UNIO
EU LAW JOURNAL

UNIO E-BOOK
INTEROP 2019

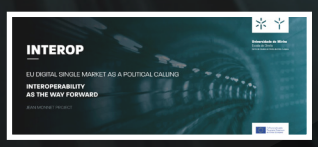
O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir

Coordenação Científica

Alessandra Silveira
Joana Covelo de Abreu
Larissa Coelho

Universidade do Minho
Escola de Direito

Cofinanciado pelo Programa Erasmus+ da União Europeia



UNIO E-BOOK 2019

O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir

Coordenação Científica:
Alessandra Silveira, Joana Covelo de Abreu e Larissa Coelho

Autores:
João Ferreira | Larissa Coelho | Laura Gomes Rodrigues | Leandra Dias | Lucas Silvestre Cortizo | Marcelo Porrua | Nataly Carvalho Machado | Nelson Alex Lorenz | Tiago Branco da Costa | Victor Moreira Mulin Leal

Edição:
Pensamento Sábio - Associação para o conhecimento e inovação
Universidade do Minho. Escola de Direito

Coordenação Técnica:
Larissa Coelho

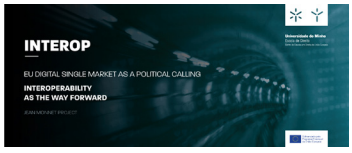
Este trabalho é financiado ao abrigo do Projeto Jean Monnet INTEROP – EU Digital Single Market as a political calling: interoperability as the way forward, com o número 587400-EPP-1-2017-1-PT-EPPJMO-PROJECT.

DOI: 10.21814/1822.61446 | ISBN: 978-989-54587-1-4

Braga, julho de 2019

Cofinanciado pelo Programa Erasmus+ da União Europeia

UNIO EU LAW JOURNAL



ÍNDICE

APRESENTAÇÃO

Os textos publicados neste e-book "O Mercado Único Digital da União Europeia como um desígnio político: a interoperabilidade como o caminho a seguir" encontram-se divididos em quatro partes, por referência aos quatro painéis da Conferência Final INTEROP "A UE e o Mercado Único Digital".

A publicação desta obra corresponde a um dos objetivos visados no Projeto *Jean Monnet* com o acrónimo "INTEROP" e subordinado ao tema "*EU Digital Single Market as a political calling: interoperability as the way forward*", desenvolvido na Escola de Direito da Universidade do Minho de setembro de 2017 a agosto de 2019, com a chancela da Comissão Europeia e do Programa ERASMUS+.

Neste contexto, o Projeto partiu da análise do Mercado Único Digital, atentando ao seu estabelecimento, desenvolvimento e sedimentação à luz da interoperabilidade administrativa, o que justifica que o primeiro tópico desta obra seja "Mercado Único Digital e interoperabilidade administrativa". Seguidamente, o Projeto visava percecionar o impacto das tecnologias de informação e de comunicação na dinâmica jusfundamental da União Europeia e apreciar os seus reflexos na cidadania europeia, o que influenciou a segunda parte deste e-book, subordinada ao tema "Direitos fundamentais e cidadania na era digital". Em terceiro lugar, o Projeto *Jean Monnet* almejava testar a viabilidade de uma interoperabilidade judiciária, catalisadora de uma tutela jurisdicional efetiva, no contexto do novo paradigma da justiça eletrónica, razão pela qual a terceira parte do e-book se subsume ao tema "Tutela jurisdicional efetiva e justiça eletrónica". Por fim, o projeto ambicionava equacionar quais os desafios que, no futuro, se divisam ao Mercado Único Digital, viés determinante para que a quarta parte da obra se intitule "Desafios prospetivos do Mercado Único Digital".

Este *e-book* resulta da consecução da componente científica associada ao Projeto INTEROP, cujo escopo passava pelo entrosamento de jovens investigadores da Escola de Direito da Universidade do Minho nas temáticas a serem desenvolvidas.

Para o efeito, foi organizada e promovida uma Mesa Redonda de Jovens Investigadores no âmbito da mencionada conferência final, que se realizou no dia 2 de maio de 2019, resultante de uma *call for papers*, divulgada no seio da comunidade académica e que contou com ampla participação.

Os trabalhos que ora se publicam correspondem aos artigos submetidos por estudantes de Mestrado e de Doutoramento da Universidade do Minho e que comprovam a amplitude de temas estudados e as sensibilidades desenvolvidas por jovens investigadores a partir do seu contacto direto com os investigadores associados ao Projeto e, bem assim, com os demais investigadores seniores, agentes interessados, agentes políticos, membros da organização administrativa e operadores judiciários que participaram nas diversas atividades promovidas no seu desenrolar. Acresce que ainda teve a capacidade de agregar o contributo de juristas que, em contexto empresarial, promovem a articulação entre o direito e as novas tecnologias de informação. Para o efeito, os Mestrandos envolvidos (alguns dos quais ainda em fase de frequência da parte escolar do Mestrado) provêm dos diversos cursos oferecidos pela Escola de Direito: Mestrado em Direito da União Europeia, Mestrado em Direito e Informática, Mestrado em Direito Administrativo, Mestrado em Direitos Humanos, Mestrado em Direito Judiciário e Mestrado em Direito dos Contratos e Empresas, alcançando, em larga medida, um público-alvo mais amplo do que o que se perspetivava como possível na propositura do Projeto.

Verifica-se, portanto, a diversidade de abordagens e o despertar de sensibilidades logo no início do percurso académico dos investigadores.

Assim, a **PARTE I – "Mercado Único Digital e interoperabilidade administrativa"** começa com o contributo de Laura Rodrigues, continua com o texto de Lucas Silvestre Cortizo e finda com a reflexão de Victor Moreira Mulin Leal.

Laura Rodrigues, Mestranda em Direito Administrativo (em fase escolar), apresenta um texto subordinado ao tema "O princípio da autonomia procedimental e o procedimento para a concessão de vistos pelos Estados-Membros da União Europeia. Os novos desafios da interoperabilidade administrativa". Com a sua reflexão, teve em vista equacionar, à luz do Direito Administrativo da União Europeia, o princípio da autonomia procedimental dos Estados-Membros no contexto específico da concessão de vistos a fim de problematizar como a interoperabilidade terá a virtualidade de corresponder aos desígnios de modernização administrativa que se buscam atualmente.

Segue-se Lucas Silvestre Cortizo, Mestrando em Direito e Informática (em fase escolar), que subsume o seu contributo ao tema "*Blockchain* e *e-Government* (paradigmas e perspetivas)", através do qual tenta perspetivar se as soluções inerentes à *Blockchain*, enquanto tecnologia de registo distribuído, poderão servir à consecução dos objetivos visados, no contexto da União Europeia, ao abrigo do *e-Government* (Administração Pública em linha, na sua tradução institucional), na medida em que este demanda que as informações se encontram disponíveis em todos os Estados-Membros da União, através de soluções que assegurem a sua integridade e autenticidade.

Encontramos ainda o contributo de Victor Moreira Mulin Leal, Mestrando em Direito e Informática (em fase escolar), com o tema "A tecnologia *Blockchain* como plataforma de interoperabilidade na União Europeia? Um estudo a partir da Decisão (UE) 2015/2240". O Autor visa aferir se as soluções associadas à *Blockchain* se mostram suficientemente desenvolvidas para promover a interoperabilidade de dados entre os serviços públicos dos diversos Estados-Membros e, simultaneamente, acautelar o elevado padrão de proteção de dados que se pretende promover no contexto da União Europeia, especialmente aquele que resulta do atual RGPD (Regulamento Geral sobre a Proteção de Dados).

A **PARTE II – "Direitos fundamentais e cidadania na era digital"** conta com os contributos de Marcelo Porrua e de João Ferreira.

Marcelo Porrua, Mestrando em Direitos Humanos (em fase escolar), aborda o tema "A Comissão Nacional de Proteção de Dados (CNPD) como instrumento de governança democrática em Portugal". No seu texto, partindo da ideia de que a democracia material se reflete na dinâmica de proteção de direitos fundamentais, disserta, quanto ao direito fundamental à proteção de dados, sobre a forma como a CNPD é capaz de efetivar os mecanismos de proteção desse direito à luz do RGPD.

Por sua vez, João Ferreira, Mestrando em Direito da União Europeia (em fase de preparação da dissertação), equaciona "Pistas para uma cidadania à luz da interoperabilidade". No seu contributo, o Autor analisa as potencialidades da interoperabilidade, enquanto método que afasta obstáculos ao desenvolvimento de um Mercado Único Digital, no exercício futuro da cidadania europeia, nomeadamente ao facilitar as interações entre os cidadãos, as empresas e os serviços públicos em todos os Estados-Membros.

Na **PARTE III – "Tutela jurisdicional efetiva e justiça eletrónica"**, contam-se os contributos de Nelson Alex Lorenz e Tiago Branco da Costa.

Nelson Alex Lorenz, Mestrando em Direito da União Europeia da Escola de

Direito da Universidade do Minho e em Ciência Jurídica pela Universidade do Vale do Itajaí – UNIVALI, Brasil (em fase escolar), debruça-se sobre o "Regulamento (UE) 2018/302 contra a discriminação digital na União Europeia e a apuração da prática do *geoblocking* e *geopricing* no Brasil". No texto, o Autor trata da discriminação digital verificada no contexto do *e-commerce* e o seu impacto nas liberdades de circulação que caracterizam o contexto da União a fim de analisar a realidade brasileira, por conta de uma decisão judicial que teve na base a atividade de operadores económicos que optaram por praticar preços diferenciados por referência à localização digital dos consumidores.

Já Tiago Branco da Costa, Mestrando em Direito dos Contratos e Empresas (em fase de preparação da dissertação), trata do tema "A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados", onde analisa o regime da responsabilidade civil do responsável pelo tratamento à luz do RGPD, a fim de intuir as dificuldades dele resultantes, nomeadamente em sede do ónus da prova emergente dos termos deste ato legislativo.

Por último, na **PARTE IV – "Desafios prospetivos do Mercado Único Digital"**, esta obra conta com os contributos de Leandra Dias, Nataly Carvalho Machado e Larissa Coelho.

Leandra Dias, Mestre em Direito Judiciário e *Product Owner* de soluções de gestão na área de Recursos Humanos, participa nesta obra com um texto intitulado "O papel da tecnologia na busca pela conformidade com o RGPD", através do qual equaciona quais as medidas tecnológicas e organizacionais que poderão ser implementadas para permitir, ao responsável pelo tratamento, uma maior segurança de conformidade à luz do RGPD (Regulamento Geral sobre a Proteção de Dados).

Segue-se o contributo de Nataly Carvalho Machado, Mestranda em Direito da União Europeia (em fase escolar), intitulado "Princípio da integração ambiental: um guia a direcionar projetos de cidades inteligentes na União Europeia", através do qual problematiza como a União Europeia visa integrar a tecnologia na construção de cidades inteligentes, nomeadamente para se dotar de sistemas energéticos mais sustentáveis, sob a lente do princípio da integração ambiental.

Por fim, Larissa Coelho, Doutoranda da Escola de Direito da Universidade do Minho e Bolseira de Doutoramento da Fundação para a Ciência e para a Tecnologia (FCT), abordou a temática "A inteligência artificial e a questão constitucional". Com o seu texto, a Autora problematizou o impacto da tecnologia no quadro dos novos problemas constitucionais, partindo da inquietação de saber se esta será uma fonte de poder ou um meio para o exercício do poder.

Por fim, cabe dedicar este e-book às Ex.mas Sras. Dras. Isabel Henriques e Célia Rocha pela criteriosa gestão financeira deste Projeto.

Alessandra Silveira
Joana Covelo de Abreu
Larissa Coelho

O princípio da autonomia procedimental e o procedimento para concessão de visto pelos Estados-Membros da União Europeia. Os novos desafios da interoperabilidade em matéria de vistos

Laura Gomes Rodrigues*

RESUMO: O Direito Administrativo Global abarca realidades parciais como o Direito Administrativo da União Europeia. Um dos princípios deste último é o princípio da autonomia institucional e procedimental dos Estados-Membros, o qual tem de ser respeitado por todos os agentes da União, tanto administrativos como legislativos. Tal princípio dá aos Estados-Membros alguma liberdade na conformação do direito da União, na medida em que deixa a seu cargo a determinação da sua organização, funcionamento e procedimento administrativos. Exemplo desta autonomia interna é o procedimento para concessão de visto, que apesar de ser imposto por Regulamento, deixa alguma margem de apreciação às autoridades internas. Tal documento assume larga importância no âmbito europeu e global por se tratar de um ato de reconhecimento transnacional. Quanto a este ato normativo está na ordem do dia uma significativa alteração legislativa.

PALAVRAS-CHAVE: Direito Administrativo Global – Direito Administrativo da União Europeia – Princípio da Autonomia Institucional – Procedimental dos Estados-Membros – Visto

ABSTRACT: The Global Administrative Law englobes partial realities such as European Union Administrative Law. One of its principles is the Member State procedural and institutional autonomy, wich has to be respected by all European agents, both administrative and legislative. This principle gives to the Member States some freedom in forming the European Union law, because it allows them to determine its administrative organization, operation and procedure. An example of this internal autonomy it's the visa granting procedure, because despite the Regulation impositions, it gives some reflection margin to internal authorities. Visa it's a document of great importance in european and global context, since it's a transnational recognition act. On the european agenda, it´s a significant legislative change to this normative act.

KEYWORDS: Global Administrative Law – European Union Administrative Law – Principle of Member State Procedural and Institutional Autonomy – Visa

* Licenciada em Direito pela Escola de Direito da Universidade do Minho. Mestranda em Direito Administrativo, na área de especialização de Justiça Administrativa na Escola de Direito da Universidade do Minho.

1. O direito administrativo da União Europeia como parte do direito administrativo global

Há muito se percebeu que a ideia de Estado nas suas três componentes tradicionais - território, povo e soberania -, enquanto elemento estruturante do direito administrativo está ultrapassada. Hoje, com os efeitos da globalização, a satisfação dos interesses públicos primários globais da sociedade como o ambiente, a saúde pública ou os mercados financeiros, extrapolam a capacidade do Estado individualmente considerado.[1] Este fenómeno gerou assim a dispersão das competências típicas de um Estado para um contexto transnacional onde esses interesses são assegurados por várias entidades internacionais. Assim, ocorreu: a transferência de porções de soberania para agentes transnacionais; a partilha de tarefas entre as várias administrações dos Estados; e a passagem de competências tradicionalmente públicas para agentes privados.[2]

Para regulamentar a atuação transnacional de todos estes entes, e porque o direito administrativo nacional não permite encontrar resposta para todas as questões transfronteiriças que surgem no âmbito global, nasce o *direito administrativo global*.[3] Direito Administrativo é o conjunto de normas e princípios que regulam a atuação da administração pública de um determinado Estado. O direito administrativo global (DAG) define-se como o conjunto de mecanismos, princípios, normas organizatórias e de funcionamento que regulamentam a atuação administrativa e controlam as relações jurídicas entre os diversos atores globais, como os Estados, as organizações internacionais e ainda as entidades privadas, sem uma hierarquia e sem fundamento constitucional. Este Direito apoia-se nos princípios basilares reconhecidos por todos os Estados - proporcionalidade, dever de fundamentação, processo justo e razoabilidade.[4]

Um dos sistemas transnacionais que integram a administração global é a União Europeia (UE). O direito administrativo da UE é, portanto, uma das fontes de DAG na medida em que os seus tratados, regulamentos e diretivas constituem a base da regulação normativa da administração orgânica e funcionalmente europeia, ou seja, das instituições, órgãos e organismos da União, mas também das administrações públicas dos Estados-Membros, assegurando a harmonia da resposta aos problemas administrativos.

2. A administração pública dos Estados-Membros como administração pública funcionalmente europeia

A UE, à semelhança dos Estados, tem também funções legislativas, jurisdicionais e administrativas. Quanto à função administrativa, esta é regulada pelo seu direito administrativo - o conjunto de regras e princípios que regulam o exercício da função específica da execução administrativa das normas previstas nos tratados constituintes da União e nos atos adotados tendentes à sua aplicação.

---

[1] Ming-Sung Kuo, "Inter-Public Legality or Post-Public Legitimacy? Global Governance and the Curious Case of Global Administrative Law as a New Paradigm of Law", *Jean Monnet Working Paper 07/11* (Nova Iorque: NYU School of Law, 2011).

[2] Miguel Prata Roque, *A dimensão transnacional do direito administrativo* (Lisboa: AAFDL, 2014).

[3] Benedict Kingsbury, "Introdução: governança global e direito administrativo global na ordem legal internacional", *Revista de Direito Administrativo* 261 (2012).

[4] Peter L. Lindseth, *Equilibrium, Demoi-cracy, and Delegation: On the 'Administrative, not Constitutional' Legitimacy of European Integration*, *Jean Monnet Working Paper 07/13* (New York: New York University School of Law, 2013).

A UE segue uma estrutura descentralizada da função administrativa, na medida em que o seu exercício cabe não só às suas próprias instituições, órgãos e organismos, como ainda é confiada às administrações públicas dos vários Estados-Membros (EM). O direito administrativo da UE não assenta, portanto, no princípio clássico da separação de poderes como ocorre no direito interno de cada Estado.[5]

Independentemente da terminologia adotada, na doutrina é clara a distinção entre três tipos de administração pública da UE do ponto de vista da aplicação por via administrativa do seu direito: aquela efetivada pelas suas instituições, órgãos e organismos - *administração organicamente europeia*; a levada a cabo pelas administrações públicas dos diferentes EM - *administração funcionalmente europeia*; e, por fim, a que mobiliza tanto os primeiros como os segundos, através de procedimentos compostos tendentes a uma decisão única.[6]

Entre as diferentes autoridades envolvidas na atuação administrativa - administração orgânica e a funcionalmente europeia -, há uma clara interdependência e cooperação. O direito administrativo da UE tem, portanto, um caráter transnacional e "mestiço" uma vez que assenta em várias fontes normativas, por um lado a ordem jurídica europeia, por outro as ordens jurídicas de cada EM.[7]

3. O Princípio da Autonomia institucional, procedimental e processual dos Estados-Membros como base da dinâmica jurídico-administrativa da União Europeia

Como vimos no ponto anterior, as Administrações Públicas nacionais dos EM atuam como administrações funcionalmente europeias, dado que aplicam direito da UE (DUE) na sua função administrativa interna. Esta atuação administrativa assenta essencialmente em três princípios: subsidariedade, cooperação leal e autonomia.

O princípio da autonomia institucional, procedimental e processual dos EM é uma peça chave do processo de integração europeu. Todavia este princípio tem um conteúdo pouco claro quanto à sua veste institucional e procedimental, uma vez que nasceu da criação jurisprudencial do Tribunal de Justiça da União Europeia (TJUE) e não se encontra positivado em qualquer norma escrita.[8] Já quanto à vertente processual, este encontra consagração no artigo 19.º, n.º 1, 2.ª parte do Tratado da União Europeia (TUE). Tal princípio no seu todo significa que cabe a cada EM a decisão quanto aos meios e formas internas de acautelar as soluções jurídicas decorrentes do DUE, como normas decorrentes de regulamentos e de diretivas. Assim, apesar de ser o direito interno de cada Estado a decidir quais os órgãos competentes e qual o procedimento de execução das normas europeias, não há total liberdade nesta tarefa, pois tal determinação interna está limitada à garantia de eficácia e de efetividade do DUE.

Esta autonomia encerra três dimensões: a) autonomia institucional - cabe a cada EM designar autonomamente quais os quadros de organização administrativa

[5] Karl-Peter Sommermann, "Towards a Common European Administrative Culture?" *Jean Monnet Working Paper 28/13* (Nova Iorque: NYU School of Law, 2013).
[6] Alice Rocha da Silva, "As diretivas europeias como norma reguladora do direito administrativo global", *Revista de Direito Internacional* 13, n.º 3 (2016).
[7] Marta Moutinho Barros, "Europeização da Organização Administrativa portuguesa: Seu alcance e efeitos na Administração Pública Nacional" (Dissertação de mestrado, Universidade Católica Portuguesa, 2013).
[8] Luciano Parejo Alfonso, "El principio de la autonomía institucional y procedimental de los estados miembros de la Unión Europea", *A&C - Revista de Direito Administrativo & Constitucional* (2012), Editora Fórum, Belo Horizonte.

que irão proceder à aplicação do DUE; b) autonomia procedimental - cabe a cada EM determinar as regras procedimentais para tramitar um determinado pedido que resulte de aplicação do DUE; c) autonomia processual - cabe a cada EM fixar as vias recursórias adequadas à tutela jurisdicional dos direitos decorrentes da ordem jurídica europeia.

