responsabilidades dos órgãos governamentais e outros atores relevantes dos setores públicos e privados.[51] [52]

Outrossim, 2016 foi um ano igualmente importante para compreender a evolução atual da cibersegurança em um contexto estratégico mais amplo para o bloco: a Estratégia Global da União Europeia.[53] Nesse documento, a cibersegurança foi apresentada como um dos enfoques estratégicos para a conquista de um futuro digital pela integração das questões cibernéticas em todas as ações políticas da União e seus Estados-Membros.[54] Seu objetivo final, menciona a Comissão Europeia, é a consolidação da soberania em meio digital do bloco e o estabelecimento de normas voltadas aos dados, às tecnologias e suas infraestruturas.[55]

Para a construção do atual momento, que chamou de "Década Digital", a Comissão União Europeia apresentou, em março de 2021, um projeto voltado à transformação digital da Europa até 2030, a qual está centrada na criação de novas competências, transformação digital das empresas, digitalização dos serviços e, finalmente, o estabelecimento de infraestruturas digitais seguras e sustentáveis. Assim, para além da criação de um quadro de princípios digitais destinados à promoção e defesa dos valores da União Europeia no ciberespaço, a "Década Digital" pretende fortalecer projetos plurinacionais que combinem investimentos e apoio a um mercado digital único e de integração dos Estados-Membros. E, como exemplo desse potencial projeto plurinacional, a Comissão apresenta a possibilidade de implementação de "uma rede de centros de operações de seguranças, alimentados por inteligência artificial, para prever, detectar e reagir a ciberataques a nível nacional e da UE."[56]

Além disso, a realização do propósito de transformação digital da União Europeia, chamada de "Um novo futuro digital para a Europa", tem como previsão trabalhar distintos domínios para esse intento, como o fomento e a regulação de serviços digitais e de mercados digitais, o avanço sobre a criação de um mercado único de dados que considere os valores comuns da União Europeia, a adaptação dos sistemas de tributação dos Estados-Membros para a economia digital, o desenvolvimento de aplicações de Inteligência Artificial com abordagem ética e centrada no ser humano, a ampliação da conectividade a todos os europeus, a criação de uma identificação digital europeia única e a digitalização da justiça.[57]

O desenvolvimento do ciberespaço amplificado pela Covid-19 e a necessária aceleração para a transformação digital da União Europeia levaram o bloco europeu a estabelecer, de maneira ainda mais integrada, em multinível e centrada nos seus valores políticos e democráticos, a ideia de uma soberania compartilhada na lógica de criação de uma cidadania europeia digital. Nela, cidadãos, empresas, Estados-Membros e União aceitam a transposição das soberanias tradicionais, físico-geográficas, para a construção de uma soberania em meio digital única, portanto integrada à noção de transformação digital enquanto uma mudança de cultura para o digital desde a perspectiva humana, quer dizer, da incorporação de comportamentos na sociedade informacional que admitem a mudança das normas então vigentes para uma compreensão digital completamente distinta.[58]

Todavia, para que essa transformação digital realmente se estabeleça, enquanto nova expressão cultural europeia na sociedade informacional, é essencial que toda a União e seus cidadãos confiem nesse processo, o

[51] ŠTITILIS, Darius *et al.* National cyber security strategies: management, unification and assessment. *IJM&P:* Independent Journal of Management & Production, v. 11, n. 9, p. 2341-2354, 2020. p. 2344.

[52] FUSTER, Gloria González; JASMONTAITE, Lina. Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. *In:* CHRISTEN, Markus; GORDIJN, Bert; LOI, Michele (ed.). *The ethics of cybersecurity.* Cham: Springer, 2020. p. 97-115. p. 104.

[53] BRANDÃO, Ana Paula; CAMISÃO, Isabel. Playing the market card: the Commission's strategy to shape EU cybersecurity policy. *JCMS:* Journal of Common Market Studies, 2021. p. 12.

[54] COMISSÃO EUROPEIA. '*Shared vision, common action:* a stronger Europe: a global strategy for the European Union's foreign and security policy'. Bruxelas, 2016. Disponível em: https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf. Acesso em: 20 nov. 2021.