Para avaliar se determinada solução nacional interna assegura de igual forma os direitos decorrentes da ordem jurídica europeia face aos estabelecidos na ordem jurídica nacional são utilizados dois subprincípios de teste: o princípio da equivalência - as medidas adotadas para efetivar DUE em determinado EM, em comparação com as previstas para pretensões similares de natureza puramente interna, não podem ser menos favoráveis do que as primeiras; e o princípio da efetividade em sentido estrito - a organização administrativa, ou as suas soluções procedimentais, não podem tornar excessivamente difícil ou impossível na prática o exercício dos direitos decorrentes da ordem jurídica europeia.

Com base neste princípio, a UE pode obrigar os EM a atingir determinados fins e objetivos; contudo, não pode impor-lhes um determinado meio de os atingir. A finalidade última deste princípio é conseguir uniformidade na aplicação administrativa do DUE pelos vários Estados sem desconsiderar algum juízo crítico que os últimos devam ter nestas matérias. Tal homogeneização de práticas administrativas leva ao estabelecimento de uma administração em rede que assenta essencialmente em dois pontos: i) cooperação mútua entre as administrações nacionais dos EM e cooperação entre estes e as instituições, órgãos e organismos da UE; ii) eficácia de um ato praticado por uma entidade nacional no território de um outro EM, tanto porque o ato vale em todo o território da UE por força de uma disposição de DUE ao abrigo do qual foi adotado, como pela extensão territorial da eficácia do ato pela imposição europeia de reconhecimento mútuo.[9]

4. Reconhecimento transnacional de atuações administrativas estrangeiras: o visto como ato administrativo transnacional

Hoje o direito administrativo não pode ser apenas pensado como intrinsecamente ligado a um princípio de territorialidade, na perspetiva de que as autoridades administrativas apenas exercem competências com aplicação dentro do território de um Estado. Pelo processo de globalização que vivemos atualmente, há necessidade de estabelecer um reconhecimento transnacional das atuações administrativas, de modo a torná-las eficientes e céleres, simultaneamente assegurando a prossecução do interesse público e a salvaguarda das garantias dos administrados. Este reconhecimento mútuo é já adotado e até imposto no contexto da UE.

O ato administrativo transnacional define-se como um ato jurídico, praticado pela administração de um determinado Estado e que produz por si só efeitos jurídicos extraterritoriais. No âmbito europeu significa que um ato praticado por uma autoridade da administração pública nacional de um dos EM terá repercussões em todo o território da União. Esta eficácia transnacional deriva, como vimos no ponto anterior, da ideia de administração em rede e assenta em três objetivos da integração europeia: i) desativação das fronteiras entre EM (artigo 3.º n.º 2 TUE); ii) criação de um sistema descentralizado de execução do DUE; iii) estabelecimento do

[9] Artur António Grando, "O Acto Administrativo Transnacional na Supranacionalidade da União Europeia e na Intergovernamentabilidade do MERCOSUL" (Dissertação de mestrado, Universidade do Porto, 2013).

reconhecimento mútuo como princípio estruturante nas matérias de funcionamento e regulação do mercado interno e na matéria do espaço de liberdade, segurança e justiça - o que a administração de um Estado decide tem de valer igualmente no território de um outro EM, salvo, por exemplo, os casos em que se verifiquem circunstâncias de restrições justificadas às liberdades económicas ou se privilegie uma determinada realidade jusfundamental.

Um dos exemplos paradigmáticos de ato administrativo transnacional são os vistos. O visto é um ato produzido por uma autoridade administrativa de um EM que permite a um determinado indivíduo proveniente de um Estado terceiro face à União, por um curto período de tempo, entrar e circular em todo o território da UE (e também no espaço Schengen), ou seja, no território dos 28 EM. Esta lógica aplica-se por força do Regulamento n.º 810/2009[10] que estabelece o Código Europeu dos Vistos (CV), portanto nesta matéria verifica-se uma intensificação do reconhecimento mútuo por força legislativa. Um regulamento é um ato legislativo vinculativo, cujo conteúdo é diretamente aplicável no ordenamento jurídico dos EM. De modo a assegurar harmonia na decisão administrativa de concessão do visto, o regulamento em causa estabelece o próprio procedimento e condições a que as autoridades nacionais devem obedecer. Todavia, para não contender com o princípio da autonomia procedimental, o regulamento deixa alguma liberdade e margem de conformação para as administrações nacionais adotarem o procedimento de acordo com as suas ordens jurídicas internas.

O acórdão Rahmanian Koushkaki contra Alemanha[11] versa precisamente sobre esta matéria. Em causa estava o indeferimento de um pedido de emissão de um visto uniforme com base na avaliação da entidade administrativa competente que entendeu não estarem preenchidas as condições para tal concessão. Da análise deste acórdão depreende-se desde logo uma ideia principal: as entidades administrativas dos Estados-Membros com competência para apreciar a existência de condições para emitir um visto uniforme estão vinculadas ao procedimento constante do CV. Tal justifica-se porque estando em causa um regulamento, falamos de uma fonte de direito da União Europeia com eficácia vinculativa direta nas ordens jurídicas dos EM. Portanto, pelo princípio do primado do direito da União, as entidades nacionais têm de observar a sua preferência aplicativa face aos seus direitos internos. Por conta deste princípio, há que atentar ao princípio da autonomia institucional, procedimental e processual dos Estados já que o mesmo, surgido no seio da União, vai determinar de que forma os procedimentos nacionais serão despoletados e tramitados, sem contender com a efetividade do DUE. No caso interessa-nos a vertente procedimental, que determina caber ao direito interno de cada Estado o estabelecimento da atuação administrativa procedimental mais adequada para prosseguir os fins da União. Neste acórdão o TJUE veio estabelecer que, quanto à emissão de vistos, impõe-se a atribuição de certa margem de valoração aos Estados para apreciarem, casuisticamente e com base na situação social, económica e política que envolve o requerente, se as condições de atribuição de visto estão asseguradas. Caso entendam positivamente, teremos um ato emanado por uma entidade administrativa interna de um EM, em âmbito parcial, a conferir o direito a certo indivíduo de circular livremente, ainda que por determinado

[10] Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho de 13 de julho de 2009 que estabelece o Código Europeu de Vistos (Código de Vistos).
[11] Acórdão do Tribunal de Justiça da União Europeia, Rahmanian Koushkaki contra República Federal da Alemanha, 19 de dezembro de 2013, caso C-84/12.

período de tempo, em todo o território da União Europeia, ou seja, num âmbito transnacional, daí a atribuição da designação de ato administrativo transnacional aos vistos de curta duração.

5. Interoperabilidade. A digitalização das administrações internas como meio de estabelecimento do Mercado Único Digital na União Europeia

No início desta década, a Comissão Europeia adotou a estratégia "Europa 2020" com vista ao crescimento inteligente e sustentável, melhorando a competitividade e produtividade dos Estados e assegurando uma economia social de mercado. No âmbito desta iniciativa, em maio de 2010 foi lançada a "Agenda Digital para a Europa" que pretendeu impulsionar a economia europeia através da implementação de medidas de desenvolvimento das tecnologias digitais dentro das empresas e dos agentes e serviços públicos dos Estados-Membros, mas também junto dos cidadãos.

Em meados de 2017, a Comissão Europeia comunicou o novo quadro europeu da interoperabilidade[12] que veio atualizar e alagar o quadro adotado em 2010, ajudando o estabelecimento do Mercado Único Digital. O objetivo principal foi, e ainda é, o de modernizar a atuação administrativa, fomentando uma transformação digital da administração pública na Europa e reforçando a presença e utilização das tecnologias de informação e comunicação (TIC), o que a tornará mais célere, económica, garantística, transparente e eficaz. A interoperabilidade desenvolve-se em três vertentes - operacional, semântica e tecnológica - o que permitirá a colaboração digital e a troca de informações entre os serviços e autoridades administrativas públicas, os cidadãos e as empresas. Para executar esta estratégia europeia de interoperabilidade foi criado o programa ISA (2010-2015) - Soluções de Interoperabilidade para as Administrações Públicas Europeias. Tendo sido relevante o contributo deste programa no intercâmbio eletrónico de informações entre as administrações europeias, foi adotado o seu sucessor - ISA^2 (2016-2020),[13] de modo a manter e reutilizar as soluções adotadas no âmbito do ISA, que criaram uma interoperabilidade transfronteiriça e intersetorial, através do aproveitamento da administração em linha e da democracia eletrónica entretanto desenvolvida. Ora com este programa pretende-se a modernização das administrações públicas europeias e consequentemente o estabelecimento do Mercado Único Digital.

Para podermos atingir uma administração em linha, ou seja, uma rede de administrações públicas europeias que cooperam entre si, tanto pela partilha de informação, como pela homogeneização da sua atuação, como ainda pelo reconhecimento mútuo das suas atuações, é eminente a necessidade de que todas elas se encontrem no mesmo patamar evolutivo - todas devem estar adaptadas aos novos avanços tecnológicos.

Em Portugal, para responder às exigências europeias de informatização do programa Portugal 2020 (concretização interna portuguesa do programa Europa 2020) foi criada, em 2007, a Agência para a Modernização Administrativa (AMA), que é responsável pela promoção e desenvolvimento da modernização administrativa em

[12] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões "Quadro Europeu da Interoperabilidade - Estratégia de execução"*, COM(2017) 134 final, Bruxelas, 23 março 2017.

[13] Decisão (UE) 2015/2240 do Parlamento Europeu e do Conselho, de 25 novembro 2015, que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus.

Portugal, aproveitando as potencialidades das TIC, consequentemente melhorando a prestação dos serviços públicos e simplificando a relação entre a administração e os utentes. No contexto da desmaterialização e melhoramento dos processos da Administração Pública, e de forma a dar resposta à necessidade de comunicação e troca de informação eletrónica entre entidades públicas e privadas, foi implementada em 2011 a Plataforma de Interoperabilidade da AP. Para 2019 a AMA tem como grandes objetivos estratégicos melhorar a qualidade da distribuição de serviços públicos, implementar estruturas tecnológicas para apoiar a modernização administrativa e simplificar o relacionamento entre a administração e os administrados. Visa alcançá-los desde logo promovendo plataformas como a Chave Móvel Digital e medidas SIMPLEX+ e desenvolvendo novas aplicações online. Procurará ainda auxiliar o governo na implementação de medidas de modernização e simplificação administrativas e cooperar com entidades estrangeiras nestes domínios.

6. Novos avanços em matéria de vistos na União Europeia

Para dar apoio à execução das políticas da União em matéria das TIC, em 2011 foi criada a eu-LISA - Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça. De entre outras funções, a eu-LISA, por meio da prestação de apoio tecnológico, permite aos países Schengen trocar dados sobre os vistos e fazer o intercâmbio de informações. Afinal, esta agência gere três sistemas informáticos: Sistema de Informação sobre Vistos (VIS), Sistema de Informação Schengen (SIS II) e Eurodac, a fim de garantir mais segurança aos cidadãos em todo o espaço Schengen.

No âmbito da interoperabilidade, o sistema VIS tem larga importância e é um elemento importante no estabelecimento de uma política comum de vistos da União. Desde logo, dos 28 Estados-Membros da União Europeia, 22 usam o VIS, e ainda mais quatro países associados, ou seja, no total estão envolvidas 26 administrações nesta partilha de informações. Assim, este apresenta um funcionamento que se intui simplificado: quando um cidadão nacional de um Estado terceiro quer entrar pela primeira vez em território da União, dirige-se ao consulado de um qualquer EM no seu país de origem e requer um visto. Os serviços administrativos do consulado vão então introduzir no sistema VIS a informação pessoal do requerente: dados biográficos, fotografia e impressões digitais, e posteriormente irão decidir conceder ou não o visto conforme estejam verificados ou não os requisitos legais. A partir desse momento qualquer outra entidade de segurança de fronteira (que utilize o VIS) que necessite de saber os dados pessoais dessa pessoa pode, desde que observando as demandas em sede de proteção de dados pessoais, aceder ao sistema e ainda aceder ao histórico de anteriores vistos pedidos, concedidos, indeferidos, revogados, estendidos ou encurtados. Isto permite, portanto, uma intercomunicabilidade e cooperação entre entidades administrativas que concedem vistos nos consulados e controlam as fronteiras nos diversos EM através de uma verdadeira rede de partilha de informações que permite mais celeridade nos procedimentos de concessão, mais segurança para viajantes porque se previnem furtos de identidade e ainda redução de casos de "visa shopping".

Face à instabilidade política que rodeia o território da UE, hoje deparamo-nos com uma grave crise de migrantes e refugiados políticos e de guerra.[14] Todavia

[14] Étienne Bassot and Wolfgang Hiller, "The Juncker Commission's ten priorities: State of play in mid-2017", Bruxelas, Parlamento Europeu, julho 2017, em www.europarl.europa.eu.

os Estados não podem simplesmente fechar as suas portas ao mundo exterior, um processo de integração económica, cultural e social a nível global torna-se imperativo para dar resposta aos novos desafios de segurança e evolução tecnológica.

Para responder a estas mudanças na sociedade, em 2017 a Comissão Europeia fez uma proposta de Regulamento para realização de várias alterações em matéria de política comum de vistos, por criação de um quadro para a interoperabilidade entre sistemas de informação da UE.[15] Tal proposta foi acolhida pelo Parlamento Europeu e Conselho, pela muito recente adoção do Regulamento 2019/817, em 20 de maio do presente ano.[16]

Por um lado, o VIS foi atualizado com o objetivo de ampliar o seu âmbito, acrescentando, ao sistema, os vistos de longa duração e de habitação e, ainda, procurar eliminar ou, pelo menos, reduzir falhas de informação no sistema através de uma interoperabilidade plena com outras bases de dados europeias.

Por outro lado, a par da atualização dos sistemas de informação já disponíveis, serão acrescentados três outros: Sistema de Entrada/Saída (SES), que pretende substituir o método antigo de carimbo de passaporte passando a efetivar-se por um registo eletrónico no portal para estadias de curta duração; Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e ainda o Sistema Europeu de Informação sobre Registos Criminais de nacionais de países terceiros (ECRIS-TCN). Entre todos estes sistemas estabelece-se uma interoperabilidade por meio da sua interligação e intercomunicabilidade, permitindo uma mútua complementaridade.

Quanto ao Código de Vistos, que estabelece os procedimentos e condições para emissão de vistos de forma uniformizada para todos os EM da União, atualmente encontra-se em revisão por proposta da Comissão Europeia, datada de março de 2018,[17/18] sendo que, no passado mês de fevereiro, o Conselho confirmou o acordo sobre as alterações a realizar. O seu objetivo passa por reforçar a política comum de vistos, tornando os procedimentos mais simples e rápidos, reforçando os controlos de segurança e, ainda, implementando medidas de pedidos digitais de vistos, através do preenchimento de formulário simplificado disponível online. Consequentemente pretende-se fomentar a economia da UE através da simplificação da atividade turística melhorando, assim, as condições para os viajantes legítimos. De entre algumas das medidas propostas, temos o estabelecimento de políticas comuns de retorno ao Estado terceiro em caso de recusa de concessão de visto, aumento das taxas cobradas para dar cobertura aos custos do tratamento dos pedidos de visto, atualização dos vistos de longa duração, estabelecimento de distinção entre vistos de curta duração e vistos de turismo, e ainda elevação de critérios de segurança no estabelecimento da

[15] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à criação de um quadro para a interoperabilidade entre os sistemas de informação da UE (fronteiras e vistos) e que altera a Decisão 2004/512/CE do Conselho, o Regulamento (CE) n.º 767/2008, a Decisão 2008/633/JAI do Conselho, o Regulamento (UE) 2016/399 e o Regulamento *(UE) 2017/2226*, COM(2017) 793 final, Estrasburgo, 12 dezembro 2017.

[16] Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 maio 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho.

[17] Maria Margarita Mentzelopoulou and Costica Dumbrava, "Revision of the Community Code on Visas", Bruxelas, Parlamento Europeu, julho 2018, www.europarl.europa.eu.

[18] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.° 810/2009 que estabelece o Código Comunitário de Vistos (Código de Vistos), COM(2018) 252 final, Bruxelas, 14 março 2018.

lista de Estados a cujos cidadãos é requerida a posse de um visto de trânsito quando atravessem a fronteira externa da UE.

7. Considerações Finais

A sociedade vive hoje dois fenómenos paralelos, a *globalização* e a *europeização*. Face aos desafios atinentes ao terrorismo, às alterações climáticas, às crises migratórias, ao desenvolvimento tecnológico e científico, é cada vez mais eminente que os Estados não podem fechar as suas portas ao mundo exterior. Aliás, um processo de integração económica, cultural e social a nível global torna-se imperativo para dar resposta eficiente a estes novos desafios. Também a nível regional surgem estas preocupações; por isso é que a UE tem trabalhado no sentido de implementar medidas como o Mercado Único Digital e novas políticas de segurança e controlo de entrada e saída de pessoas do seu território.

A adoção de uma política comum de vistos em 2010 permitiu facilitar as deslocações legítimas para a União Europeia, e entre os seus EM, ajudou no crescimento do turismo e facilitou em muito as trocas comerciais. Concomitantemente é também essencial para garantir a segurança dos cidadãos pois previne imigração irregular e estabelece critérios uniformizados para a permissão de entrada no espaço Schengen. Teve, portanto, um papel fundamental no estabelecimento do espaço de liberdade, segurança e justiça da União. Face às novas realidades sociais e tecnológicas é premente uma reforma desta política, uma vez que os procedimentos atuais para emissão de vistos são morosos, complexos e desatualizados, pelo que hoje, em vez de facilitarem tal circulação, estão já a prejudicar essa liberdade. São necessários mais recursos, novos procedimentos e plataformas eletrónicas modernas para a comunicação entre a administração e os cidadãos.

A interoperabilidade tem aqui um papel de particular relevância porque permite que esta modernização administrativa se alastre a todo o território da UE. As administrações internas de cada EM têm de se atualizar para poderem entrar nesta rede de partilha e troca de informações e assim tirar para si e para os seus cidadãos o melhor proveito dessa intercomunicabilidade.

Em suma o que se pretende é uma Europa atual, modernizada e adaptada ao aproveitamento das vantagens que advêm das novas tecnologias que vão surgindo e que estão em crescente (senão exponencial) evolução nos dias de hoje.

Blockchain e e-Government (paradigmas e perspectivas)

Lucas Silvestre Cortizo*

RESUMO: Blockchain é uma tecnologia de registro distribuído que encontra na descentralização, criptografia e estrutura linear / temporal a sua segurança e confiabilidade. Por isso, é pertinente pensá-la para viabilizar a implementação de um e-Government que precisa de registro com soluções de integridade e autenticidade. Neste trabalho são apresentados vários casos de utilização da Blockchain na Administração Pública e no contexto da União Europeia para fins de compatibilidade com as tecnologias de livro-razão distribuído, tendo por referência o Plano de Ação Europeu 2020 para a Administração Pública em linha e a Resolução 2016/2007 (INI).

PALAVRAS CHAVE: Blockchain – Administração Pública em Linha – Administração Pública

ABSTRACT: Blockchain is a distributed ledger technology that finds in decentralization, cryptography and linear / temporal structure its security and reliability. Therefore, it is pertinent to think of it to enable the implementation of an e-Government, which needs registration with solutions of integrity and authenticity. There are a couple of cases of Blockchain's use in Public Administration and in the European Union's context for compatibility with distributed ledger technologies, bearing as references the European Union e-Government Action Plan 2020 and the Resolution 2016/2007 (INI).

KEYWORDS: Blockchain – e-Government – Public Administration

* Mestrando em Direito e Informática da Universidade do Minho – Portugal. Advogado.

1. Notas Introdutórias

Uma tecnologia que envolve todos os elementos para despertar curiosidade, eis que a *Blockchain* a cada dia mostra uma nova faceta e uma diferente utilização. Na tradução literal, *Blockchain* (BC) é uma cadeia de blocos que consegue, através da descentralização, garantir autenticidade e segurança a operações. Analogicamente, imagina-se um livro de milhares de páginas e cada página uma sequência linear de quadrados ou blocos; este livro vai ser acessado, em tempo real, por todos os participantes, obedecendo ao tripé: descentralização, autenticidade e integridade.

De maneira mais técnica, uma definição possível diz-nos que a *Blockchain* envolve uma matriz que contém uma lista de dados organizados de forma linear, de acordo com o tempo, em lista compartilhada de crescimento contínuo com acesso público a registros criptografados, "seguros de qualquer adulteração ou revisão".[1]

Originalmente, a tecnologia serviu para registrar o histórico de transações da criptomoeda *Bitcoin,*[2] entretanto, atualmente, já há casos de uso na *Internet* das Coisas (IOT), Inteligência Artificial, *Supply Chain*, transações digitais e nos casos que serão analisados no âmbito do *e-Government*. É por isso que muito se fala que a *Blockchain* é uma tecnologia disruptiva, pois consegue aliar a segurança criptográfica com uma revolução no armazenamento de dados em diversos setores.

No que diz respeito à segurança, a *Blockchain* utiliza a criptografia, uma ciência egípcia milenar[3] que foi adaptada a novas realidades digitais. A maneira como o registro é feito em cada bloco é o que garante a autenticidade e integridade do sistema *Blockchain*: dentro do bloco, além dos dados a serem registrados, há um resultado da operação *hash* do bloco imediatamente anterior, ou seja, um algoritmo matemático que recebe um *input* de dados de determinado tamanho e comprime a um tamanho fixo em uma "função *one-way*",[4] matematicamente irreversível.

Trata-se, então, de uma função criptográfica que reúne dados e faz uma "digestão", transformando-os sempre numa sequência de igual tamanho (o "*digest*"). Cada bloco carrega a "*message digest*" do bloco imediatamente anterior, o que liga os blocos entre si, e pelo fato da *Blockchain* ser uma estrutura linear,[5] consegue-se a imutabilidade não apenas dos dados inseridos, mas da ordem temporal da cadeia inteira. No final das contas, não é possível falsificar os dados de um bloco, afinal teria que alterar o bloco posterior e depois o posterior ao posterior e assim sucessivamente: para adulterar um bloco precisa alterar toda a cadeia de blocos. E é devido a isso que "muito mais que algoritmos criptográficos, o one-way hash é a força motriz da criptografia moderna".[6]

A autenticidade e integridade da *Blockchain* sinaliza uma possível solução para o ideal de uma Administração Pública em linha. O que precisa ser analisado é como eficientemente compatibilizar os dois modelos para que seja possível atingir a plenitude de um e-*Government* através de um modelo seguro em que os cidadãos depositem a sua

---

[1] Laza Kekic, "The Economist Intelligence Unit's index of democracy", *The Economist*, December 21, 2007, 1-11.

[2] Huasheng Zhu e Zach Zhizhong Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China", *Financial Innovation*, 2, no. 1 (2016): 29.

[3] Stephen Pincock, *Codebreaker: the history of codes and ciphers* (New York: Walker & Company, 2006).

[4] Gerald P. Dwyer, "The economics of Bitcoin and similar private digital currencies*", Journal of Financial Stability* 17 (2015): 81-91.

[5] Tong Jin, et al., "Blockndn: A bitcoin blockchain decentralized system over named data networking", *Ubiquitous and Future Networks (ICUFN)*, 2017 Ninth International Conference (Beijing: IEEE, 2017).

[6] Bruce Schneier, "Cryptanalysis of MD5 and SHA: Time for a New Standard", *Computerworld* 19 (2004).

confiança. Dentre uma perspectiva coletiva, toda mudança de paradigma – inclusive o proposto pela *Blockchain* – precisa passar por um processo de revolução no pensamento social.

2. Contexto Histórico

Se de maneira simples, a *Blockchain* é apenas uma ferramenta de armazenamento de dados, precisa-se entender o contexto de seu surgimento para vislumbrar o potencial disruptivo. Casey e Vigna, em sua obra,[7] desenvolvem uma evolução histórica elucidativa para explicar como a *Blockchain* promete alterar um sistema-padrão de Contabilidade que é usado há séculos.

Até o Século XIII, a Europa praticamente não possuía conhecimento contábil-matemático, o que mudou com a aritmética ensinada pelo livro *Liber Abaci* do mercador Fibonacci que, a partir do ano 1202, trouxe dos árabes conceitos matemáticos[8] que permitiram desenvolver o comércio europeu, gerando uma enorme quantidade de dados para a época que necessitavam de uma forma de armazenamento. Já em 1494, Luca Pacioli criou o sistema de partidas dobradas - ou "*double-entry bookkeping*" (DEB) - que permitiu armazenar dados de forma eficiente, através de livros de registro. Este método permite que cada informação seja registrada em livros armazenados por entidades de confiança, sendo o método que deu origem à ciência contábil. De imediato, essa técnica expandiu o volume das relações comerciais, mas sua eficiência permitiu o desenvolvimento da estrutura do Estado-governo burocrático que perdura até hoje.

A forma burocrática da Administração Pública é fruto desse método de partidas dobradas, em que os livros-registro são a fonte de prova e verdade, e as informações que nele estiverem gozam de presunção *juris tantum*. Não é à toa que o país fundador do modelo ocidental de Administração Pública,[9] a França, na mesma época usou o DEB para o controle na arrecadação de tributos, de forma inédita.[10] Portugal foi um dos países pioneiros europeus a adotar o DEB como modelo contábil oficial do Tesouro Real, o que se verificou a partir de 1761.[11]

Portanto, nota-se que o modelo da Administração Pública tradicional é fundamentado no sistema de partidas dobradas. E é crucial salientar que esse método de registro contábil revolucionou, primeiramente, o comércio, mas sua eficiência acabou por atingir a estrutura estatal que o adotou como fundamento da Administração Pública (a mesma expectativa ocorre em relação à *Blockchain* que surgiu no contexto da criptoeconomia, mas é vislumbrada para ser uma solução para a Administração Pública em linha). Esta é a revolução proposta pela *Blockchain*, não apenas pela mudança

[7] Michael J. Casey e Paul Vigna, *The Truth Machine: The Blockchain and the Future of Everything* (New York: St. Martin's Press, 2018).

[8] Laurence Sigler, *Fibonacci's Liber Abaci: a translation into modern English of Leonardo Pisano's book of calculation* (New York: Springer Science & Business Media, 2003).

[9] Francisco Mafra, "História do Direito Administrativo: idéias para um debate", *Âmbito Jurídico*, VIII, n. 20, (Fev. 2005), http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=918k.

[10] Yannick Lemarchand, "Introducing double-entry bookkeeping in public finance: a French experiment at the beginning of the eighteenth century", *Accounting, Business & Financial History* 9.2, (1999): 225-254.

[11] Delfina Gomes, Garry D. Carnegie e Lúcia Lima Rodrigues, "Accounting change in central government: the adoption of double entry bookkeeping at the Portuguese Royal Treasury (1761)", *Accounting, Auditing & Accountability Journal* 21.8 (2008): 1144-1184.

impactante no modelo burocrático-contábil da Administração Pública, mas por poder ser um instrumento para a efetivação de uma revolução ideológica, em que os cidadãos poderão confiar na tecnologia como fundamento de um *e-Government*.

O atual *mindset* social está acostumado a confiar em informações registradas de forma centralizada: afinal, para cada documento estatal emitido, existe uma referência correspondente armazenada e centralizada pela Administração Pública. A exemplo do serviço público de emissão de uma certidão de nascimento, o valor jurídico de um pedaço de papel decorre do fato de algum órgão centralizar um segundo registro com a mesma informação.

O contexto histórico de surgimento da *Blockchain* já é um indício que há falhas no atual modelo de registro que podem ser sanadas pela nova tecnologia. No ano emblemático de 2008, além da concretização da primeira criptomoeda, a empresa *Lehman Brothers* iniciou o ano publicando seu livro fiscal com a informação que havia declarado um recorde de capitalização, chegando aos incríveis 60 bilhões de dólares.[12] Apenas 9 meses depois ela declarou falência, e afetou diretamente a ordem econômica mundial. A concessão de *subprime loans* e a publicação de um balanço falso apenas é prova que as instituições são capazes de centralizar armazenamento de dados e manipular contabilidade e livros de registro, tendo em vista que dependem da reputação que possuem.[13]

3. Da segurança oferecida

Manipulação de dados centralizados significa, ao mesmo tempo, uma ameaça à segurança jurídica das relações, além de afetar a confiança depositada em instiuições, sendo um cenário que estimula o crescimento de um mercado financeiro alternativo. E foi nesse contexto de desconfiança em grandes instituições que foi criada uma moeda digital que não precisaria de uma entidade de confiança centralizadora. Mas isto não afetaria seu lastro? Segundo Nakamoto, o misterioso idealizador da *Blockchain*, a "*timestamp*", que se refere à verificação e validação da autenticidade de cada transação, garantiria o seu lastro.[14]

Alguns criticam as criptomoedas por entenderem que não existe lastro monetário e que não estão elas abrangidas pela gestão pública, capaz de regulamentar a ordem econômico-financeira por referência a desígnios de interesse público. Mas o lastro serve para assegurar uma escassez de oferta, sendo a gestão pública capaz de garantir apenas uma demanda mínima, mas não uma inelástica oferta, ou seja, o lastro público não garante uma "boa" moeda; ao contrário, pode até conduzir a uma possível moeda ruim com aceitação de mercado. E na ótica econômica, a *Blockchain* oferece uma legítima escassez, é intangível, matemática e criptograficamente garantida,[15] obedecendo, de verdade, aos fundamentos da ciência econômica.

Mas a *Blockchain*, além de fazer registro linear e temporal pelo citado *timestamp*, gera confiança por ser imutável. A arquitetura da cadeia de bloco é delineada para que

[12] "The Collapse of Lehman Brothers: a Case Study", última modificação Maio 19, 2019, https://www.investopedia.com/articles/economics/09/lehman-brothers-collapse.asp.
[13] Michael J. Casey e Paul Vigna, *The Truth Machine*.
[14] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Bitcoin.org*, https://bitcoin.org/en/bitcoin-paper.
[15] Fernando Ulrich, "A verdade sobre o lastro do Blockchain", *Moeda na era digital*, Abril 22, 2014. https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/3206256/verdade-sobre-lastro-bitcoin.

não exista entidade centralizadora (o registro fica distribuído de forma *peer-to-peer*) e os dados sejam inseridos por confirmação da maioria de todos os usuários da rede. Ou seja, uma verdadeira "democracia consensual no armazenamento de dados", onde a maioria absoluta dos usuários deve permitir o registro do bloco, que, uma vez feito, torna-se imutável pela propriedade criptográfica *hash* utilizada: cada bloco gera seu próprio *digest* que depende do conteúdo ali armazenado, eventuais tentativas de alteração do conteúdo do bloco gerariam um novo *digest*, conflitando com o *hash* original.[16]

Por segurança, o mecanismo de consenso[17] busca, na maioria da rede, uma confirmação para validar a transação, funcionando como um conjunto de regras e procedimentos que permitem manter a coerência do registro, uma vez que novas transações não são automaticamente adicionadas à cadeia de blocos. Neste caso, ficam armazenadas até a decisão majoritária da rede, que, no caso da *Bitcoin*, é por volta de 10 minutos e, após a validação consensual dos *nodes* por deliberação majoritária, a informação será inserida na *Blockchain* e não mais poderá ser adulterada.

A estrutura majoritária e consensual da tecnologia *Blockchain* já despertou curiosidade sobre se esse modelo seria compatível com o sistema eleitoral, e levantou-se questionamento se essa tecnologia poderia ser aplicada em eleições através do i-*voting*.[18] Em março de 2018, houve a primeira eleição com uso da tecnologia *Blockchain* que ocorreu em Serra Leoa,[19] graças a transparência e segurança que lhe estão associadas. Logo em seguida, ocorreu na West Virginia, EUA, a primeira votação americana parcialmente baseada em *Blockchain*.[20]

Para alguma novidade tecnológica ser aplicada a sistemas eleitorais, *a priori*, precisava ser virtualmente impossível de apresentar falhas, e é isto que oferece a criptografia de chaves públicas privadas usadas pela *Blockchain*.[21] As chaves usadas para verificar a assinatura da transação têm um tamanho de 512-bit, o que é "inconvenientemente grande"[22] e que torna o caminho inverso (partindo do *digest* gerado pelo *hash* até a descoberta da chave) uma tarefa atualmente impossível. Pela atual capacidade de todos os computadores, segundo Casey, a rede demoraria "4,500 trilhões trilhões trilhões de anos"[23] para, através da força bruta, conseguir quebrar o *hash* algorítmico SHA-256, famoso por proteger os dados da *Bitcoin*. Para ter-se uma ideia, este lapso temporal é "36.264 trilhões trilhões de vezes mais longo que a provável idade do universo".[24]

---

[16] Matheus Passos Silva, "A segurança da democracia e a blockchain", *Projeção, Direito e Sociedade*, v. 9, n. 1 (2018): 119-138.

[17] Tim Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems" Report, available online, (Abril, 2015). https://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems/.

[18] Ahmed Ben Ayed, "A conceptual secure blockchain-based electronic voting system", *International Journal of Network Security & Its Applications* 9.3 (2017): 01-09.

[19] Usman Chohan, "Blockchain Enhancing Political Accountability? Sierra Leone 2018 Case", SSRN (2018) http://dx.doi.org/10.2139/ssrn.3147006.

[20] Adam Reese, "America's first partially blockchain-based election takes place in West Virginia". *ETHNews*. https://www.ethnews.com/americas-first-partially-blockchain-based-election-takes-place-in-west-virginia.

[21] Conner Fromknecht, Dragos Velicanu e Sophia Yakoubov, "A Decentralized Public Key Infrastructure with Identity Retention", *IACR Cryptology ePrint Archive* (2014): 803.

[22] Paul Müller et al., "The Bitcoin Universe: An Architectural Overview of the Bitcoin Blockchain", in *11. DFN-Forum Kommunikationstechnologien*, orgs. P. Müller, B. Neumair, H. Reiser, G. Dreo Rodosek (Bonn: Gesellschaft für Informatik, 2018).

[23] Michael J. Casey e Paul Vigna, *The Truth Machine*.

[24] Ibid.

Até este momento já se demonstrou que a *Blockchain* apresenta uma arquitetura linear, temporal e segura, que funciona em modelo transparente e aberto, com extrema escalabilidade, o que torna pertinente trazê-la para uma perspectiva da Administração Pública, especialmente, para o paradigma da Administração Pública em linha.

4. Paradigmas de uso da *Blockchain* na Administração Pública em linha (*e-Government*)

Alguns Estados-Membros já estão a acelerar a transformação digital da Administração Pública tal como foi desenhada pela Comissão Europeia. Se entendermos que a plenitude de uma Administração Pública em linha é uma revolução que está em curso, torna-se necessário avaliar aqueles que já iniciaram a corrida, não sendo exagero afirmar que a Estônia está na vanguarda disruptiva: está avançada na implementação de um *e-Government* e não à toa foi o primeiro país a usar *Blockchain* a nível nacional.

A lição estoniana demonstra que a implementação do *e-Government* apenas foi possível com fundamento na *Blockchain* como arquitetura segura ideal para essa nova forma de administração. Na busca por uma assinatura digital, a Estônia desenvolveu a KSI *Blockchain*, um sistema de autenticação escalável *exabyte* com poder de ser expandida a todos usuários da rede mundial. A *Blockchain* KSI da Estônia é usada para verificação independente de todos os processos de governo e para proteger os serviços da Administração Pública em linha[25] que foi desenvolvida por conta dessa tecnologia. Essa arquitetura é capaz de processar 1 trilhão de transações por segundo e apresenta excelente rendimento energético e foi desenhada para escala industrial.

Uma vez que a arquitetura de uma Administração Pública em linha já foi comprovadamente implementada e de uma forma escalável através da *Blockchain*, o Governo estoniano encontrou as bases para desenvolver-se de forma exponencial e sem precedentes. A Estônia é, provavelmente, o único país onde 99% dos serviços públicos são disponíveis *online* 24 horas por dia e os 7 dias da semana (24/7), verificando-se que a exceção se fica a dever à impossibilidade de se realizarem casamentos, divórcios e transações de segurança nacional por via digital.[26]

Além da prestação dos serviços públicos, a Estônia armazena os dados na chamada *Government Cloud*. Por sua vez, desenvolveu um portal[27] que, através da assinatura eletrônica de cada cidadão, permite a realização das eleições de forma completa através do *i-voting*;[28] não obstante, desenvolveu um site de *e-services*, no qual é possível - através de assinatura criptografada - solucionar burocracias quotidianas perante os serviços públicos. Até mesmo as estruturas físicas dos gabinetes e ministérios foram transformadas pelos *e-Cabinet*, baseado em um *software* de rede que, somado a um equipamento audiovisual, permite que inclusivamente as decisões ministeriais possam ser tomadas de forma remota, gerando economia e eficiência.[29]

---

[25] "eGovernment. Powering Accountable Governance", Guardtime, acesso Janeiro 9, 2019 https://guardtime.com/solutions/egovernment.

[26] "E-governance", acesso Janeiro 5, 2019, https://e-estonia.com/solutions/e-governance/.

[27] "Valimised", acesso Janeiro 7, 2019 https://www.valimised.ee/en.

[28] Ahmed Ben Ayed, "A conceptual secure blockchain-based electronic voting system", *International Journal of Network Security & Its Applications* 9, no. 3 (2017): 01-09.

[29] Efraim Turban, et al., "Innovative EC Systems: From E-Government to E-Learning, E-Health, Sharing Economy, and P2P Commerce", *Electronic Commerce 2018*. Springer, Cham, (2018): 167-201.

E, na perspectiva de uma Administração Pública em linha, existe um método que se tornou fundamental para a sua viabilização: o da interoperabilidade. De fato, Abreu traz bem essa relação de que muitos entendem o *e-Government* como sendo a face visível da interoperabilidade,[30] o que significa que a Administração precisa utilizar de ferramentas de TI para desenvolver soluções interoperáveis. E o Parlamento Europeu a considera fundamental, pois vai permitir um intercâmbio transfronteiriço de informações, com acesso facilitado em todos os âmbitos da Administração.[31] Entretanto, para que essas informações sejam trocadas de maneira segura e armazenadas sem chances de fraude, eis que a *Blockchain* surge novamente como a estrutura perfeita e a Estônia como paradigma de sucesso.

Na senda das construções relativas à interoperabilidade administrativa e ao estabelecimento do paradigma da Administração Pública em linha, o governo estoniano entendeu que a Administração Pública, para ser digitalmente adequada, precisa trabalhar em conjunto, a fim de que os dados dos cidadãos sejam requisitados "uma única vez". Para isso, viabilizaram o *X-Road*®[32] que permite que setores públicos e privados funcionem com bases de dados interligadas de forma harmônica, sem perder a segurança nas trocas que ocorrem através de dados assinados e criptografados.

Todavia, não é apenas a Estônia que se preocupou em desenvolver um *e-Government* ou usar a *Blockchain* como base nessa perspectiva. Na Europa, merecem destaque três iniciativas[33] que utilizam a tecnologia *Blockchain* na estrutura da Administração Pública, a saber: em Malta, os certificados acadêmicos são criados e verificados em um portal aberto de arquitetura *Blockchain*; na Suíça, já existe o portal público *uPort* para emissão de identidades e, na Finlândia, utilizou-se a tecnologia *Blockchain* para assegurar o serviço de imigração, em um sistema chamado *MONI's*, que permite inclusivamente pagamentos em tempo real ao serviço público competente e correspondente registro na *Blockchain*.[34]

Fora do âmbito europeu, salienta-se um ousado projeto de *e-Government* projetado sobre a tecnologia *Blockchain* na China. O chamado "Guangdong Province Big Data Comprehensive Experimental Area" visa desenvolver uma única plataforma em que os cidadãos podem aceder a múltiplos serviços públicos,[35] sendo as ideias de interoperabilidade administrativa e de Administração Pública em linha que vêm sendo buscadas.

Conforme Hung, a escolha pela *Blockchain*, segundo o governo chinês, passou por dois conceitos fundamentais: 1) a estrutura capaz de preservar todos os registros

[30] Joana Rita Sousa Covelo Abreu, "Digital Single Market under EU political and constitutional calling: European electronic agenda's impact on interoperability solutions", *UNIO–EU Law Journal* 3, no. 1 (2017): 123-140.

[31] Decisão (UE) 2015/2240 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, acesso Janeiro 5, 2019, https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32015D-2240&from=EN.

[32] "Data Exchange Layer X-tee", acesso Janeiro 8, 2019, https://www.ria.ee/en/state-information-system/x-tee.html.

[33] Charalampos Alexopoulos, Aggeliki Androutsopoulou, Zoi Lachana, Michalis Avgerinos Loutsaris e Yannis Charalabidis, "BlockChain Technologies in Government 3.0: A Review", *EGOV-CeDEM-ePart* 2018, ed. Shefali Virkar, et. al. (Krems: Edition Donau-Universität Krems, 2018), 11.

[34] Michael Kuperberg, Sebastian Kemper e Cemil Durak, "Blockchain Usage for Government-Issued Electronic IDs: A Survey", in *Advanced Information Systems Engineering Workshop*, ed. H. Proper and J. Stirna (Berlin: Springer, 2019), 155-167.

[35] Heng Hou, "The application of Blockchain Technology in E-government in China", *Computer Communication and Networks (ICCCN), 2017 26th International Conference* (Vancouver: IEEE, 2017): 1-4.

e a possibilidade de garantir a autenticidade durante a transmissão em tempo real; 2) e a maleabilidade para ser aplicado, nomeadamente em temas delicados de subsistência humana. A *Blockchain* está a ser utilizada no programa *Smart Farmers Market*, no qual os produtores rurais registram, na cadeia, dados como fabricação, validade e rastreamento,[36] a fim de garantir a segurança alimentar de produtos perecíveis.