[55] COMISSÃO EUROPEIA. *Uma Europa preparada para a era digital:* empoderar as pessoas graças a uma nova geração de tecnologias. 2021. Disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pt. Acesso em: 22 nov. 2021.

[56] COMISSÃO EUROPEIA. *Década digital da Europa:* objetivos digitais para 2030. 2021. Disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt. Acesso em: 22 nov. 2021.

[57] CONSELHO DA UNIÃO EUROPEIA. *Um futuro digital para a Europa.* Bruxelas, 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/a-digital-future-for-europe/. Acesso em: 22 nov. 2021.

[58] HEMERLING, Jim *et al. It's not a digital transformation without a digital culture*. Boston: BCG, 2018.

que, mais uma vez, leva à centralidade da cibersegurança. Isso porque, ao ser entendida como um conjunto de precauções e ações que podem ser utilizadas para proteger o ciberespaço e manter a disponibilidade, a integridade das redes, suas infraestruturas e a confidencialidade das informações nelas contidas[59], a cibersegurança passa a ser considerada, também, como uma estratégia voltada a "reforçar a resiliência da Europa contra as ciberameaças e garantir que todos os cidadãos e empresas possam beneficiar-se plenamente de serviços e ferramentas digitais fiáveis e credíveis."[60]

Para tanto, outras atividades ligadas à cibersegurança passam a ser revisitadas e/ou fomentadas. Uma dessas atividades é a ampliação do combate à cibercriminalidade para áreas sensíveis para a União e seus Estados-Membros, como a luta contra a fraude em pagamentos eletrônicos, a segurança das crianças na Internet e a justiça e aplicação da lei, tais como as provas eletrônicas, a encriptação e a conservação de dados. Ademais, para também proteger o bloco, a União Europeia tem envidado esforços para o desenvolvimento de uma ciberdiplomacia que garanta resposta diplomática às ciberameaças provenientes de países terceiros por meio da cooperação e do diálogo diplomático que garanta instrumentos de ciberdiplomacia focados na prevenção de ciberataques e sanções pela União e seus Estados-Membros.[61]

Assim, também na lógica da defesa da soberania, a cibersegurança se mostra como uma estratégia comum do bloco[62]. Isso porque, além de o Conselho da União Europeia atualmente considerar o ciberespaço como o quinto teatro de guerra (além da terra, ar, mar e espaço), sua amplitude material e imaterial leva a uma grande estratégia de cooperação e compartilhamento da soberania dos Estados-Membros para a defesa coordenada "desde as redes de informação e telecomunicações, as infraestruturas e os dados que suportam, até aos sistemas informáticos, processadores e controladores."[63] Isso significa que, além do apoio especializado da ENISA e da Europol, também na Agência Europeia de Defesa (AED), ações especializadas em cibersegurança permitem a cooperação da União em torno da defesa militar do ciberespaço, compartilhando, inclusive, força de guerra em meio digital (*cyber war*).

Prova disso são as recentes ações da Agência na defesa supranacional do ciberespaço enquanto quinto domínio de guerra, especialmente diante das ameaças apresentadas pela Guerra Rússia-Ucrânia, oportunidade na qual o Conselho Europeu reconheceu, em março de 2022, que o domínio da informação e do ciberespaço deve não somente promover ações de defesa, mas passar a considerar o estágio de confronto, exigindo, assim, estratégia de ciberdefesa da Europa a partir da sua visão supranacional de cibersoberania.[64] Essa postura sedimentou atividades e normativas até então realizadas para desenvolvimento de um programa de defesa cibernética que já considerava, entre outros, o fortalecimento de um modelo de gestão de riscos nas cadeias de suprimentos e a federalização das áreas cibernéticas militares dos Estados-Membros. Assim, a UE desenvolve a sua cibersoberania pela coerência das suas atividades cibernéticas desenvolvidas em cooperação nas suas distintas agências especializadas, como a própria AED, a Agência da União Europeia para a Cibersegurança (ENISA), a CERT-EU e a EC3/Europol.[65]

Além disso, essas iniciativas consolidam as atualizações normativas ocorridas na União Europeia desde 2019 para a cibersegurança e a efetiva proteção do ciberespaço europeu. A primeira dessas iniciativas foi a aprovação do Regulamento (UE) 2019/881, de 17 de abril de 2019, voltado a garantir a centralidade da cibersegurança tanto pelo fortalecimento e reestruturação da Agência da União Europeia para a Cibersegurança (ENISA) como pelo estabelecimento de critérios para a

[59] Aqui admitindo o conceito apresentado pela própria Estratégia da União Europeia para a cibersegurança. Vide notas de rodapé 43 e 44.

[60] CONSELHO DA UNIÃO EUROPEIA. *Cibersegurança*: como combate a UE as ciberameaças. Bruxelas, 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acesso em: 22 nov. 2021.

[61] CONSELHO DA UNIÃO EUROPEIA. *Cibersegurança*: como combate a UE as ciberameaças. Bruxelas, 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acesso em: 22 nov. 2021.

[62] MARTINS, José Carlos Lourenço. *Gestão de segurança da informação e cibersegurança nas organizações:* sistema e método. Faro: Sílabas e Desafios, 2021. p. 90.

[63] CONSELHO DA UNIÃO EUROPEIA. *Cibersegurança*: como combate a UE as ciberameaças. Bruxelas, 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acesso em: 22 nov. 2021.

[64] EUROPEAN DEFENCE AGENCY. Ukraine war confirms need to define a longterm strategy to ensure the defence of Europe. *In European Defence Matters*, n. 23, p. 22, 2022. Disponível em: https://eda.europa.eu/docs/default-source/eda-magazine/full-edm-23-(final).pdf. Acesso em: 10 out. 2022.

[65] EUROPEAN DEFENCE AGENCY. *Cyber*. Bruxelas, 2022. Disponível em: https://eda.europa.eu/what-we-do/capability-development/cyber. Acesso em: 10 out. 2022.

certificação da cibersegurança das tecnologias da informação e comunicação.[66]

O que chama a atenção no regulamento é que, ao longo dos seus 110 *consideranda*, o Parlamento Europeu e o Conselho da União Europeia não apenas ratificam a importância que tem o ciberespaço para o desenvolvimento do União e seus Estados-Membros, como também reconhecem a insuficiência dos níveis de segurança para as propostas a serem implementadas pelo bloco, como a cibercriminalidade (considerando 15), a ciberdiplomacia (considerando 54) e a ciberdefesa (considerando 43). Resta claro que a cibersegurança passa a ser uma nova *raison d'être* (razão de ser) da União Europeia na medida em que "atendendo à natureza transfronteiriça das ciberameaças, é necessário aumentar a nível da União as capacidades suscetíveis de complementar a ação dos Estados-Membros."[67]

E, nesse mesmo sentido, iniciativas ainda em trâmite como a revisão da Diretiva SRI (chamada de SRI 2.0)[68] revelam a necessidade constante de respostas ao cenário das novas ameaças cibernéticas e à transformação digital acelerada pela Covid-19 também no ambiente europeu. Serão essas condicionantes, portanto, que levarão a cibersegurança à revisão cíclica de suas políticas e estratégias, seja para a construção da cibercidadania europeia, para o desenvolvimento de um mercado digital livre, para o combate às ciberameaças, para o estabelecimento da ciberdefesa da União e seus Estados-Membros ou, ainda, para o alcance de uma nova cibersoberania transfronteiriça, compartilhada, imaterial. Toda essa transformação poderá levar a União Europeia, finalmente, a um ciberconstitucionalismo multinível, compartilhando no ciberespaço europeu leis e valores democráticos, como pensado, ainda que de forma analógica, em Maastricht.

5 Considerações finais

O artigo refletiu a evolução da sociedade informacional e as ameaças cibernéticas existentes no meio digital, de modo a compreender como esse cenário tem levado as nações em todo mundo a refletir sobre como bem tutelar o ciberespaço, inicialmente imaginado como um ambiente imaterial de plena integração e liberdade global com o advento da Internet. Pelo seu paradigmático rompimento com as compreensões físicas e territoriais sobre soberania, advindos desde a Paz de Westfália, essa tutela passou a ser compreendida sob a necessária lógica de integração internacional entre as Nações, o que encontra dificuldades práticas na medida em que o ciberespaço tão somente reproduz (e, às vezes, amplifica) os desafios e potenciais conflitos geopolíticos já existentes no mundo físico, analógico.