5. *Blockchain* no contexto da União Europeia

Entusiastas da *Blockchain* viram um enorme panorama abrir-se com a publicação do Plano de Acção Europeu (2016-2020) para a Administração Pública em linha, que dentre outros princípios, elencou expressamente: abertura, transparência, credibilidade e segurança.[37] Não suficiente, todo o Plano gira em torno de uma modernização da Administração Pública no âmbito europeu em que a *Blockchain* aparenta ser o vetor tecnológico crucial buscado pela Comissão. Ao que parece, a Comissão sinaliza compatibilidade com as benesses que a *Blockchain* é capaz de trazer; afinal, mesmo tendo surgido no contexto financeiro, já se percebe seu potencial no contexto da Administração Pública.

Ainda, na Decisão 2015/2240, o Parlamento Europeu definiu expressamente princípios como preservação da informação, modernização administrativa, segurança com respeito da privacidade e da proteção de dados, abertura e transparência, dentre outras a serem observadas no processo de implementação da interoperabilidade na Administração Pública.

E diante do horizonte das possibilidades, foi publicada a Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre moedas virtuais (2016/2007(INI)).[38] Dentre os documentos que, nomeadamente, motivaram esta instituição europeia, vislumbra-se o relatório do conselheiro científico principal do Serviço Científico do Governo do Reino Unido, de 2016, que expressamente fala da aplicação das tecnologias de "distributed ledger" (livro razão distribuído ou "DLT"), sobre a qual a *Blockchain* baseia-se que, se aplicadas propriamente (levando em conta questões de privacidade, segurança, identidade e confiança), constituem oportunidades genuínas para a Administração Pública.[39]

O Parlamento Europeu, na Resolução acima mencionada, buscou pronunciar-se sobre o mercado de moedas virtuais, sobretudo pelas questões de evasão fiscal e até como forma de clamar pela soberania e resistência a um possível uso de *Bitcoin* para financiar o terrorismo. A própria doutrina[40] já vem interpretando a Resolução 2016/2007 nos diversos pontos que diz respeito à Administração Pública, de acordo

[36] Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology", *13th International Conference on Service Systems and Service Management (ICSSSM)* (Kunming: IEEE, 2016), 1-6.

[37] "Comissão Europeia. Plano de ação europeu (2016-2020) para a administração pública em linha Acelerar a transformação digital da administração pública", acesso Janeiro 9, 2019 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016DC0179&rid=1.

[38] Resolução do Parlamento Europeu, de 26 de maio de 2016, sobre moedas virtuais (2016/2007(INI), acesso Janeiro 10, 2019, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228+0+DOC+XML+V0//PT.

[39] "Applications in Government of Distributed ledger technology", acesso Janeiro 10, 2019 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[40] Marcella Atzori, *Blockchain Governance and The Role of Trust Service Providers: The TrustedChain*® Network (London: British Blockchain Association JBBA, 2017).

com as suas disposições: usar as DLT na proteção da privacidade (Art. 1º - d, e); aumentar a transparência e a confiança entre os agentes, independente de quem sejam (Art. 8º); ajudar na redução de fraudes como branqueamento de capitais e corrupção (Art. 11º); e facilitar o registro público (Art. 12º).

Entretanto, crucial foi a visão de futuro do Parlamento que já buscou mencionar, na Resolução 2016/2007, que "[a] utilização da tecnologia de livro-razão [foi] distribuído para além do domínio dos pagamentos". No seu Considerando nº 5, esta Resolução expressamente fala das potencialidades da tecnologia de livro-razão distribuído em três vertentes perante o desígnio da Administração Pública em linha: "prestador de serviços, como supervisor e como legislador".

Dentre os imensos questionamentos sobre como compatibilizar uma *Blockchain* estatal com questões de soberania, controle de interesse público de rede descentralizada, consentimento expresso e direito de ser esquecido previstos no Regulamento Geral de Proteção de Dados (RGPD)[41] devem ser respondido à luz da estrutura técnica maleável sobre a qual a *Blockchain* pode ser desenvolvida, através de permissões de acesso controladas (nas chamadas *Permissioned ledgers*),[42] dos diferentes sistemas de verificação (diferentes do protocolo da *Bitcoin* chamado de *Proof of Work*)[43] e de uma forma que os dados registrados não sejam propriamente visíveis,[44] entretanto continuem sendo íntegros.

6. Considerações finais

Tendo em vista o conceito explorado, pode-se considerar que a *Blockchain* é uma tecnologia de livro-registro distribuído que encontra na descentralização, criptografia e estrutura linear/temporal sua segurança e confiabilidade. É uma arquitetura que possui imenso potencial de uso e adaptação na implementação de uma Administração Pública em linha, ao garantir imutabilidade formal (a *timestamp* que existe em cada bloco, garante a ordem linear e cronológica entre eles) e material (uma vez que o conteúdo também permanece inalterável pelo *hash oneway*, quase que impossível de ser revertido por força-bruta).

A *Blockchain*, além de tecnologia inovadora, propõe uma verdadeira revolução ideológica, pois promete alterar o modelo burocrático-contábil da Administração Pública, e sobretudo ser uma tecnologia segura para que os cidadãos possam não apenas confiar em livros de registro centralizados. Vislumbra-se um paulatino processo de transformação, com a consequente predominância dos sistemas de livro-registro distribuído ("*distributed ledger technologies*" ou DLT), em detrimento aos sistemas de partidas dobradas (DEB ou *double-entry bookekeeping*). E o melhor dos caminhos é sempre que a tecnologia desperte a confiança dos cidadãos, só assim poderemos pensar em um modelo de efetiva Administração Pública em linha.

Os resultados da análise realizada, face aos países que já utilizam a *Blockchain*, confirmam que é possível utilizar essa tecnologia nos mais diversos setores. A Estônia,

[41] Paul Voigt e Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, (Vol. 18. Berlin: Springer International Publishing AG, 2017).

[42] Tim Swanson, "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems", (Report, Apr. 2015). https://pt.scribd.com/doc/261055188/Consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributed-ledger-systems.

[43] Iddo Bentov, Charles Lee, Alex Mizrahi e Meni Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake", *IACR Cryptology ePrint Archive 2014* (2014): 452.

[44] Atzori, *Blockchain Governance*.

pelo avançado uso tecnológico, é um paradigma de consolidação de *e-Government*, não sendo coincidência que também foi o primeiro país a utilizar a *Blockchain* a nível nacional. O segredo está, não apenas na facilidade que a DLT gera em aspectos associados ao funcionamento dos serviços públicos, mas também na segurança e confiabilidade fornecida pela *Blockchain*, o que é fundamental para que os cidadãos confiem em institutos que representam a soberania para estruturas completamente digitais, a exemplo do *i-voting*.

Por fim, foi necessário trazer o assunto para a perspectiva da União Europeia. Abertura, transparência, credibilidade e segurança são princípios desejados pelo Plano de Acção Europeu (2016-2020), e, ao mesmo tempo, são características que definem a tecnologia *Blockchain*, o que já demonstra a compatibilidade do pensamento da Uniao Europeia com o futuro das relações. É interessante notar que um dos objetivos da União Europeia passa, precisamente, pela modernização da Administração Pública e muitos estudos e projetos se desenvolvem para viabilizar, de forma equânime ao redor do continente.

E conforme foi demonstrado, a *Blockchain* revela o potencial de viabilizar algo fundamental para a União Europeia que é o intercâmbio transfronteiriço de informações, com acesso facilitado em todos âmbitos da Administração, na implementação de uma verdadeira interoperabilidade. Pensar nesta eficiente e segura forma de registrar demonstra ser um indicativo para seguirmos as diretrizes da União Europeia e seguir em um promissor caminho para implementar um Mercado Único Digital e propiciar a emergência de um verdadeiro *e-Government*.

A tecnologia *Blockchain* como plataforma de interoperabilidade na União Europeia? Um estudo a partir da Decisão (UE) 2015/2240

Victor Moreira Mulin Leal*

RESUMO: A interoperabilidade tornou-se fundamental para uma estratégia de concretização da Agenda Digital europeia, isso porque, através de mecanismos de governação interoperáveis, a União Europeia se torna capaz de aprimorar aspectos da Administração Pública, promovendo serviços públicos melhores, mais transparentes e eficientes, consequentemente tornando-se mais competitiva em uma nova realidade econômica mundial. No entanto, para alcançar esse método interoperável, é necessária uma mudança de paradigma através da adoção de novas tecnologias voltadas ao setor público, notadamente adaptáveis aos novos padrões de uma sociedade digital. Para tanto, a Blockchain é apresentada criticamente como uma dessas novas tecnologias que possibilitam uma plataforma interoperável, podendo ser utilizada como um banco de dados descentralizado (entre Estados-Membros), que irá registrar dados e informações de forma cronológica, segura e imutável, com níveis de acesso, visualização, envio e registro diferenciados, o que promoverá maior sentimento de cooperação, autenticidade, segurança e confiança, tanto na relação entre Estados-Membros, quanto na relação entre governos e administrados.

PALAVRAS-CHAVE: Agenda Digital – Interoperabilidade – Novas Tecnologias – Blockchain

ABSTRACT: Interoperability has become essential in a strategy for achieving the European Digital Agenda. Through interoperable governance mechanisms, the European Union becomes able to improve aspects of public administration, promoting better, more transparente and efficient public services and, consequently enhancing its competitivity in a new global economic reality. However, in order to achieve this method of interoperable governance, a paradigm shift is needed through the adoption of new technologies thought to the public sector, notably adaptable to the new standards of a digital society. To this end, the Blockchain is critically presented as one of these new technologies that enables an interoperable platform, which can be used as a decentralized database (among Member States), that will record data and information in a chronological, safe and immutable way, with differentiated access and insertion levels, both in the Members States' relations and in the Governments and Citizens' relationships.

KEYWORDS: Digital Agenda – Interoperability – New Tecnologies – Blockchain

* Mestrando em Direito e Informática na Escola de Direito da Universidade do Minho.

1. Notas introdutórias

A 4ª Revolução Industrial apresenta novas perspectivas para a utilização das tecnologias de informação e comunicação (TIC) nos ambientes sociais e econômicos. Em decorrência deste cenário, a sociedade cria novas formas de interação, que passam a ser percepcionadas nos relacionamentos privados e públicos, observados, sobretudo numa forma moderna de se realizar negócios. Deste modo, a transformação digital permite a construção de uma sociedade sem fronteiras.

Neste contexto, embora as tecnologias digitais sejam apresentadas como fatores que transformam o mundo, em verdade, muitos são os obstáculos que ainda impedem que tanto os cidadãos quanto as empresas usufruam de uma melhor versão dos bens e serviços públicos acessíveis através das plataformas digitais. Porém, com esta nova perspectiva de sociedade, vai se tornando imperativo que os Estados aperfeiçoem seus mecanismos de governação, de modo a se tornarem menos burocráticos, mais confiáveis e eficientes, promovendo serviços que aprimorem uma participação mais democrática, com uma troca de dados e informações constantes, bem como uma cooperação entre agentes e organismos da Administração Pública, aproximando os governos dos cidadãos e das empresas.

E entre as características necessárias para a promoção de uma governação eletrônica, destacamos uma qualidade imperativa que todo setor público deve possuir, principalmente no que tange à guarda, proteção, utilização e reutilização de dados e informações, qual seja, a *interoperabilidade* desenhada na Decisão (UE) 2015/2240.

Neste contexto, visando alcançar esse método de governação é necessário que se promova uma mudança de paradigma através da adoção de novas tecnologias voltadas ao setor público, adaptáveis aos novos padrões de uma sociedade digital. Para tanto, a *Blockchain* tem vindo a ser apresentada como uma dessas novas tecnologias que poderão possibilitar uma plataforma interoperável, por permitir o registro de dados e informações de forma cronológica, segura e imutável, promovendo uma maior cooperação, autenticidade, segurança e confiança, tanto na relação entre Estados-Membros, quanto na relação entre os governos e os administrados.

2. A Decisão (UE) 2015/2240 e a interoperabilidade como caminho a seguir[1]

No âmbito da sociedade da informação, a interoperabilidade é definida como a "capacidade de múltiplos sistemas trocarem e reutilizarem informação sem custos de adaptação, preservando o seu significado".[2] No entanto, esta interoperabilidade pode ser classificada como técnica, semântica e organizativa, sendo que, enquanto a interoperabilidade técnica é estabelecida como a capacidade de sistemas e dispositivos trocarem dados com confiabilidade e sem o acréscimo de custos; a sua classificação semântica traduz-se na capacidade de manter o significado da informação que está sendo disponibilizada; ao passo que, por último, a interoperabilidade organizativa é, afinal, a capacidade de cooperação entre organizações, através da uma padronização de processos.[3]

[1] Utiliza-se esta expressão por referência ao título do projeto que esteve na base do presente artigo.
[2] Agência para Modernização Administrativa, "Interoperabilidade na Administração Pública", acesso em Fevereiro 12, 2019, https://www.iap.gov.pt/guia_adesao_iap_v3_0_2.pdf.
[3] Joana Covelo de Abreu e Francisco C. P. Andrade, "Da interoperabilidade à mediação eletrónica: um novo desafio para a Administração Pública", in *A mediação administrativa: contributos sobre as (im) possibilidades*, coord. Isabel Fonseca (Coimbra: Almedina, 2019), 325-343.

Contudo, o conceito de interoperabilidade, assim como a sua aplicação no setor público, não são uma novidade desta década, pois que, desde os princípios dos anos 2000, organizações e líderes governamentais advogam no sentido de que a sua implementação facilitaria a cooperação e tornaria os serviços públicos melhores. Estas declarações podem ser observadas através da leitura do Considerando 1º da Decisão (UE) 2015/2240,[4] que narra que, numa série de declarações ministeriais, quais sejam, i) a de Manchester de 24 de novembro de 2005; ii) a de Lisboa de 19 de setembro de 2007; iii) a de Malmö, 18 de novembro de 2009; e por fim, iv) a de Granada de 19 de abril de 2010, "os ministros convidaram a Comissão a facilitar a cooperação entre os Estados-Membros através da aplicação de soluções de interoperabilidade transfronteiriças e intersectoriais que permitam tornar os serviços públicos mais eficientes e mais seguros". No 2º Considerando, encontramos a informação de que a Comissão reconheceu, em 2010, que "a interoperabilidade é essencial para maximizar o potencial social e económico das tecnologias da informação e da comunicação (TIC) e que, por conseguinte, a agenda digital só poderá ser efetiva se a interoperabilidade estiver assegurada".

Como se percebe, a União Europeia reconheceu a interoperabilidade como elemento fundamental numa estratégia para a concretização da Agenda Digital europeia. E foi neste contexto que surgiu a Decisão 2015/2240, com o objetivo de promover um programa de soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus como um meio de modernizar o setor público.

Neste sentido, o artigo 2.º, n.º 1 da Decisão supracitada, apresentou a sua definição de interoperabilidade, na qual entende ser esta "a capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo, implicando a partilha de informações e conhecimentos entre si, no âmbito dos processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC".

Assim, a partir da compreensão de sua definição, pode-se perceber que a interoperabilidade pode apresentar inúmeras vantagens, ao se tornar um meio adequado para a execução de políticas públicas, como consta nos Considerandos de n.ºs 6, 13 e 14 que retratam, respectivamente, matérias no campo do direito das sociedades[5], de livre acesso a documentos administrativos[6] e no domínio da identificação eletrônica[7]. Para

[4] Parlamento Europeu e Conselho, "Decisão (UE) 2015/2240 que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA2) como um meio para modernizar o setor público", acesso em Janeiro 13, 2019, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32015D2240.

[5] "No domínio do Direito das Sociedades, a Diretiva 2012/17/UE do Parlamento Europeu e do Conselho impõe a interoperabilidade dos registos centrais, comerciais e das sociedades dos Estados-Membros através de uma plataforma central. A interconexão dos registos das sociedades permitirá o intercâmbio transfronteiriço de informações entre registos e facilitará o acesso, a nível da União, das empresas e dos cidadãos aos dados sobre sociedades, melhorando, desse modo, a segurança jurídica do ambiente empresarial na União" cf. Decisão (UE) 2015/2240, Considerando n.º 6.

[6] "No domínio das informações do setor público, a Diretiva 2013/37/UE do Parlamento Europeu e do Conselho sublinha que os organismos do setor público deverão, sempre que possível e adequado, disponibilizar os documentos em formatos abertos e compatíveis com a leitura por máquina, juntamente com os respetivos metadados, ao melhor nível de precisão e granularidade, num formato que garanta a interoperabilidade, a reutilização e a acessibilidade", cf. Decisão (UE) 2015/2240, Considerando n.º 13.

[7] "No domínio da identificação eletrónica, o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho estabelece um quadro de interoperabilidade para fins da interoperabilidade de sistemas nacionais de identificação eletrónica", cf. Decisão (UE) 2015/2240, Considerando n.º 14.

tanto, não apresenta a Decisão europeia o *modus operandi* adequado para a implementação desta troca de informação, ou seja, para se alcançar a interoperabilidade, permitindo que a doutrina aponte a tecnologia a adotar, podendo a chamada *Blockchain* divisar-se como uma via apropriada para se prosseguir tal finalidade.

3. A tecnologia *Blockchain* como plataforma de interoperabilidade: características, expectativas e limitações

Para compreender a tecnologia *Blockchain* como o meio adequado à implementação da interoperabilidade entre os Estados-Membros e com as instituições europeias torna-se necessário entender esta tecnologia no contexto de suas peculiaridades históricas. Embora o ano de 2008 seja considerado como o de seu registro de nascimento, em função do desenvolvimento e divulgação da criptomoeda *Bitcoin*, muito se discute se já existe um claro entendimento sobre o que é a *Blockchain*.

Primeiramente, deve-se esclarecer que a *Blockchain* não está restrita às criptomoedas, tampouco ao mercado de transações financeiras digitais; por exemplo, pode ser adotada como um banco de dados descentralizado, que registra dados e informações de forma cronológica e imutável, conferindo segurança através de criptografia, o que promove o sentimento de confiança sobre os documentos lá registrados, comportamento importante para o setor público. Por isso, tem sido considerado, pela literatura especializada, como um marco tão importante quanto o surgimento da internet[8].

Neste contexto, a *Blockchain* pode ser entendida como uma espécie de um livro-razão virtual e distribuído (*distributed ledger technology*) que funciona como um registro aberto e confiável de transações realizadas de um nódulo (*node*) para outro (ou para múltiplos nódulos), sendo que o registro deste livro-razão não é armazenado e gerido por uma autoridade central,[9] destacando-se que todos os registros realizados nesta plataforma são criptografados, utilizando a função criptográfica *hash*, que permite que cada documento ou informação inserida possua uma "impressão digital" incorruptível.

Assim, partindo da interpretação dos elementos da definição supracitada, o termo *distribuída* significa que "todas as cópias de um documento são constante e automaticamente sincronizadas de forma idêntica a todo o momento [em que] 'não há uma cópia canônica, [pois que] todas as cópias são igualmente criadas"'.[10] Dessa forma, o facto de os nódulos armazenarem, de forma idêntica e atualizada, o registro do livro-razão, permite que auditorias sejam realizadas sempre que necessário, promovendo uma maior transparência entre os nódulos de uma rede *blockchain*.

Especificamente sobre os *nódulos*, estes são entendidos como sendo os usuários ou computadores conectados à plataforma *Blockchain*, podendo, por sua vez, ser distinguidos entre integrais ou parciais.[11] Os nódulos integrais (*full nodes*) são aqueles que detêm um grande poder computacional, e possuem, cada um deles, uma cópia

[8] Ameer Rosic, "What is Blockchain technology the new internet? A step-by-step guide for beginners", 2016, acesso em Janeiro 12, 2019, https://blockgeeks.com/guides/what-is-blockchain-technology/.

[9] J. Berryhill, T. Bourgery e A. Hanson, "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", *OECD Working Papers on Public Governance*, n.º 28, (Paris: OECD Publishing, 2018), https://doi.org/10.1787/3c32c429-en.

[10] Tess Rinearson, "Making Money: Bitcoin Explained (with Emoji), Part 1", *Medium Online*, 2017, acesso em Janeiro 12, 2019, https://medium.com/@tessr/makingmoney-530d2bb2b8f7.

[11] Luiz Fernando Israel Assunção e Pedro Vilela Resende Gonçalves, "Ethereum e Blockchain: Desafios Jurídicos das Plataformas Descentralizadas", acesso em Fevereiro 13, 2019, https://www.academia.edu/29701285/Ethereum_e_Blockchain_Desafios_Jur%C3%ADdicos_das_plataformas_descentralizadas.

integral de todo o registro da *Blockchain*, sendo, de certa forma, os responsáveis por alcançar o consenso dos dados e informações enviados, bem como pela publicação dos novos blocos de dados. Já os nódulos parciais (*lightweight nodes*) são os utilizadores que não possuem tanto poder computacional. No entanto, embora não armazenem uma cópia integral dos registros, são os que tendem a enviar os dados e as informações que serão processadas e validades.