Ocorre que, no âmbito da União Europeia, muito embora a proposta inicial de um constitucionalismo multinível tenha fracassado, o Tratado de Lisboa teve um papel fundamental por manter no bloco europeu as premissas de um pensamento de integração e cooperação que se estrutura sobre o compartilhamento de importantes premissas do constitucionalismo democrático, como a cidadania e a soberania de seus povos.

Não obstante alguns conflitos e tensões atualmente vividos no ambiente Europeu, como a crise social e sanitária da Covid-19, a efetivação do Brexit, os movimentos antidemocráticos vividos na Hungria e na Polônia e a recente Guerra da Ucrânia — esta com impactos diretos na compreensão do ciberespaço enquanto espaço de guerra e na construção de uma cibersoberania, como visto —, o que se tem de concreto é que a União Europeia mantém o seu espírito de integração, o que é amplamente demonstrado pela crescente tutela compartilhada do ciberespaço europeu enquanto expressão do seu pluralismo cultural e político.

O artigo esclarece, portanto, que essa tutela compartilhada se mostra, a partir das reflexões de Gráinne De Búrca, como a nova *raison d'être* da União Europeia,

[66] CONSELHO DA UNIÃO EUROPEIA. *Regulamento (UE) nº 2019/881, 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 e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança). Bruxelas, 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019R0881&from=EN. Acesso em: 24 nov. 2021.

[67] CONSELHO DA UNIÃO EUROPEIA. *Regulamento (UE) nº 2019/881, 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 e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança). Bruxelas, 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019R0881&from=EN. Acesso em: 24 nov. 2021.

[68] Pela nova proposta, novas regras serão estabelecidas a fim de reforçar as obrigações das empresas em matéria de segurança, assegurar práticas de cibersegurança nas cadeias logísticas e trazer maior capacidade de supervisão, compartilhamento de informações e cooperação. Para acesso à proposta da SRI 2: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

não apenas porque promove a integração econômica e a prosperidade dos Estados-Membros, mas também os posicionam num papel de relevância sobre o tema frente a outras potências globais como os Estados Unidos, a Rússia e a China.

A distinção da União Europeia nesse novo jogo de xadrez em meio digital, porém, está justamente no fato de esse acesso à tutela do ciberespaço ocorrer no bloco com base na mesma lógica de supranacionalidade e integração dos povos e Nações, atualmente ameaçada no ambiente de guerra. Por essas razões conjugadas, a União Europeia parece melhor compreender os desafios do ciberespaço na medida em que os seus Estados-Membros há décadas refletem sobre outros desafios, até então analógicos, que exigem igual atuação transfronteiriça e estruturação supranacional de políticas que alcancem o efetivo bem-estar econômico e social de seus povos. Talvez por isso, então, que a necessária construção de um ciberespaço seguro, aberto e protegido seja cada vez melhor compreendida no contexto europeu e sob o cuidado da União Europeia.

Neste aspecto e tal como discutido, pelo menos desde os anos 2000, a União Europeia estrutura a construção e a disponibilidade desse ciberespaço comum sob a lógica da confiança mútua, a partir da Segurança da Informação e do consequente desenvolvimento de estratégias de cibersegurança que protejam não apenas esse espaço cibernético, seus sistemas informáticos e os dados neles contidos, mas também outros serviços digitais, seus mercados, suas comunicações e suas infraestruturas críticas. Além disso, o risco de um novo conflito no continente exige o desenvolvimento, ainda mais assertivo, de meios de integração e defesa que na realidade atual ultrapassa os limites da territorialidade. Por isso, fica claro para a União Europeia que a integração, a partir dos seus valores, e o desenvolvimento desse ambiente digital global passam, necessariamente, por iniciativas transnacionais que assegurem, por meio da cibersegurança, uma nova noção de soberania compartilhada, a cibersoberania, que se funda na efetiva cooperação institucional e na compreensão compartilhada de segurança.

Prova disso, como destacado, é a atuação do bloco na proposição e desenvolvimento de outras atividades ligadas à cibersegurança, como o equilíbrio entre o livre fluxo de dados com a proteção dos dados pessoais dos cidadãos europeus, o constante aperfeiçoamento e ampliação do combate à cibercriminalidade como forma de responder aos cibercrimes, os esforços para o desenvolvimento de uma ciberdiplomacia que dê respostas diplomáticas eficazes às ciberameaças na relação do bloco com países terceiros e, por fim, o aprimoramento da ciberdefesa militar para a sua atuação no ciberespaço enquanto quinto teatro de guerra, atualmente em teste no conflito da Ucrânia.

Em conclusão, as frentes multidirecionais permitidas pela centralidade da cibersegurança no desenvolvimento do ciberespaço europeu parecem mostrar que União Europeia terá uma nova oportunidade de revisitar, sob o signo digital e por meio do compartilhamento supranacional e transfronteiriço da soberania dos seus Estados-Membros no ciberespaço (de sua cibersoberania), os seus valores democráticos e de justiça pensados desde Maastricht. Em consequência disso, poderá surgir a construção de uma nova ideia de constitucionalismo multinível, o ciberconstitucionalismo construído sobre bases de uma nova ciberpolítica como sucedâneo da geopolítica vigente desde a Paz de Westfália, ultrapassando, assim, as barreiras físico-geográficas postas à União Europeia em 2005 para a integração total dos Estados nacionais e seus povos.

Referências

BRANDÃO, Ana Paula; CAMISÃO, Isabel. Playing the market card: the Commission's strategy to shape EU cybersecurity policy. *JCMS: Journal of Common Market Studies*, 2021.

BURCA, Gráinne de. Europe's raison d'être. *In:* KOCHENOV, Dimitry; AMTENBRINK, Fabian (ed.). *The European Union's shaping of the international legal order.* Cambridge: Cambridge University Press, 2014. p. 21-37.

CARRAPICO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. *European Politics and Society,* v. 19, n. 3, p. 299-303, 2018.

CARRAPICO, Helena; BARRINHA, André. The EU as a coherent (cyber) security actor? *JCMS: Journal of Common Market Studies*, v. 55, n. 6, p. 1254-1272, 2017.

CASTELLS, Manuel. *A era da informação:* economia, sociedade e cultura. São Paulo: Paz e Terra, 2020.

CAVELTY, Myriam Dunn. A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers,* v. 23, 2013.

CHRISTOU, George. The EU's approach to cybersecurity. *University of Essex Paper Series*, 2017.

COMISSÃO EUROPEIA. '*Shared vision, common action:* a stronger Europe: a global strategy for the European Union's foreign and security policy'. Bruxelas, 2016. Disponível em: https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf. Acesso em: 20 nov. 2021.

COMISSÃO EUROPEIA. *Década digital da Europa:* objetivos digitais para 2030. 2021. Disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pt. Acesso em: 22 nov. 2021.

COMISSÃO EUROPEIA. *Uma Europa preparada para a era digital:* empoderar as pessoas graças a uma nova geração de tecnologias. 2021. Disponível em: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_pt. Acesso em: 22 nov. 2021.

CONSELHO DA UNIÃO EUROPEIA. *Cibersegurança*: como combate a UE as ciberameaças. Bruxelas, 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acesso em: 22 nov. 2021.

CONSELHO DA UNIÃO EUROPEIA. *Decisão-Quadro n.º 205/222, de 24 de fevereiro de 2005*. Relativa a ataques contra os sistemas de informação. Bruxelas, 2005. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32005F0222&from=PT. Acesso em: 13 nov. 2021.

CONSELHO DA UNIÃO EUROPEIA. *Regulamento (UE) nº 2019/881, 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 e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança). Bruxelas, 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32019R0881&from=EN. Acesso em: 24 nov. 2021.

CONSELHO DA UNIÃO EUROPEIA. *Um futuro digital para a Europa*. Bruxelas, 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/a-digital-future-for-europe/. Acesso em: 22 nov. 2021.

CRAIGEN, Dan; DIAKUN-THIBAULT, Nadia; PURSE, Randy. Defining cybersecurity. *Technology Innovation Management Review*, v. 4, n. 10, 2014.