Quanto a segurança da rede, esta é realizada através da *criptografia*,[12] que corresponde ao ato de criar códigos que permite que determinado dado seja mantido em segredo. Logo, a criptografia converte dados e informações num formato que somente poderá ser descodificado por utilizadores que possuírem autorizações, impedindo o acesso a informações sensíveis por aqueles que não sejam devidamente autorizados.

No entanto, embora esta tecnologia tenha ganho notoriedade pelas transações financeiras realizadas numa *Blockchain* pública (*permissionless ledger*), é possível se programar uma *Blockchain* privada (*permissioned ledger*). Deste modo, entende-se por *Blockchain* pública,[13] cujo exemplo é aquela associada ao *Bitcoin*, a transação que "permite que qualquer pessoa envie dados e informações para o livro-razão, e que todos [que estejam] em posse do registro do livro-razão (*ledger*) possuam uma cópia idêntica". Diferentemente, a *Blockchain* privada tende a limitar as contribuições de dados a um grupo restrito de utilizadores que possuem autorização. Contudo, esta restrição é aplicada tanto ao envio como ao acesso e à visualização dos dados e informações que estejam disponibilizados na plataforma.

Quanto à validação dos dados a cargo dos nódulos integrais, estes são percepcionados por via de um modelo de consenso, que corresponde ao conjunto de regras e diretrizes que determinam a forma, o momento e os requisitos de validação de dados e informações no livro-razão.[14] Assim, dentro de uma *Blockchain* pública, o modelo de consenso utilizado é o chamado de *prova de trabalho* (*Proof of Work*) ou o de *prova de participação* (*Proof of Stake*),[15] sendo que esses protocolos são utilizados nos casos em que não exista uma confiança prévia entre os utilizadores da rede, sendo este o modelo aplicado, sobretudo, para a realização de transações financeiras.

Já no caso da *Blockchain* privada, o modelo de consenso apropriado é designado de *prova de autoridade* (*Proof of Authority*) ou *Round Robin*. Estes modelos têm em sua base a concessão de autorizações para que apenas utilizadores integrais (*full nodes*) possam validar e publicar blocos, mas também se baseiam na concessão de permissões para que utilizadores parciais (*lightweight nodes*) possam introduzir e visualizar informações. Para Marchionni esta é a forma mais adequada a ser aplicada no setor público, por permitir uma adaptação à complexa forma de gestão dos governos, assim como às características intrínsecas do processo decisório.[16]

Por fim, destaca-se a característica da *imutabilidade* da *Blockchain*, que corresponde à impossibilidade de o dado ser desfeito após o seu envio, processamento, validação e registro. Este elemento é um dos principais aspectos que contribuem para a confiabilidade

[12] Berryhill, Bourgery e Hanson, "Blockchains Unchained".
[13] Mark Walport, *Distributed Ledger Technology: Beyond Block chain. A Report by the UK Government Chief Scientific Advisor* (London: Government Office for Science, 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
[14] Berryhill, Bourgery e Hanson, "Blockchains Unchained".
[15] Pavel Vasin, "BlackCoin's Proof-of-Stake Protocol v2", acesso em Abril 28, 2019, https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf.
[16] Pietro Marchionni, "The Next Generation e-government", 2018, acesso em Janeiro 13, 2019, https://www.linkedin.com/pulse/next-generation-e-government-pietro-marchionni.

das transações nesta tecnologia. Assim, distingue-se de um banco de dados tradicional, pelo facto de que neste, "quando os usuários adicionam ou modificam dados, eles se conectam com um servidor que realiza essas alterações, e os dados continuam no servidor", enquanto, através dos métodos tradicionais, "toda a informação passa a ser mantida em um só lugar, ou seja, sob a responsabilidade de uma única autoridade centralizadora", e, portanto, "se a segurança do servidor estive[sse] comprometida, os dados pode[ria]m ser alterados ou deletados", situação que podia ocorrer "sem que ninguém sequer tenha notado".[17]

E é em razão dos elementos descritos que a *Blockchain* tem sido entendida como uma plataforma que não permite que os dados registrados sejam alterados ou apagados, visto se tratar de uma rede distribuída, ou seja, que se fundamenta na existência de diferentes nódulos integrais, que possuem cópias completas e atualizadas dos registros do livro-razão, impossibilitando que ataques cibernéticos que visam bloquear o funcionamento de um servidor tenham efeito.

No entanto, embora a doutrina se incline para a utilização da tecnologia *Blockchain* privada na implementação de uma Administração Pública em linha, a verdade é que podemos estar diante de uma opção não tão adequada, visto ser uma característica intrínseca da Administração Pública a atualização e possibilidade de apagamento ou de retificação de dados, correspondendo tais dimensões aos direitos decorrentes do Regulamento Geral sobre a Proteção de Dados que também vincula entidades públicas ao elevado padrão de proteção de dados no contexto da União. Daqui se intui que poderemos estar diante de um conflito entre este direito fundamental e a sua observância e a própria estrutura e funcionamento empírico da *Blockchain*, enquanto tecnologia que radica na característica da imutabilidade – que é também aquela que lhe imprime particular fiabilidade. Assim, em função deste quesito, até que sejam harmonizadas as ferramentas da *Blockchain* com o disposto no RGPD, somos de opinião de que a aplicação desta tecnologia nos serviços públicos deve ser pensada com particular cautela porque as soluções adotadas publicamente têm de se revelar particularmente escaláveis no tempo.

4. Considerações finais

Observando o atual paradigma social e tecnológico verificamos que a Administração Pública necessita de uma reformulação quanto ao modelo de governança adotada, tendo por finalidade a busca por melhores serviços públicos, com menor pendor burocrático e que seja mais eficiente e envolvendo menos recursos, visando colmatar a falta de confiança que assola o cidadão e as empresas nas relações que mantém com os serviços públicos. Para tanto, busca-se implementar um sistema que promova maior transparência e cooperação a fim de resgatar a confiança do cidadão.

Neste sentido, a União Europeia através da Decisão (UE) 2015/2240 apresenta a interoperabilidade como a resolução para este impasse, ao permitir a intercomunicação de dados e informações a nível transnacional e transfronteiriço. Para tal, tem sido defendido pela doutrina o uso da plataforma *Blockchain* como a via adequada para que seja alcançado tal desiderato no contexto da Administração Pública da União.

Com vista a cumprir tal objetivo a União Europeia tem realizado diversas pesquisas nesta área como, por exemplo, o estabelecimento de um Observatório e de

[17] Shaan Ray, "Blockchains versus Traditional Databases", 2017, acesso em Janeiro 13, 2019, https://hackernoon.com/blockchains-versus-traditional-databasesc1a728159f79.

um Fórum para tecnologia *Blockchain*,[18] criados no ano de 2018, assentes em medidas que se destinam a compreender aspectos legais da Administração Pública em linha e do método da interoperabilidade no âmbito do Mercado Único Digital.[19]

De acordo com a doutrina, para o setor público tem sido defendida a utilização da *Blockchain* privada, por meio da adoção dos modelos de prova de autorização e/ou *Round Robin*, uma vez que através destes se pode determinar, exatamente, quais utilizadores podem aceder e visualizar as informações, além de que os próprios Estados-Membros podem atuar como nódulos integrais, tornando-se responsáveis pelo processamento, validação e registro de informações dentro da plataforma. Enquanto isso, do outro lado, cidadãos, empresas e demais autoridades podem se posicionar como nódulos parciais e, a todo momento, enviar e consultar esses mesmos dados e informações.

Em uma rede descentralizada cada Estado-Membro armazena uma cópia integral e sincronizada do registro do livro-razão, e por isso, auditorias podem ser realizadas sempre que necessário, imprimindo transparência à atividade administrativa. Além de que esta rede se encontra protegida contra ataques cibernéticos, uma vez que os bancos de dados não ficam sob o controle de uma autoridade central, o que implica que, para aceder a esses dados, seria necessário um ataque sincronizado a todos dos Estados-Membros. Assim, essas condições são capazes de garantir uma maior transparência e cooperação, elementos essenciais para que a confiança recíproca entre as administrações públicas dos Estados-Membros e destas face às instituições se possa ver reforçada sob a égide da criptografia e da capacidade de imutabilidade dos dados que impede uma manipulação maliciosa ou que os mesmos sejam apagados.

Face ao exposto, é por essas características que a tecnologia *Blockchain* tem sido defendida como sendo adequada para implementar a interoperabilidade na Administração Pública, pois que é apontada como sendo capaz de reduzir a burocracia, o conflito entre agências, ao mesmo tempo que permite o compartilhamento eficiente de conhecimento,[20] alcançando assim o objetivo inscrito na Decisão (UE) 2015/2240, que prima por uma integração interoperável transfronteiriça e intersetorial, viabilizando a execução de políticas europeias materializadas em diretivas como a Diretiva 2012/17/UE (relativa aos serviços do mercado interno), Diretiva 2013/37/UE (relativa à reutilização de informações do setor público) e no Regulamento (UE) nº 910/2014 (relativo à identificação eletrônica).

No entanto, é preciso ter em atenção que, embora esta tecnologia demonstre ser o caminho adequado para a promoção da interoperabilidade, a arquitetura atual da *Blockchain* pode conflituar com o elevado padrão de proteção de direitos fundamentais no contexto europeu, nomeadamente por referência ao direito à proteção de dados e aos direitos concretizadores, reconhecidos ao titular dos dados e que são, por este, oponíveis também aos serviços públicos. Logo, embora a aplicação desta tecnologia à Administração Pública possa garantir uma maior transparência e celeridade, criando uma nova versão – digital – dos serviços públicos, esta ainda não é a solução para todos os problemas públicos, pois o avanço tecnológico acarreta também a necessidade de acautelar diferentes dimensões jusfundamentais a que tal tecnologia ainda não é capaz

[18] "EU Blockchain Observatpry and Forum", acesso em Janeiro 03, 2019, https://www.eublockchain-forum.eu/.
[19] Para mais desenvolvimentos quanto à perspetiva da interoperabilidade como um método, Alessandra Silveira e Joana Covelo de Abreu, "Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Government paradigma", *EJLT – European Journal of Law and Technology*, vol. 9, n.º 1, (2018): 7.
[20] Berryhill, Bourgery e Hanson, "Blockchains Unchained".

de dar corte.

Neste sentido, embora muitas sejam as vantagens da tecnologia *Blockchain*, sobretudo no cumprimento do desígnio de uma Administração Pública em linha e, especialmente, através da interoperabilidade, diversas são também as barreiras ou, utilizando a expressão da moda, diversos são os "muros (!)" cujo cimento tende a dificultar a sua efetivação.

A Comissão Nacional de Proteção de Dados (CNPD) como instrumento da governança democrática em Portugal

Marcelo Porrua*

RESUMO: A construção de governanças legítimas, que respeitem os direitos fundamentais, passa pela defesa do direito à privacidade, uma vez que ela está presente no rol das liberdades individuais, sem as quais a democracia não se sustenta. As demandas do mundo digital exigem uma reflexão aprofundada sobre as diferentes dimensões da privacidade e os mecanismos para sua proteção, principalmente no que toca aos limites ao acesso à*s informações pessoais. Nesse viés, o Regulamento Geral sobre a Proteção de Dados (RGPD) mostra-se um instrumento de cidadania já que, sem as ações empreendidas pela Comissão Nacional de Proteção de Dados (CNPD), teria sua eficácia reduzida na imprescindível defesa do sistema democrático, tanto no que toca à utilização de dados, como* à *sua limitação.*

PALAVRAS-CHAVE: Democracia – Direitos fundamentais – Liberdade individual – Regulamento Geral sobre a Proteção de Dados – Comissão Nacional de Proteção de Dados

ABSTRACT: The construction of legitimate governances, which respect fundamental rights, involves the defense of the right to privacy, since it is present in the roll of individual liberties, without which democracy does not sustain itself. The demands of the digital world require in-depth reflection on the different dimensions of privacy and the mechanisms for its protection, especially with regard to limits on access to personal information. In this setting, the General Regulation for Data Protection (RGPD) shows itself as an instrument of citizenship that, without the actions made by the National Commission for Data Protection (CNPD), would have its effectiveness reduced in the indispensable defence of the democratic system, both in terms of the use of data and in terms of their limitation.

KEYWORDS: Democracy – Fundamental rights – Individual freedom – General Regulation of Data Protection – National Commission for Data Protection

* Mestrando em Direitos Humanos (2018/2019) – Escola de Direito – Universidade do Minho.

Para a construção de governanças legítimas é imperiosa a prática efetiva do respeito pelos direitos fundamentais e liberdades individuais, sem a qual a democracia não se sustenta. No rol das proteções podem ser elencados diferentes direitos, dentre os quais podemos evidenciar o direito à proteção de dados pessoais como um dos pilares de sustentação dos direitos da personalidade. Todavia, o constante e inevitável desenvolvimento das tecnologias de informação torna possível a recolha de muitas informações de caráter pessoal, podendo torná-las um produto, e por isso comercializáveis, em detrimento das garantias de respeito impostas em diferentes planos normativos a essas mesmas informações.[1]

Em exposição no universo digital, podem estar diferentes informações de cunho pessoal que refletem aspectos pessoais da personalidade; esse panorama exige uma reflexão aprofundada sobre as diferentes dimensões da privacidade e os mecanismos para sua proteção, principalmente no que toca aos limites de acesso às informações pessoais, aspecto que pode ser agravado pela intensa disseminação de valores que refletem posturas autoritárias que não se coadunam com as expetativas democráticas, algumas delas na origem da deflagração de crises políticas importantes, pelas quais a Europa está a passar.

Portanto, percebe-se a necessidade de mecanismos de vigilância contra as investidas que visem a recolha, o registo, a organização, a conservação, a adaptação, a utilização, a transmissão, o bloqueio, o apagamento ou a destruição dos dados pessoais dos cidadãos, atividade essa perpetrada por entidades públicas ou privadas, para que se garanta a harmonia social e a manutenção dos valores democráticos. Nesse contexto, o Regulamento Geral sobre a Proteção de Dados, aplicável desde 25 de maio de 2018, mostra-se um forte instrumento de cidadania quando enfatiza a proteção dos dados pessoais de sujeitos singulares, ao mesmo tempo que garante a circulação segura desses dados, sob o escrutínio de autoridades de proteção.

Entre os inúmeros termos presentes no Regulamento, encontra-se a consagração das autoridades de controlo, em conformidade com os artigos 51.º e seguintes, que estabelecem as competências e legitimam as ações das autoridades de controlo na defesa dos "direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e [para] facilitar a livre circulação desses dados na União". Tais competências, reconhecidas no artigo 55.º do Regulamento, acarretam um reforço do papel das autoridades de controlo nacionais designadas.

No caso português, a Comissão Nacional de Proteção de Dados (CNPD), em atividade desde o ano de 1994, na condição de autoridade de controlo, possui inúmeras atividades em razão da proteção de dados e, apesar da imensa demanda de trabalho, acha-se em processo de adaptação de suas competências funcionais para assegurar a plena vigência do RGPD.

Atualmente a sua tutela jurídica encontra-se prevista na Lei de Proteção de Dados [Lei n.º 67/98, de 26 de outubro (de acordo com a redação da última atualização promovida pela Lei n.º 103/2015, de 24 de agosto)], na qual reconhece, no artigo 21º, a CNPD como sendo a autoridade de controlo nacional, estabelecendo sua natureza e competências. Este ato legislativo foi adotado para transpor a Diretiva n.º 95/46/CE, que assim como o atual RGPD, determinava caber aos Estados-Membros a criação de uma ou mais autoridades públicas competentes para a fiscalização da

[1] A saber: o princípo da autodeterminação informação presente na Constituição Portuguesa de 1976, no Regulamento Geral de Proteção de Dados da União Europeia (2016/679) e Proposta de Lei 120/XIII/3ª sobre a proteção de dados.

aplicação das normas que visem a tutela do tratamento de dados pessoais.

Com competências que se estendem desde as atividades de informação cujos destinatários são os diferentes setores sociais, com o intuito de observarem as condutas que devem ser tomadas para a efetiva proteção dos dados, até a adoção de medidas que visam fiscalizar as ordenações ou verificar as contraordenações, a CNPD possui um papel importante na manutenção dos direitos e defesa das liberdades, fundamentos basilares da democracia.

1. Bases democráticas da normatização da proteção de dados

No entendimento de Bobbio "[...] a democracia é, no essencial, um método de governo, um conjunto de regras de procedimento para a formação das decisões coletivas [...]"[2] e foi com esse espírito democrata que a Convenção 108 de 1981 do Conselho da Europa foi delineada e protagonizou o primeiro instrumento normativo europeu em matéria de protecção de dados que assenta-se no direito fundamental à privacidade. Portanto, a referida Convenção para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais é um instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados, que visa "garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal".[3]

Numa atitude vanguardista, de proteção das liberdade e garantia de direitos, é importante recordar que Portugal, muito antes de outras nações democráticas, reconheceu a protecção de dados como direito fundamental na Constituição de 1976, mais precisamente em seu artigo 35º que diz respeito à *utilização da informática*.[4] No ano de 1974, Portugal retomou os moldes da democracia, e assim começou a configuração de um governo que não economizou esforços para garantir aos cidadãos que direitos e liberdades ficassem protegidas diante das inúmeras violações outrora acontecidas. Nesse movimento de redemocratização, foi incluída na Constiuição Portuguesa, acertadamente, tópico sobre a utilização da informática, cujo potencial

[2] Norberto Bobbio, *O Futuro da Democracia: uma defesa das regras do jogo* (Rio de Janeiro: Paz e Terra, 1986), 7.

[3] Cf. Proteção de Dados Pessoais, acesso em Abril 21, 2019, http://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais, p. 2.

[4] Cf. Constituição da República Portugesa, artigo 35.º Utilização da informática. 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei. Cabe-nos ressaltar que a redação deste artigo sofreu grandes alterações sobretudo a partir da entrada em vigor da Diretiva n.º 95/46/C, cf. Jorge Miranda e Rui Medeiros, *Constituição Portuguesa Anotada*, Tomo I, 2 ed., rev. e actual. (Coimbra: Coimbra Editora, 2010), 779.

de uso e de aplicação já se mostravam bastante promissores.

Nas últimas três décadas, a evolução tecnológica nunca deixou de nos surpreender, tendo atingido patamares verdadeiramente admiráveis, que permitiram a construção de sistemas informacionais cada vez mais complexos, rápidos e eficientes em relação ao processamento dos dados e informações que lhes são fornecidos. Tamanha capacidade operacional tem sido aproveitada por diferentes setores, tanto públicos como privados. Neste campo, as relações entre a tecnologia e a economia, quando se aliam em prol das exigências do mercado globalizado, têm gerado importantes e necessárias reflexões em relação ao acesso aos dados que compõem a vida privada das pessoas, parte mais vulnerável de tais relações, mesmo que autorizado, sob pena de, cada vez mais, os sujeitos abdicarem de sua privacidade e liberdade, em nome de interesses públicos ou privados, ou mesmo para minimizar o medo provocado por incertezas nas relações com tais entidades.

Esta capacidade tecnológica tem permitido também a criação de grandes sistemas de informação, interoperáveis, que processam e cruzam milhões de dados pessoais a um ritmo crescente, com a elaboração de algoritmos cada vez mais complexos. Não se pode negar que as sinergias tecnológicas e económicas têm sido geradoras de preocupantes intrusões na privacidade de todos e de cada um.

Mesmo diante de um fenómeno que não admite retrocessos, como se tem configurado o universo digital, não podemos deixar de compreender que o fracasso na salvaguarda da privacidade coloca em causa outros direitos e liberdades, como a liberdade de expressão, o direito à não discriminação, o direito à livre circulação, o direito ao anonimato e, como limite, a dignidade da pessoa humana.

Para que essas forças possam se equilibrar, numa sociedade democrática, há que se concretizar, a todo o momento, as garantias necessárias para um efectivo exercício das liberdades e dos direitos humanos fundamentais, mesmo contra os desmandos do Estado e, muito mais, do espírito dos mercados, num constante movimento de equilíbrio entre o Estado Liberal e o Estado Democrático.[5] Assim, as ações empreendidas pela CNPD reafirmam o compromisso da defesa da protecção de dados e da privacidade, e esboçam o que pode ser compreendido como um instrumento de garantia da democracia e das liberdades individuais, empreendendo diferentes frentes de trabalho, como veremos a seguir.

2. As atividades da CNPD e o exercício efetivo da salvaguarda de direitos e liberdades

De antemão, não retirando a responsabilidade de cada cidadão na vigilância de seus próprios direitos, bem como no exercício de suas liberdades individuais, com todos os reflexos na esfera das responsabilidades, o controlo estatal, configurado como uma forma superior de controlo da sociedade, se manifesta por duas formas básicas: preventiva e repressiva, como afirma Bobbio

[5] Cf. Bobbio, *O Futuro da Democracia*, 19 "o estado liberal é o pressuposto não só histórico mas jurídico do estado democrático. Estado liberal e estado democrático são interdependentes em dois modos: na direção que vai do liberalismo à democracia, no sentido de que são necessárias certas liberdades para o exercício correto do poder democrático, e na direção oposta que vai da democracia ao liberalismo, no sentido de que é necessário o poder democrático para garantir a existência e a persistência das liberdades fundamentais. Em outras palavras: é pouco provável que um estado não liberal possa assegurar um correto funcionamento da democracia, e de outra parte é pouco provável que um estado não democrático seja capaz de garantir as liberdades fundamentais. A prova histórica desta interdependência está no fato de que estado liberal e estado democrático, quando caem, caem juntos".

> […] uma preventiva, que tem um aspecto principalmente psicológico, pelo temor às conseqüências legais do abuso, e outra material, em casos que o Estado considera de excepcional importância; e a repressiva, *post facto*, pela qual se punem os que abusam das liberdades e dos direitos assegurados na ordem jurídica, mediante, já agora, instrumentos corretivos, de reposição das coisas no *statu quo ante*, e instrumentos punitivos, pelos quais os responsáveis pelos atos abusivos sofrem as penalidades previamente fixadas nas leis.[6]

Para tanto, os Estados contam com diferentes instrumentos que, de forma especializada, e respaldados normativamente, garantem a defesa desses direitos e liberdades. Uma dessas instituições em solo português é a CNPD[7] que, sob o fundamento do RGPD, possui a missão de proteger os dados pessoais de pessoas singulares no âmbito da União Europeia contra as violações praticadas pelo próprio Estado ou contra as investidas do mercado que não mais se configura de modo simples, mas acaba por revelar-se como uma teia complexa de interesses de diferentes grupos (às vezes com apoio do próprio Estado).[8]

Entretanto, a partir da aplicação do RGPD (25 de maio de 2018), os tratamentos de dados pessoais que deviam ser notificados à CNPD, deixaram de ser, uma vez que o Regulamento não mais lhe atribui a competência de controlo prévio, por via da autorização desse tratamento. Portanto, o centro das atividades do CNPD está dividido em dois diferentes polos, o de orientação genérica sobre tratamentos de dados (pareceres, diretrizes e outros esclarecimentos) e o da garantia dos direitos dos cidadãos e a correspondente fiscalização dos tratamentos de dados empreendidos por pessoas ou instituições públicas ou privadas, com claro caráter sancionatório.

> Por essa razão, o número de processos abertos entre 25 de maio e 31 de dezembro de 2018 diminuiu drasticamente: apenas 1223 novos processos, dos quais 610 de averiguações (podendo originar a apreciação de ilícitos contraordenacionais) e 29 relativos a pedidos de parecer no âmbito de procedimentos legislativos, regulamentares ou ainda de autorização de instalação de sistemas de videovigilância no espaço público.[9]

Até 31 de dezembro de 2018, foram abertos 161 processos de violação de dados pessoais (*Data Breach*)[10] que correspondem a uma obrigação de notificação imposta

---

[6] Cf. Felippe Augusto Miranda Rosa, *Sociologia do Direito: O fenômeno jurídico como fato social* (Rio de Janeiro: Jorge Zahar Editor, 2004), 189.

[7] A Comissão Nacional de Protecção de Dados é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República. Tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei. A CNPD é a Autoridade Nacional de Controlo de Dados Pessoais, cooperando com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro. Informação disponível em: https://www.cnpd.pt/bin/cnpd/acnpd.htm.

[8] Cf. Bobbio, *O Futuro da Democracia*, 22 "Os grupos e não os indivíduos são os protagonistas da vida política numa sociedade democrática, na qual não existe mais um soberano, o povo ou a nação, composto por indivíduos que adquiriram o direito de participar direta ou indiretamente do governo, na qual não existe mais o povo como unidade ideal (ou mística), mas apenas o povo dividido de fato em grupos contrapostos e concorrentes, com a sua relativa autonomia diante do governo central (autonomia que os indivíduos singulares perderam ou só tiveram num modelo ideal de governo democrático sempre desmentido pelos fatos)".

[9] Cf. Relatório de atividades da Comissão Nacional de Proteção de Dados 2017-2018, acesso em Abril 22, 2019, https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201718.pdf, p. 22.

[10] Cf. Informações disponíveis em https://www.portaldodpo.pt/glossario/ a violação de dados pessoais, ou *Data Breach,* corresponde à violação de segurança que provoque de modo acidental ou

pelo RGPD aos responsáveis por tratamentos de dados, sempre que se verifique uma violação de segurança com repercussão nos dados pessoais.

Percebeu-se uma grande diminuição no número de decisões, num total de apenas 660 atos jurídicos decisórios, correspondendo a 558 deliberações, 64 projetos de deliberação e um projeto de regulamento. Devem ser contabilizados os pareceres emitidos pela CNPD, no âmbito da sua função consultiva, prevista no RGPD[11] e em lei nacional (esta no contexto da vídeo-vigilância em espaço público).

As atividades orientadoras da CNPD cresceram muito, uma vez que a extinção do controlo administrativo prévio dos tratamentos de dados fez demandar ainda mais a necessidade de orientação e esclarecimento dos cidadãos bem como das empresas e organismos públicos enquanto responsáveis pelo tratamento. Um excelente exemplo foi a aprovação de uma diretriz relativa à disponibilização de dados pessoais dos estudantes, dos docentes e demais trabalhadores no sítio da Internet das instituições do ensino superior.[12]

O perfil "educativo" adotado pela CNPD tem a ver com o que afirma Bobbio sobre a insuficiente educação para a cidadania, reafirmando que ela é importante para que as democracias se mantenham; ao mesmo tempo reafirma que a educação se faz na medida do seu próprio exercício. Em especial relação com esse tópico de reflexão sobre o futuro da democracia, podemos atentar aos relatórios emitidos pela CNPD, através dos quais esta publicou as orientações para a aplicação do novo regime jurídico europeu de proteção de dados, através da disposição de um conjunto de perguntas e respostas frequentes (FAQ's), com vistas a esclarecer as dúvidas mais comuns que chegam até a CNPD. Nesse mesmo sentido, a CNPD tem publicitado, no "Espaço RGPD", informação específica relativa ao regulamento, que permite o acesso direto a documentos orientadores e a consultas públicas lançadas pelo Grupo de Trabalho do artigo 29º[13] e pelo Comité Europeu para a Proteção de Dados.[14]

São claras as ações de cunho educativo que tomam diferentes formas e são colocadas à disposição dos cidadãos pela CNPD. Cada uma dessas iniciativas visa realizar as propostas dos Planos de Atividades preparadas e que norteiam também outros propósitos das ações da CNPD. Essas ações são exercícios democráticos que atingem uma parcela não quantificável da população, que pode auxiliar-se desses dados na proteção de seus direitos e no exercício de suas liberdades, conforme afirma Bobbio de que "[…] a educação para a democracia surgiria no próprio exercício da prática democrática".[15]

---

ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais conservados sujeitos a qualquer outro tipo de tratamento.

[11] Cf. n.º 4 do artigo 36.º, alínea c) do n.º 1 do artigo 57.º e alínea b) do n.º 3 do artigo 58.º do RGPD.

[12] Nesse sentido, em relação ao procedimento da sua elaboração, realizou-se uma consulta pública do projeto de diretriz, de modo a colher as perspetivas dos interessados nesse contexto. Informações disponíveis em https://www.cnpd.pt/bin/decisoes/Diretrizes/Diretriz_1_2018_disponibilizacao_dados_on- line_instituicoes_ensino_superior.pdf.

[13] O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD). Informação disponível em https://edpb.europa.eu/our-work-tools/article-29-working-party_pt.

[14] O Comité Europeu para a Proteção de Dados (CEPD) é um organismo europeu independente que contribui para a aplicação coerente de regras em matéria de proteção de dados na União Europeia e promove a cooperação entre as autoridades de proteção de dados da UE. Informação disponível em https://edpb.europa.eu/about-edpb/about-edpb_pt.

[15] Cf. Bobbio, *O Futuro da Democracia*, 30.

Em conformidade com o Relatório da Comissão Nacional de Protecção de Dados 2017/2018, a atividade fiscalizadora tem continuado, apesar de não ter alcançado a intensidade pretendida e necessária, uma vez que "[…] a grande mediatização do regulamento e o aumento da consciencialização para o direito à proteção de dados levaram a que se registasse um maior reporte à CNPD de situações de infração".[16]

Em decorrência desse contexto, entre a entrada em vigor do RGPD - 25 de maio - e o fim do ano de 2018, foram feitas 238 ações de fiscalização que, somadas às 70 realizadas no início de 2018, perfazem um total de 308 inspeções, o que contrasta com as 170 realizadas no ano de 2017 e as 117 em 2016.[17]

A CNPD ainda é competente legalmente para aplicar sanções, quando a prática dos responsáveis pelo tratamento de dados, públicos ou privados, constituir contraordenação, isto é, não atenderem ao que o RGPD lhes impõe como conduta própria.[18] Nesse cerne, durante o segundo período de 2018, logo após a entrada em vigor do RGPD, foram abertos 610 processos de natureza contraordenacional, mantendo-se a tendência de aumento das denúncias ou mesmo de queixas dos cidadãos, que se cifraram em 439. O claro aumento da demanda pode significar a atenção ao novo Regulamento demonstrado por outras autoridades, pois delas foram recebidas participações das quais emergiram 173 processos e foram iniciadas 7 averiguações por iniciativa da CNPD.

> No quadro desta atividade, desde 25 de maio de 2018, a CNPD aplicou 22 coimas**,** num valor total de 408 990,40 EUR. Assinale-se que a maior parte do número de coimas é aplicado ainda ao abrigo do regime legal anterior (LDPD), e não ao abrigo do RGPD, por se reportarem a factos praticados antes da aplicação do diploma europeu e a lei nacional anterior definir molduras sancionatórias mais favoráveis aos arguidos.[19]

Em relação às coimas aplicadas, há uma evidente diminuição do seu número uma vez que, além de um caráter claramente sancionatório, também há um caráter pedagógico que tem validade para quem recebe as coimas, mas também para outras entidades, no sentido de estarem mais atentas às exigências do RGPD. Conforme o relatório publicado pela CNPD, as coimas diminuíram desde 2016, quando foram aplicadas 256, chegando a 160 no ano de 2017 e apenas 72 no ano de 2018. Contudo, os valores têm aumentado em proporção inversa, pois no ano de 2016 o valor se cifrou em 509 milhões de euros, em 2017 alcançou o montante de 266 milhões de euros e um valor de 488 milhões em 2018, sendo 80 antes de 25 de maio e 408 milhões depois.[20]

Importa compreender que o escopo da CNPD é a proteção de dados e não a aplicação de coimas; esta configura-se apenas como uma atividade meio, mas essencial

---

[16] Cf. Relatório de atividades da Comissão Nacional de Proteção de Dados 2017-2018.

[17] Cf. Relatório de atividades da Comissão Nacional de Proteção de Dados 2017-2018, p. 18.

[18] As alíneas b) e d) do nº 2 do artigo 83º do RGPD referem que as condições gerais para a aplicação de coimas devem considerar o carácter intencional ou negligente da infração e o grau de responsabilidade tendo em conta as medidas técnicas ou organizativas implementadas nos termos dos artigos 25º e 32º. O n. 3 do artigo 83º do RGPD limita e subordina estabelecendo que se o responsável pelo tratamento ou o subcontratante violar, intencionalmente ou por negligência, no âmbito das mesmas operações de tratamento ou de operações ligadas entre si, várias disposições do regulamento, o montante total da coima não pode exceder o montante especificado para a violação mais grave. No plano interno ver: alínea n) do art. 23º e os arts. 35º e 41º da Lei n.º 67/98 e a alínea h), do nº 1 do art. 19º da Lei 43/2004.

[19] Cf. Relatório de atividades da Comissão Nacional de Proteção de Dados 2017-2018, p. 28.

[20] Cf. Relatório de atividades da Comissão Nacional de Proteção de Dados 2017-2018, p. 28-29.

para manter o comportamento desejado nos responsáveis pelo tratamento. Essa é mais uma forma de o Estado exercer o poder a ele conferido pelos cidadãos, como o mediador de interesses conflitantes. Conforme Bobbio "[…] ter poder significa, em poucas palavras, ter a capacidade de premiar ou punir, isto é, de obter comportamentos desejados, ou prometendo, e estando em condições de dar, recompensas, ou ameaçando, e estando em condições de infligir, punições".[21] Portanto, as coimas são aplicadas na medida em que, apesar das ordenações impostas pelo RGPD, as mesmas são negligenciadas e acabam por caracterizar-se como contraordenações, e por isso, passíveis de serem penalizadas.

Mesmo com ações tão importantes, percebe-se, não sem apreensão, que acentuam-se as tendências para recolher cada vez mais informações pessoais sobre as pessoas singulares, para controlar os seus movimentos, para conhecer os seus hábitos e as suas preferências, para vigiar as suas opções individuais, o que nos faz lembrar o que nos diz Miranda Rosa quando afirma

> o exercício de qualquer direito é acompanhado do risco do abuso. O abuso do direito é fato comum na ordem jurídico-social e diante dele a sociedade estabelece remédios diversos, prevendo o seu controle, a sua correção e punição, obedecendo sempre ao grau de probabilidade de que ocorram, da gravidade de suas manifestações, e da importância dos valores assim atingidos.[22]

Portanto, da mesma forma que deve existir um determinado "controlo" dos poderes constituídos, deve-se ter em mente que certos direitos fundamentais não podem ser ingeridos em excesso.

3. A proteção de dados pessoais como sustentáculo da liberdade e o desafio da democracia

O exercício democrático, atrelado essencialmente às demandas coletivas, tem, na defesa das liberdades individuais, seu grande desafio material e normativo. Para tanto, o Estado deve manter mecanismos de vigilância capazes de evitar a violação de direitos fundamentais, o que não afasta, de todo, que o próprio Estado possa ser o violador desses direitos. A respeito da necessidade de que mesmo o Estado seja controlado perante a intromissão que deseja ter sobre a vida de seus cidadãos, Bobbio afirma ser

> Inútil dizer que o controle público do poder é ainda mais necessário numa época como a nossa, na qual aumentaram enormemente e são praticamente ilimitados os instrumentos técnicos de que dispõem os detentores do poder para conhecer capilarmente tudo o que fazem os cidadãos. Se manifestei alguma dúvida de que a computadorcracia possa vir a beneficiar a democracia governada, não tenho dúvida nenhuma sobre os serviços que pode prestar à democracia governante.[23]

A manifestação do pensamento e de opinião também são exemplos de liberdades fundamentais essenciais à existência da sociedade democrática, mas que devem ser sopesadas na relação com outros princípios e com eles coexistir, sem que, para tanto, nenhum dos direitos seja sacrificado, como, por exemplo, o da privacidade. Contudo, a presença de aparatos tecnológicos que recolhem compulsoriamente diferentes dados, autorizados ou não por seus sujeitos, acabam por relativizar esse direito; a profusão de sistemas biométricos, de videovigilância e de geolocalização é disso um

[21] Cf. Bobbio, *O Futuro da Democracia*, 180.
[22] Cf. Rosa, *Sociologia do Direito*, 188.
[23] Cf. Bobbio, *O Futuro da Democracia*, 29.

bom exemplo.

Nesse mesmo seguimento, o registo em larga escala da actividade dos internautas, a elaboração de perfis individuais detalhados e a consequente rotulagem discriminatória das pessoas[24] se posicionam contra o que a lata interpretação do artigo 35º da Constituição da República Portuguesa também se manifesta, e estende-se à proliferação de listas negras e de índex, por exemplo.

> Mas o preceito apresenta ainda uma vertente de defesa deste direito, desdobrada na proibição do tratamento de dados suscetíveis de implicar a discriminação do seu titular e ainda na proibição de acesso aos dados por terceiros. Note-se que, se inicialmente concebido como um direito de defesa perante o Estado, explicitado nas proibições vertidas nos n.º 3 e 4 do artigo 35.º, este direito nasce já num período histórico em que ao Estado se exige, não apenas a abstenção de ingerência na esfera jurídica dos cidadãos, como também uma função ativa para prevenir tal ingerência por parte de terceiros, sendo pacífico que o artigo 35.º vincula também as entidades privadas responsáveis pelos tratamentos de dados pessoais[25].

O monitoramento de dados pessoais, não necessariamente de dados íntimos, é um sintoma de uma sociedade vigiada, que pode caminhar para um verdadeiro controlo social do indivíduo. Acresce que o tratamento massivo de informação pessoal é feito, não raramente, de modo pouco transparente e quase imperceptível para as pessoas.

Mesmo assim, com a disseminação desses mecanismos de controlo, o cenário mundial em termos de proteção de dados é inquietante e tem-se agravado por razões de segurança, em nome da qual se reforça a utilização e convergência de tecnologias de vigilância, que recaem sobre a generalidade dos cidadãos.

---

[24] Quando se fala em rotulagem das pessoas através da veiculação de informações por meio digital, podemos inferir que se trata de um tipo de rotulagem direta, ou uma forma de discriminação direta. Mas nem sempre é assim, pois a discriminação assume formas bastante dissimuladas para poder sobreviver nos meios digitais sem que sejam alvo dos questionamentos daqueles que não concordam com esse tipo de postura discriminatória e defendem o direito à preservação da imagem de qualquer forma que seja, como expressão da dignidade humana. Assim, em relação à discriminação, além de ofender a Carta dos Direitos Fundamentais da União Europeia, em seu art. 21º, sobre a proibição da discriminação, o seu poderio de destruição das individualidades, também ofende o artigo 20º que diz respeito ao igual tratamento dos cidadãos. Para melhor esclarecimento, a discriminação, pode-se expressar de forma direta ou indireta. Cf. informações disponíveis em http://cite.gov.pt/pt/acite/dirdevtrab004.html. Considera-se que existe discriminação direta sempre que uma pessoa seja sujeita a tratamento menos favorável do que aquele que é, tenha sido, ou venha a ser dado a outra pessoa em situação comparável. Considera-se que existe discriminação indireta, sempre que uma disposição, critério ou prática aparentemente neutro seja suscetível de colocar uma pessoa, por motivo de um fator de discriminação, numa posição de desvantagem comparativamente com outras, a não ser que essa disposição, critério ou prática seja objetivamente justificado por um fim legítimo e que os meios para o alcançar sejam adequados e necessários.

[25] Cf. Filipa Urbano Calvão, "O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois", in *Jornadas nos Quarenta anos da Constituição da República Portuguesa. Impacto e Evolução*, Manuel Afonso Vaz (*et. al.*) (Porto: Universidade Católica Editora, 2017), https://repositorio.ucp.pt/bitstream/10400.14/23542/1/Nota%20introdutória.PDF. "O que é notado, de forma particular, na específica proibição de acesso por terceiros, bem como na vertente de proibição de tratamento de dados pessoais que são suscetíveis de gerar tratamento discriminatório, que exige ou pode exigir uma intervenção mais proativa do Estado. Note-se que esta última vertente, de fixação de um regime reforçado de proteção de certas categorias de dados, está diretamente ligada com a garantia de igualdade entre os cidadãos, demonstrando que a proteção dos dados pessoais não tem em si mesmo apenas um objetivo de tutela da privacidade, mas também uma importante função social de garantia da igualdade" (p. 90).

Será sempre necessário fazer verdadeiros juízos de proporcionalidade e encontrar as soluções mais adequadas. É imprescindível que, antes de feitas as opções e tomadas as decisões com reflexos para os direitos das pessoas, se façam estudos de impacto ao nível da privacidade e se avaliem de modo integrado, e não avulso, as consequências de tais medidas na vida dos cidadãos.

4. Algumas considerações conclusivas

A ordem democrática, longe de ser algo comum e natural na complexa organização dos Estados que a adotam, requer mecanismos de manutenção dos direitos fundamentais e das liberdades individuais que, conjugadas, garantem e sustentam a democracia.

Assim, o Estado Democrático estabelece mecanismos de proteção que atuam para regular as relações entre os cidadãos, mas também destes com o Estado e, contemporaneamente, o foco também se coloca nas relações entre os mercados e os grupos que o gerem e os cidadãos, dando forma ao aspeto regulador do Estado. Dada a quase incapacidade de cada cidadão fazer valer, por si mesmo, os seus direitos, o Estado deve proteger esses interesses, estendendo suas mãos protetivas no combate a quaisquer violações, inclusive as suas próprias, justificando a emergência de organismos independentes que são constituídos por iniciativa estatal para assegurar essa regulação setorial.