EUROPEAN DEFENCE AGENCY. *Cyber*. Bruxelas, 2022. Disponível em: https://eda.europa.eu/what-we-do/capability-development/cyber. Acesso em: 10 out. 2022.

EUROPEAN DEFENCE AGENCY. Ukraine war confirms need to define a longterm strategy to ensure the defence of Europe. *In European Defence Matters*, n. 23, p. 22, 2022. Disponível em: https://eda.europa.eu/docs/default-source/eda-magazine/full-edm-23-(final).pdf. Acesso em: 10 out. 2022.

FLORIDI, Luciano. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. *Philosophy & Technology,* v. 33, n. 3, p. 369-378, 2020.

FUSTER, Gloria González; JASMONTAITE, Lina. Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. *In:* CHRISTEN, Markus; GORDIJN, Bert; LOI, Michele (ed.). *The ethics of cybersecurity*. Cham: Springer, 2020. p. 97-115.

GERALDES, Sofia Martins. A estratégia de cibersegurança da União Europeia: catastrofista, realista e/ou otimista? *Nação e Defesa*, 2019.

HABERMAS, Jürgen. The crisis of the European Union in the light of a constitutionalization of international law. *European Journal of International Law*, v. 23, n. 2, p. 335-348, 2012.

HEMERLING, Jim *et al. It's not a digital transformation without a digital culture*. Boston: BCG, 2018.

HOEKSMA, Jaap; SCHOENMAKER, Dirk. The sovereign behind the Euro. *Duisenberg School of Finance Policy Paper*, n. 15, 2011.

KELEMEN, R. Daniel. The European Union's authoritarian equilibrium. *Journal of European Public Policy*, v. 27, n. 3, p. 481-499, 2020.

KOVACS, László. Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review*, v. 23, n. 1, p. 16-24, 2018.

LÈVY, Pierre. *O que é virtual?* São Paulo: Ed. 34, 1996.

MAIAS, André; BRAVO, Rogério. *Geopolítica, geoestratégia e ciberespaço.* Lisboa: Academia, 2010.

MARTINS, José Carlos Lourenço. *Gestão de segurança da informação e cibersegurança nas organizações:* sistema e método. Faro: Sílabas e Desafios, 2021.

MEZZAPELLE, Daniele; ZARRILLI, Luca. Border and cyberspace: some reflections of political geography. *Romanian Review on Political Geography,* n. 2, p. 133-139, 2009.

NATO, Alessandro; BIFULCO, Raffaele. *The concept of sovereignty in the EU:* past, present and the future. Reconnect Working Paper, 2020.

PARLAMENTO EUROPEU. *Tratado da União Europeia (TUE).* 2021. Disponível em: https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/maastricht-treaty. Acesso em: 12 nov. 2021.

SCHWAB, Klaus. *A quarta revolução industrial.* São Paulo: Edipro, 2016.

SHEN, Yi. Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, v. 1, n. 1, p. 81-93, 2016.

ŠTITILIS, Darius *et al.* National cyber security strategies: management, unification and assessment. *IJM&P: Independent Journal of Management & Production*, v. 11, n. 9, p. 2341-2354, 2020.

VIEIRA, Vasco Rocha. A União Europeia de Maastricht a Nice: uma reflexão sobre o futuro. *Nação e Defesa,* v. 2, n. 100, p. 37-49, 2001.

VILLAR, Gregorio Cámara. Los derechos fundamentales en el proceso histórico de construcción de la Unión Europea y su valor en el Tratado Constitucional. *Revista de Derecho Constitucional Europeo,* n. 4, p. 9-42, 2005.

VIRGA, Joy Marie. International criminals and their virtual currencies: the need for an international effort in regulating virtual currencies and combating cyber crime. *Revista de Direito Internacional*, Brasília, v. 12, n. 2, p. 511-526, 2015.

VON HEINEGG, Wolff Heintschel. Territorial sovereignty and neutrality in cyberspace. *International Law Studies US Naval War College*, v. 89, n. 1, p. 127-156, 2013.

YELI, Hao. A three-perspective theory of cyber sovereignty. *Prism*, v. 7, n. 2, p. 108-115, 2017.