O resguardo dos dados pessoais, como componentes da privacidade de cada cidadão, tem como finalidade a garantia da liberdade individual. Por isso, as ações da CNPD, tanto na esfera preventiva em relação às violações, como coercitivas, no sentido de investigar possíveis contraordenações e de estabelecer coimas, possuem um caráter garantidor da ordem democrática. A democracia, como uma forma de estabelecimento das relações de poder, deve sempre demandar que se equilibrem os interesses do Estado Liberal e do Estado Social, garantindo principalmente que os direitos, inclusive das minorias, sejam respeitados. Seguindo a senda da argumentação apresentada por Filipa Urbano Calvão,

> De facto, a ideia fundamental é a de que a proteção dos dados pessoais, ou seja, a informação relativa a pessoas singulares identificadas ou identificáveis, é condição necessária para reduzir ou eliminar as influências externas na esfera individual. Enquanto modo de garantir a privacidade, afirma-se ainda como instrumento de garantia da liberdade (liberdade de ação, de expressão, de pensamento) e de desenvolvimento da personalidade de cada um e da livre participação na sociedade. Nessa medida, é ainda imprescindível para assegurar a própria democracia, no sentido de aí ser reconhecido um espaço próprio de pensamento e de escolhas, livre de influências e pressões externas públicas e privadas[26].

Assim, as ações empreendidas pela CNPD figuram dentro de uma moldura essencial que visa a manutenção de direitos e a garantia da liberdade do ser humano, aspetos sem os quais sua dignidade está insegura, e sem a qual, em médio e longo prazo, a democracia não pode se sustentar. Afinal, sem a liberdade individual, a democracia se sustenta? Logo, a breve exposição das atividades empreendidas pela CNPD tem o claro intento de demonstrar a importância dessas ações para o fortalecimento do processo democrático, uma vez que as mesmas, tanto em sua

[26] Cf. Calvão, "O direito fundamental à proteção dos dados pessoais", 88.

atividade fim – a proteção dos dados pessoais de pessoas singulares –, quanto em sua atividade meio – emissão de pareceres, consultas, fiscalização, aplicação de coimas, sensibilização de pessoas singulares ou de instituições, tanto públicas como privadas –, fundamentam-se no desejo e na missão de proteção do direito à privacidade como componente essencial da dignidade humana e a defesa das liberdades individuais, como base da democracia.

Sob pena de fracassarmos definitivamente na função social fundamental de garantir o respeito e a promoção da dignidade da pessoa humana – como decorre do artigo 1.º da CRP –, que, da mesma forma se encontra presente em normativos europeus e internacionais, há que traçar um limite à tutela dos valores que estão numa relação de tensão entre a privacidade e a liberdade, já que estes constituem também pilares do Estado de Direito Democrático.

Pistas para uma cidadania à luz da interoperabilidade

João Ferreira*

RESUMO: Para eliminar os obstáculos a um mercado único digital, a Comissão lançou a temática da interoperabilidade, representando um debate crucial para o futuro do exercício da cidadania na UE. Um cidadão desloca-se no espaço único, como portador de direitos que têm de ser assegurados. Os setores públicos têm procurado garantir o exercício de direitos comuns aos cidadãos europeus, onde os estados trabalham em acordos comuns para que seja facilitado esse mesmo exercício, como a uniformização de informação de identificação ou sistemas de reporte comuns. Quando se abre caminho à digitalização da administração pública, tem-se em vista poupar tempo, reduzir custos, aumentar a transparência e melhorar tanto a qualidade dos dados e serviços públicos. Todavia, não poderemos esquecer os desafios que são colocados à inclusão na cidadania digital. Portanto, deveremos afinar questões atinente à cidadania digital – e tudo o que isso implica - e a portabilidade de direitos dentro da União.

PALAVRAS-CHAVES: Cooperação transfronteiriça – Interoperabilidade – e-Governança – Cidadania digital

ABSTRACT: In order to remove obstacles to a digital single market, the Commission launched the interoperability theme, representing a crucial debate for the future of citizenship in the EU. A citizen moves in the single space, as a bearer of rights that have to be ensured. The public sectors have sought to ensure the exercise of rights common to European citizens, where states work on common agreements to facilitate this exercise, such as standardization of identification information or common reporting systems. When digitizing the public administration, the aim is to save time, reduce costs, increase transparency and improve the quality of public data and services. However, we can not forget the challenges to inclusion in digital citizenship. Therefore, we must refine issues regarding digital citizenship - and all that implies - and the portability of rights within the Union.

KEYWORDS: Cross-border cooperation – Interoperability – e-Governance – Digital citizenship

* Investigador JusGov, Advogado, Presidente PPJur – Plataforma de Pensamento Jurídico e Formador.

1. Introdução

A realidade da integração europeia, por via económica, trouxe-nos diversos desafios num espaço em que não existe um poder federal tradicional – que suprisse de forma unilateral as dificuldades que surgem em processos deste tipo – dando lugar ao um mercado comum. Na verdade, esta integração foi a forma que o projeto europeu encontrou para responder às diferenças entre administrações e Estados, fomentando as soluções comuns e interoperáveis para problemas que não se resolvem de forma individual, mas através da partilha, dando lugar a uma cidadania compatível com este mercado, com tudo o que implicava.

Ora, a União Europeia (UE) tem desenvolvido uma ação de promoção do desenvolvimento harmonioso, de modo a reforçar a coesão económica, social e territorial.[1] Para tal, a criação das bases de uma União Económica e Monetária foi fundamental, pautando-se por objetivos claros de "plena realização do mercado interno […]; regras comuns adequadas a assegurar a competição leal […]; satisfatória política de coordenação macroeconómica […]"[2] e, como já referimos, a coordenação económica e social no seu conjunto. Harmonizar seria o ponto chave para um progresso político, económico e social no espaço político europeu que só encontrou esse respaldo no aperfeiçoamento realizado à sua arquitetura aquando do Tratado de Maastricht, contribuindo para manter a paz em todo o território.

Foi-se desenvolvendo um mercado comum interno de oportunidades em que cada um dos Estados-Membros exponenciasse o seu desenvolvimento e, através da circulação que daria aos seus cidadãos, poderia procurar expandir os horizontes de afirmação económica dos seus tecidos empresarias e mão-de-obra – fosse mais especializada, fosse mais qualificada. Desta forma, criou-se um grau superior de integração económica onde circulam bens e fatores de produção, não assentando numa visão fechada de eliminação dos entraves à livre circulação das mercadorias – pelo contrário –, procurando um desenvolvimento harmonioso e equilibrado das atividades económicas no conjunto da União.

Para garantir que a integração fosse uma realidade surgiu a necessidade de que as administrações estivessem em linha, criando condições e regras comuns de ação. Ora, um cidadão quando se desloca no espaço único é ele em si mesmo portador de direitos que têm de ser assegurados e, por essa razão, os setores públicos têm procurado garantir o exercício de direitos comuns aos cidadãos europeus. Assim, os estados devem trabalhar ao nível da UE, entre sectores, de modo a evitar que se optem por soluções incompatíveis entre si, suscetíveis ao aparecimento de barreiras à prestação de serviços públicos europeus, como a uniformização de informação de identificação ou sistemas de reporte comuns. Como nota Joana Covelo de Abreu "[é] por isto que ´atingir a plena interoperabilidade no interligado [Mercado Único Digital] irá [permitir] aos serviços públicos oferecer […], aos cidadãos, serviços transfronteiriços`".[3]

---

[1] Art. 174.º Tratado de Funcionamento da União Europeia (TFUE)

[2] João Luís Mota de Campos e João Mota de Campos, *Manual de direito europeu: o sistema institucional, a ordem jurídica, o ordenamento económico da União Europeia,* 6ª edição (Coimbra: Coimbra Editora, 2010).

[3] Joana Covelo de Abreu, "O Mercado Único Digital e o seu desígnio político constitucional: o impacto da Agenda Eletrónica Europeia nas soluções de interoperabilidade", *UNIO - EU Law Journal* III, nº 1 (Janeiro 2017): 130-150.

2. A realidade (trans)fronteiriça

Falar de casos em que as comunicações e troca de experiências transfronteiriças funcionam verdadeiramente só seria possível com a aferição de vários e diferentes critérios. Um mercado único surge para que as fronteiras físicas não sejam um entrave à circulação dos bens que se pretendem ver em movimento. Ora quando essas fronteiras são eliminadas, existe um espaço de oportunidade e de compreensão mútuas das potencialidades que a cooperação entre os diferentes lados das fronteiras pode fomentar e proporcionar. Não é fácil debater esta questão de forma linear porque se poderão envolver autoridades locais e regionais, administrações nacionais ou realidades supranacionais (como é o caso das instituições europeias), propiciando o encontro de desafios comuns onde as autoridades têm capacidades de resposta diferentes a estes.

Portanto, atualmente, subsistem dúvidas e desafios para uma verdadeira implementação de realidades transfronteiriças que tão somente o alinhamento e a concertação de práticas não irão resolver. Numa organização política onde a questão da soberania é difícil de resolver, onde a sua perda relativa – e, consequentemente, da sua representação – acabam por ser causa-efeito da resistência em aceitar um processo de integração, onde as disparidades de desenvolvimento económico e social entre os diferentes lados da fronteira acabam por dificultar o avanço, amiúde, de qualquer esforço de integrar em realidades comuns diferentes territórios, terão que ser encontradas vontades que se cruzem de forma a enfrentar paulatinamente e por pequenos passos os vários desafios que se colocam.

No campo do universo digital o suplantar das fronteiras também se faz no presente, não podendo a ideia de um mercado digital ser desassociada da existência de barreiras a este mercado, tal como na realidade territorialidade. Para eliminar os obstáculos a um mercado único digital, a Comissão lançou a temática da interoperabilidade, representando um debate crucial para o futuro do exercício da cidadania na UE com o auxílio das administrações nacionais. As organizações administrativas de cada um dos estados, funcionando numa rede interoperável irão paulatinamente criar meios de confiança recíproca nos agentes dos diferentes lados da fronteira.[4]

Abordar a temática da interoperabilidade tem por vista a busca por maior eficiência no trabalhado de uma ou das administrações públicas, redução de custos, criação de economias de escala e maior rapidez no que diz respeito à resposta a problemas comuns.

Devemos referir os três conceitos distintos que nos trazem a um debate de atualidade na governação eletrónica, onde a E-Administração[5] assume uma importância

[4] Então, dar-se-á o incremento do fomento da "observância dos princípios do reconhecimento mútuo e da confiança recíproca entre Administrações Públicas de diferentes Estados-Membros, promovendo ainda mais o efeito administrativo horizontal quando as Administrações Públicas nacionais atuam como administrações funcionalmente europeias sem que se vejam ataviadas por barreiras geográficas". Ao mesmo tempo teremos um compromisso quase total entre as Administrações públicas nacionais e as instituições europeias "através de mecanismos de interconexão que se encontram a ser estabelecidos em todo o tipo de áreas de modo a que quer a confiança recíproca, quer o reconhecimento mútuo possam sair reforçados entre as administrações nacionais e europeia", cf. Abreu, "O Mercado Único Digital e o seu desígnio político constitucional", 130-150.

[5] Aqui teremos que ter presente os conceitos que um direito administrativo ao nível do espaço europeu terá que considerar, sendo eles "um direito administrativo multinível ou plural, num contexto de interadministratividade". Sophie Perez Fernandes relembra a distinção feita por Suzana Tavares da

acrescida no que diz respeito à relação com o conceito de interoperabilidade. Na disponibilização de informações e serviços ao público pela via eletrónica de modo mais eficaz e eficiente na resposta a este problema, salvaguardando-se a imperiosidade de as administrações funcionarem em linha, ou melhor, em rede – pois a linha pressupõe-se apenas entre dois intervenientes –, em plataforma uniformizadas para facilitação de procedimentos e respostas a problemas comuns.[6] Por vezes, esta prática de atos comuns revela-se por instrumentos de convergência internormativa de sentido descendente, onde o Direito da União Europeia conforma e modela, de forma imperativa ou sugestiva (*soft law*), os direitos administrativos dos Estados-Membros.

De seguida, a e-Governação[7] diz respeito aos canais de comunicação que as tecnologias de informação e comunicação permitem criar para participação no processo de elaboração de políticas incluindo os problemas reais da população que os faz chegar diretamente aos últimos decisores.

Já a e-Democracia[8] terá a ver com a disponibilização efetiva dos meios que permitem uma democracia próxima, aberta e, muitas vezes, em tempo real, com plataformas de observação do trabalhado dos agentes políticos, etc. Assim, uma União vocacionada para a interoperabilidade deverá ter em conta estas vertentes na sua atuação.

3. A cidadania

A Carta dos Direitos Fundamentais da União Europeia, quando estabelece a liberdade de circulação e de permanência no seu artigo 45.º como um direito fundamental, não se alheia à consagração da cidadania europeia em Maastricht. Habermas propôs três caminhos para compreendermos a questão da cidadania "em

---

Silva "1) o direito administrativo europeu multinível, assente em ´procedimentos complexos, mas de administração direta, ou seja, os casos em que a decisão administrativa é tomada pelas entidades administrativas da União, embora o procedimento administrativo seja instruído, em parte ou totalmente, pelas entidades administrativas de um Estado-Membro`; e 2) o direito administrativo europeu das inter-relações, também assente em ´procedimentos administrativos complexos, mas de administração indireta`, estando aqui em causa, por um lado, ´procedimentos em que as atrocidades dos Estados-Membros adoptam decisões segundo o direito europeu, que valem para todo o território Europeu` e, por outro, ´procedimentos em que as autoridades dos Estados-Membros adoptam decisões segundo o direito europeu, cujos efeitos [se] estendem a todo o território Europeu`". Sophie Perez Fernandes, "Administração Pública" in *Direito da União Europeia - Elementos de Direito e Políticas da União*, coord. Alessandra Silveira, Mariana Canotilho e Pedro Madeira Froufe (Coimbra: Almedina, 2016), 73-161.

[6] Nos domínios da justiça e segurança, avanços recentes nas plataformas interoperáveis irão permitir que os sistemas existentes se complementem mutuamente, facilitando a identificação correta das pessoas e contribuindo para combater a fraude de identidade. São máxime disso o portal europeu de pesquisa (que permitirá às autoridades competentes efetuarem pesquisas simultaneamente em vários sistemas de informação da UE, utilizando dados biográficos e biométricos); o serviço partilhado de correspondências biométricas (que permitirá a pesquisa e a comparação de dados biométricos -impressões digitais e imagens faciais - existentes nos vários sistemas); o repositório comum de dados de identificação (que incluirá os dados de identificação biográficos e biométricos de nacionais de países terceiros disponíveis em vários sistemas de informação da UE); o detetor de identidades múltiplas (que verifica se os dados de identidade biográficos da pesquisa existem noutros sistemas abrangidos, a fim de permitir detetar identidades múltiplas ligadas ao mesmo conjunto de dados biométricos).

[7] Para mais considerações ver Abreu, "O Mercado Único Digital e o seu desígnio político constitucional".

[8] *Idem*

termos de mercado, termos etno-culturais (orientados para laços culturais comuns) e em termos cívicos (visando a partilha de normas e valores)".[9]

A construção deste conceito avançou do conceito de cidadania de mercado (relacionada com o exercício de direitos económicos) para uma cidadania social (ligada às questões da solidariedade social, tendo em vista o reconhecimento dos direitos fundamentais e o envolvimento dos cidadãos). Veja-se o acórdão Martínes Sala[10] que deu um grande passo para a "desvinculação entre estatuto de cidadania (direitos e liberdades que lhe são associados) e exercício de atividades económicas".[11]

O cidadão tornou-se no ator principal da construção europeia quando foi institucionalizado o mercado interno, "a partir do momento em que a garantia essencial de uma não discriminação económica em razão da nacionalidade (igualdade predominantemente económica) foi atingida no espaço da integração".[12] Maastricht tornou em realidade formal o conceito de "cidadão" como forma de legitimação do processo de construção europeia, numa cidadania complexa em dupla vertente – nacional e europeia.

Inclui-se nesta realidade uma cidadania supranacional que confere direitos aos cidadãos europeus como a livre circulação em todo o espaço, independentemente do estatuto económico de trabalhador ou de prestador de serviços, sem necessidade de uma razão que a justifique economicamente ou de invocar alguma liberdade para que circule. O Tribunal de Justiça da União Europeia (TJUE) foi fundamental na criação e construção progressiva do conceito de que alguns autores apelidam de "cidadania de mercado".[13]

Esta foi uma das mais importantes consagrações, a da cidadania da UE: afinal, a cidadania europeia não se destina a suplantar outras identidades, porque qualquer nacional de um Estado-Membro é cidadão da União. Por esta via, a cidadania da União deve complementar e não substituir a cidadania nacional, criando uma estreita ligação com e entre os povos da Europa.

Todavia, nos dias de hoje, é imperativo colocar no seio do debate o exercício de outros tipos de direitos que esta cidadania acarreta, a cidadania no mundo digital – chamar-lhe-ia cidadania digital. Este exercício de um cidadão digital num mundo global denota vários desafios e envolve diversos saberes, por isso não podemos pensar na infoinclusão como que reduzida ao saber "clicar" ou abrir um determinado serviço no computador, antes exige-se mais do que isso.

Um cidadão do mundo global terá de ser, necessariamente, alguém informado, mas que percebe o mundo digital – não por intuição, mas por perceção do que está à sua frente. Facilmente o *homo digitalis* se liga a uma rede social, partilha conteúdos

---

[9] J. Cunha Rodrigues, "Artigo 45º - Liberdade de circulação e de permanência" in *Carta dos Direitos Fundamentais da União Europeia. Comentada*, coord. Alessandra Silveira e Mariana Canotilho (Coimbra: Almedina, 2013), 519-529.

[10] Acórdão TJUE Martínez sala, de 12 de maio de 1998, processo C-85/96.

[11] Alessandra Silveira, "Cidadania Europeia e Direitos Fundamentais" in *Direito da União Europeia - Elementos de Direito e Políticas da União*, 17-72.

[12] Pedro Madeira Froufe e José Caramelo Gomes, "Mercado Interno e Concorrência" in *Direito da União Europeia - Elementos de Direito e Políticas da União*, 449-504.

[13] Aproveitando para uma pequena referência a um acórdão que aprofundou a dupla vertente da cidadania europeia, o acórdão Ruiz Zambrano, de 8 de março de 2011, processo C-34/09 onde o TJUE refere no considerando n.º 41 que "o estatuto de cidadão da União tende a ser o estatuto fundamental dos nacionais dos Estados-Membros" e no seu considerando n.º 42 "o artigo 20.º TFUE obsta a medidas nacionais que tenham o efeito de privar os cidadãos do gozo efetivo do essencial dos direitos conferidos pelo seu estatuto de cidadão da União".

para o outro lado do mundo e tem na mão mais tecnologia do que um qualquer computador dos anos 80. Estamos a viver na era da "geoeconomia das plataformas"[14] onde se pede um carro que permita a deslocação em 5 segundos e se reservem umas férias noutros tantos, num processo desmaterializado onde não se consegue compreender, muitas das vezes, com quem se interage ou o que é que efetivamente se está a contratar ou a confirmar.

Colocar em debate a temática do mundo digital reduz-se, muitas das vezes, a referir programas públicos de contacto com as tecnologias que se destinam a trabalhadores desempregados, os quais se vislumbram sem aplicação prática à realidade em que se quer voltar a inserir aqueles cidadãos. Obrigatoriamente, o futuro passará por dar condições para que qualquer cidadão se sinta capaz de exercer a sua cidadania digital num mundo complexo que fala de excluídos da informação, conotando-os com quem não sabe usar ou não usa as tecnologias de informação e comunicação. Os pensadores destas temáticas esquecem-se que, nos dias de hoje, existem antenas de *wi-fi* em locais púbicos, e que ter dados móveis para aceder à rede é mais barato e um aparelho onde se aceda a conteúdos digitais é mais acessível do que há vários anos atrás, adquirindo-se um telemóvel pelo valor equivalente a um ou dois salários mensais, porque se tem esse equipamento como fundamental para a vida em sociedade ou para a liberdade individual de cada um.

Em Portugal, tornou-se comum programas de promoção da modernização administrativa onde se trocam computadores antigos por novos, se refresca a aparência dos sistemas e se introduzem novas ferramentas. Todavia, esta atividade de chamada "modernização" é posta em prática com um consequente incremento em vários casos da carga burocrática do processo que se dizia querer simplificar, acabando por replicar as ações que se fazem pelos meios tradicionais nos meios digitais como preenchimento de processos, assinatura de processos de forma digital e manual, etc. A consciência para a simplificação que a digitalização permite é algo que a cultura administrativa portuguesa tem percecionado aos poucos, e que poderá num futuro próximo levar a uma efetiva eficiência de sistemas, lembrem-se de programas como o Simplex que visa eliminar atos desnecessários na relação do cidadão com a administração e, desse modo, utilizando meios eletrónicos em linha, objetiva-se responder mais rapidamente às necessidades. Não se esqueçam, também, as imensas plataformas de acesso a serviços da administração pública que proliferam com limitações quanto ao avanço tecnológico de *softwares* ou ao uso de assinatura digital.

Clama-se, cada vez mais, pela 'smartificação' da sociedade e dos indivíduos que a compõem, mas não se dá, verdadeiramente, ferramentas. Para ser *smart* será necessário que se aja de modo *smart* e se ensine a compreender este processo que a sociedade moderna está a experimentar de constante adaptação e de saberes muito diversos que não se coaduna com uma visão balizada e unidisciplinar. O estado-administração também teria de se digitalizar, não apenas do ponto de vista de colocar meios tecnológicos, mas também de dar as competências necessárias – e até

[14] "A revolução digital põe em causa não apenas a intermediação económica e comercial, mas, a prazo breve, também, a intermediação política e a fonte de legitimação democrática e representativa tal como nós a conhecemos nas sociedades ocidentais, razões mais do que suficientes para que o conservadorismo político-partidário tome as medidas defensivas e cautelares que se justificam nesta conjuntura. Seja como for, a revolução digital é imparável e mudanças profundas ocorrerão nas relações entre a sociedade civil, o estado e as plataformas digitais." António Covas, "A geoeconomia das plataformas e o homo digitalis", *Público*, Janeiro de 2019, https://www.publico.pt/2019/01/11/opiniao/opiniao/geoeconomia-plataformas-homo-digitalis-1857303.

aprofundadas – para poder funcionar de modo inteligente, vejam-se os princípios assentes no "Plano de ação europeu (2016-2020) para a administração pública em linha"[15] do digital por definição[16] e da interoperabilidade por definição,[17] onde se prevê que os serviços públicos das administrações públicas devem ser prestados de forma privilegiada por via eletrónica – através de um único ponto de contacto, de forma uniforme, aos diferentes canais do mercado único.

Como tal, falar da cultura organizacional hodierna é referir o grau de literacia digital da população e da administração pública para enfrentar os novos desafios da nova administração de serviço público.[18] Como abordámos acima, não se trata de manipular um qualquer dispositivo inteligente, porque aí a população tem demonstrado que, com serviços intuitivos, se consegue adaptar aos poucos, mas sim a aculturação digital necessária para que a inteligência da administração se torne produtiva e não um obstáculo ao seu bom e melhor funcionamento. São questões como estas que nos devem fazer refletir no sistema de educação geral, onde já existem escolas dos primeiros ciclos de estudos que começam por ensinar a programar e a linguagem deste ato como ferramenta funcional fundamental na base do futuro processo educativo e formativo, podendo incluir-se a formação para a cidadania e para o pensamento e compreensão da sociedade.

Alguém que está no cerne destas questões sabe que se potenciar a disponibilização de serviços eletrónicos integrados e transversais de acordo com as necessidades do cidadão, respondendo à necessidade de comunicação e troca de informação eletrónica entre agentes públicos e privados irá criar desafios de índole técnica, funcional e administrativa no que diz respeito à interação entre setores disciplinares tão diferentes, por vezes, dentro de uma mesma administração comum. Não se tratará, portanto, de converter um quadro organizativo e administrativo informático num quadro digital, mas sim de tratar toda a estrutura organizacional hierárquica pelos cânones participativos e colaborativos das plataformas. Referimo-nos à superação dos entraves que o nosso pensamento lógico, dedutivo e tradicional cria a novas formas de atuar.

4. Conclusão

Cumpre-nos lembrar que subsistem problemas à aplicação destas realidades

[15] Comissão Europeia, "Plano de ação europeu (2016-2020) para a administração pública em linha: acelerar a transformação digital da administração pública", Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, 2016.

[16] "as administrações públicas devem prestar os serviços por via eletrónica (incluindo informações legíveis por meios mecânicos) como opção privilegiada (mantendo outros canais abertos para quem não utiliza esta via por preferência ou necessidade). Além disso, os serviços públicos devem ser prestados através de um único ponto de contacto ou de um balcão único e através de canais diferentes", *idem.*

[17] "os serviços públicos devem visar trabalhar uniformemente no Mercado Único e através de domínios organizacionais, com base na livre circulação de dados e serviços digitais na União Europeia", *idem.*

[18] Portugal lançou, através da Agência para a Modernização Administrativa, a iAP (Interoperabilidade na Administração Pública) que é uma plataforma central, orientada a serviços, tendo como principal objetivo dotar a Administração Pública de ferramentas partilhadas para a interligação de sistemas, federação de identidades, fornecedor de autenticação, *messaging*, pagamentos, entre outras, que permitam de uma forma ágil e com economia de escala, a composição e disponibilização de serviços eletrónicos multicanal mais próximos das necessidades do cidadão e empresas. Compreende essencialmente um conjunto de 3 macro-serviços: plataforma de integração; plataforma de pagamentos da administração pública e *gateway* de SMS da administração pública (que permite a receção e envio de SMS entre a administração pública e o cidadão).

aos territórios, desde logo as diferenças na cobertura digital numa lógica de infraestruturação entre os diferentes lados do território e as assimetrias existentes. Depois, o grau de competência digital e de literacia nestes enredos por parte das populações, referindo-se, por esta via, o modo como os sistemas de ensino, educação e formação de profissionais está estruturado.

Quando se abre caminho à digitalização da administração pública, tem-se em vista poupar tempo, reduzir custos, aumentar a transparência e melhorar tanto a qualidade dos dados e serviços públicos. Todavia, não poderemos esquecer os desafios que são colocados à inclusão na cidadania digital.

Os programas públicos que se implementam devem dotar-se de flexibilidade do aplicador em relação ao público alvo a que se destinam e preocupar-se menos com rankings e estimativas, mas antes com os objetivos que efetivamente acompanham esse tipo de iniciativas. Adiantaria que qualquer um dos objetivos passará por dar capacidade de exercício de uma cidadania digital discernida, informada e crítica, sem esquecer as ferramentas de compreensão e que permitem o uso das plataformas e conteúdos digitais – o que está à frente de cada cidadão é tantas vezes algo que fica distorcido aos olhos de um qualquer leigo apresentando-se com um interface simples, escondendo um emaranhado de questão e desafios como a proteção dos dados pessoais de cada um.

Deve a União providenciar por uma maior e melhor comunicação com e entre as administrações públicas e uma maior sensibilização das mesmas em matéria de interoperabilidade. Ao mesmo tempo, os serviços públicos nacionais têm de estar ligados e interligado, extravasando fronteiras que barrem a sua interconexão com outros do mesmo cariz ao nível da UE, aprofundando o mercado digital único. Não se poderá achar que esta será uma ação sem coordenação em diferentes níveis de decisão, pois, no caso de isso acontecer, existirá uma fragmentação digital entre os serviços públicos que ficou por solucionar – desde o processo legislativo, ao processo administrativo, passando pelas plataformas digitais criadas para articulação entre as administrações.[19]

O êxito da execução de programas de interoperabilidade exige o envolvimento ativo e coordenado de todos os intervenientes na ação europeia, nacional e subnacional, especialmente das administrações públicas. Para dar uma resposta rápida aos atuais desafios, os EM encetam esforços em abordagens individuais e divergentes quanto à matéria de interoperabilidade, resultando em soluções incompatíveis entre si que não dão uma resposta cabal aos problemas detetados, mas criam maiores gastos e atropelos fragmentados ao bom funcionamento de uma administração em rede com anseios comuns.

Portanto, deveremos afinar questões atinente à cidadania digital – e tudo o que isso implica - e a portabilidade de direitos dentro da União. A cidadania desterritorializou-se, desmaterializou-se e foram criados novos direitos fundamentais num mundo com menos barreiras que as de um território físico.

[19] "Atualmente, as administrações públicas gerem grandes quantidades de dados em diferentes formatos, utilizando métodos de gestão de dados diferentes, guardando várias cópias em muito repositórios diferentes e publicando-os frequentemente em portais de toda a Europa, sem qualquer tipo de harmonização em termos de conteúdo e de apresentação." Comissão Europeia, "Quadro Europeu de Interoperabilidade – Estratégia de execução", Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, 2017.

Regulamento (UE) 2018/302 contra a discriminação digital na União Europeia e a apuração da prática do *geoblocking* e *geopricing* no Brasil

Nelson Alex Lorenz*

*RESUMO: O presente artigo examina aspectos do Regulamento (UE) 2018/302 sobre a discriminação digital (*geoblocking*) disseminada no âmbito do* eCommerce. *A prática viola o exercício da legítima vontade do interessado na compra de bem ou serviço em razão da sua nacionalidade, local de residência ou de estabelecimento, e prejudica a livre circulação de mercadorias – a primeira das quatro liberdades fundamentais do mercado interno europeu. O objetivo é cotejar quest*ões centrais *desse novo diploma legal com as fundamentaç*ões *traduzidas pelo Ministério Público do Rio de Janeiro (MPRJ) e pelo Departamento de Proteção e Defesa do Consumidor (DPDC) do Brasil nos processos judiciais e administrativos movidos em face da empresa Decolar.com. Segundo consta nos autos, a empresa teria bloqueado ofertas de reservas em estabelecimentos hoteleiros e praticado precificação diferenciada em razão da localização digital.*

PALAVRAS-CHAVE: Discriminação digital – Geoblocking – eCommerce

ABSTRACT: This article examines aspects of Regulation (EU) 2018/302 on digital discrimination (geoblocking) disseminated within eCommerce. The practice infringes the legitimate interest of the person concerned in the purchase of goods or services on account of his nationality, place of residence or establishment and undermines the free movement of products - the first of the four fundamental freedoms of the European internal market. The objective is to compare the central issues of this new legal diploma with the grounds translated by the Public Ministry of Rio de Janeiro (MPRJ) and the Department of Consumer Protection and Defense (DPDC) of Brazil in the judicial and administrative proceedings brought against the company Decolar.com. According to the records, the company would have blocked offers of reservations in hotel establishments and practised differential pricing due to the digital location.

KEYWORDS: Digital Discrimination – Geoblocking – eCommerce

* Mestrando em Direito da União Europeia pela Universidade do Minho (UMinho – Portugal) e em Ciência Jurídica pela Universidade do Vale do Itajaí (Univali – Brasil). Contato: lorenz@edu.univali.br.

1. Introdução

O mercado interno europeu se projeta como um espaço sem fronteiras físicas e digitais,[1] sustentado pela força da livre circulação de pessoas, bens, serviços e capitais e agora reforçado pela edição do Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho.[2] A norma tem a finalidade de prevenir o bloqueio geográfico injustificado e discriminações em razão da nacionalidade, local de residência ou local de estabelecimento dos adquirentes de bens e serviços no mercado europeu.

A União Europeia dispõe, portanto, de um marco regulatório moderno e complementar a outros instrumentos normativos instituídos desde o início da sua formação a partir da segunda metade do século XX. O Relatório da Comissão Europeia ao Conselho e ao Parlamento Europeu,[3] relativo ao inquérito setorial sobre comércio eletrônico,[4] conduzido pelo método de *mystery shopping*,[5] apurou, em 2016, que 63% de 10 mil sites examinados operavam o bloqueio geográfico, não permitindo a compra a partir da localização do interessado em outro Estado-Membro. As rotinas de discriminação geográfica mais comuns foram as seguintes:

> Negando acesso. 2% de todos os sites bloquearam o acesso ou redirecionaram automaticamente os compradores misteriosos.
>
> Impedindo o registro. 27% dos sites onde os compradores misteriosos tentaram se registrar como uma etapa necessária para prosseguir com a compra impediram que eles se registrassem com sucesso.
>
> Recusa em entregar. Depois que o registro em um site transfronteiriço foi concluído com sucesso, 32% dos vendedores *on-line* se recusaram a entregar o produto ou fornecer o serviço ao país dos compradores.
>
> Recusa de pagamento. Durante a fase de pagamento do processo de compra, em 26% dos sites transfronteiriços, os compradores não puderam pagar porque os meios de pagamento não foram aceitos/oferecidos ou porque não conseguiram inserir os dados do cartão com sucesso.

[1] Comissão Europeia, "Prioridades para o mercado único digital da União Europeia", acesso em Março 22, 2019, https://ec.europa.eu/commission/priorities/digital-single-market_pt.

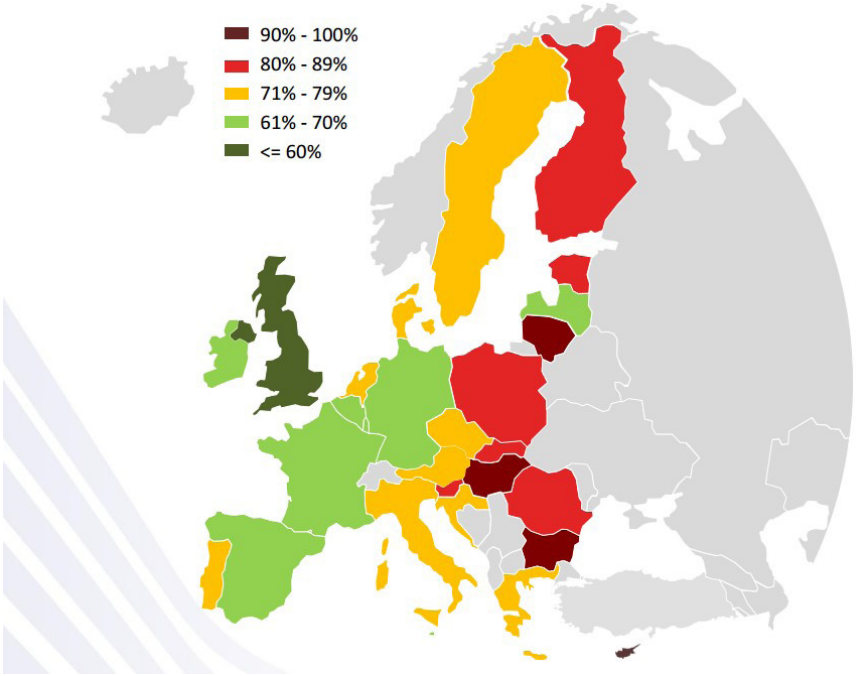
[2] Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018, que visa prevenir o bloqueio geográfico injustificado e outras formas de discriminação baseadas na nacionalidade, no local de residência ou no local de estabelecimento dos clientes no mercado interno, e que altera os Regulamentos (CE) n. 2006/2004 e (UE) 2017/2394 e a Diretiva 2009/22/CE (Texto relevante para efeitos do EEE) JO L 60I de 2.3.2018, p. 1-15, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R0302.

[3] Comissão Europeia, "Relatório da Comissão ao Conselho e ao Parlamento Europeu – Relatório final relativo ao inquérito setorial sobre o comércio eletrônico", acesso em Março 22, 2019, http://ec.europa.eu/competition/antitrust/sector_inquiry_final_report_pt.pdf.

[4] Cfr. Comissão Europeia, "The European Commission sheds light on territorial restrictions in the online environment", acesso em Março 23, 2019, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=30050.

[5] Entende-se o método de pesquisa na forma de "cliente oculto" ou *mystery shopper* ou *mystery shopping* como aquele realizado por pesquisadores contratados com a finalidade de agir como se fossem clientes, para relatar a experiência de compra e o papel da equipe de vendas. Esta atividade está em expansão e possui associação profissional, a exemplo da *Mystery Shopping Professionals Association* – MSPAÒ Europe/Africa, acesso em Junho 30, 2019, https://www.mspa-ea.org/mystery-shoppers.html.

Figura 1: Prevalência global de bloqueio geográfico por país do retalhista online no Mercado Único Digital da União Europeia – Inquérito[6] publicado em maio 2016.



Comissão Europeia: inquérito setorial sobre o bloqueio geográfico relativo ao comércio eletrônico na União Europeia.

Os resultados do inquérito setorial evidenciaram a generalização do bloqueio geográfico em parte substantiva dos 28 Estados-Membros [Figura 1]. Em alguns deles o entrave foi quase intransponível ou absoluto para os consumidores residentes na faixa leste de países integrados à UE. De acordo com a Comissão Europeia,[7]

> Cada vez mais produtos e serviços são comercializados através da Internet, mas as vendas transfronteiras em linha no interior da UE só estão a crescer lentamente. As conclusões iniciais da Comissão decorrentes do inquérito setorial hoje publicado [março de 2016] abordam uma prática, designada bloqueio geográfico, pela qual os retalhistas e os fornecedores de conteúdos digitais impedem os consumidores em linha de comprarem bens de consumo ou de acederem a serviços de conteúdos digitais em virtude da sua localização ou país de residência. Este é um dos fatores que afetam o comércio eletrónico transfronteiras.

O novo diploma legal tem como alvo principal combater o *geoblocking*[8] – ou bloqueio geográfico – e suas derivações, como o *geopricing* (diferenciação do preço

[6] Comissão Europeia, "Mystery Shopping Survey On Territorial Restrictions And Geo-Blocking In The European Digital Single Market", acesso em Março 22, 2019, p. 6, https://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=14917.

[7] Comissão Europeia, "The European Commission sheds light on territorial restrictions in the online environment".

[8] Cfr. "*The Center for Internet and Society (CIS)*", ligado à Universidade de Stanford (CA, USA), o conceito de *geoblocking* ainda prescinde de melhor definição, posto que o sentido atual aplica-se às relações de consumo sem considerar outros aspectos igualmente relevantes, como os direitos autorais, a aquisição de armas e o uso de ferramentas como TOR e VPN (Virtual Privade Network) para navegar anonimamente pelo ciberespaço sem uma geolocalização territorial específica. Cfr. Center for Internet and Society, "Law, Borders, And Speech: Geoblocking Technologies", January 18, 2018, acesso em Janeiro 20, 2019. http://cyberlaw.stanford.edu/blog/2018/01/law-borders-and-speech-geoblocking-technologies.

da oferta conforme origem do pedido de compra), além da obtenção de dados sem consentimento do cliente. Por outro lado, o efeito pretendido é o de estimular o consumidor europeu a escolher o comércio eletrônico como canal preferido de compras, para intensificar a presença das empresas europeias na nova fronteira de negócios em escala planetária.

Para o presente artigo importa examinar, nesse contexto, alguns aspectos do Regulamento (UE) 2018/302 sobre a discriminação geográfica digital, uma prática lesiva aos três domínios antes referidos pela normativa europeia, que, no Brasil, foi objetivo da atuação de autoridades estaduais e federais no Caso Decolar. Nele se verificou a oferta e a precificação diferenciadas com base na geolocalização digital dos consumidores. As supostas irregularidades ensejaram a propositura de ação civil pública, no plano judicial, e a responsabilização administrativa por violação aos interesses coletivos dos consumidores.

A UE quer derrubar muros virtuais, tarefa que se faz pela sensibilização da massa consumidora e dos meios administrativos e judiciais empregados. O esforço pretende "alargar a escolha dos clientes e o acesso a bens e serviços, tendo ao mesmo tempo em conta a liberdade dos comerciantes para organizarem a sua política comercial em conformidade com o direito da União e com o direito nacional".[9]

Assinala-se, a propósito, a vigência de amplo ordenamento legal em matérias correlatas,[10] tais como:

- Regulamento (UE) 2017/2394 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2017, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de proteção dos consumidores e que revoga o Regulamento (CE) n. 2006/2004;
- Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho, de 14 de junho de 2017, relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno;
- Regulamento (UE) 254/2014 do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativo a um programa plurianual «Consumidores» para o período 2014-2020 e que revoga a Decisão n.o 1926/2006/CE;
- Diretiva 2009/22/CE do Parlamento Europeu e do Conselho, de 23 de abril de 2009, relativa às ações inibitórias em matéria de proteção dos interesses dos consumidores (versão codificada); e
- Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de Maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Directiva 84/450/CEE do Conselho, as Directivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.° 2006/2004 (Diretiva relativa às práticas comerciais desleais).

Em termos de adaptação ao atual turbilhão tecnológico, a União Europeia concentra parte dos seus esforços integrativos na consolidação do Mercado Único Digital (MUD),[11] com a disposição de "eliminar barreiras para explorar as oportunidades on-line", segundo seu principal *slogan*, e implementar estratégicas que se ramificam em três domínios: (1) melhorar o acesso dos consumidores e das

[9] Regulamento (UE) 2018/302, Considerando n. 5.
[10] Portal EUR-Lex, Direito da União Europeia, "Bloqueio geográfico: entrada em vigor do novo regulamento", acesso em Janeiro 20, 2019, https://eur-lex.europa.eu/content/news/geo-blocking-regulation-enters-into-force.html?locale=pt.
[11] Comissão Europeia, "Mercado único digital", acesso em Janeiro 20, 2019, https://ec.europa.eu/commission/priorities/digital-single-market_pt.

empresas aos bens e serviços provenientes do *eCommerce*, (2) criar um ambiente propício ao desenvolvimento das redes e serviços digitais e (3) tornar a economia digital um motor de crescimento europeu.

A engenhosidade dos códigos de programação embarcados nos sites e aplicativos de *eCommerce* prospera ante os esforços regulatórios no mercado digital. Em qualquer parte do planeta o interesse real é arrebatar a avidez consumerista e satisfazer os interesses comerciais num ambiente extremamente competitivo, de propriedade internacional muitas vezes oculta, sem interface física e sem *compliance* nos negócios tecnológicos dominados por algoritmos aos quais foi delegada "autoridade para decidir".

Yuval Noah Harari[12] vaticina:

> Em breve a autoridade pode mudar novamente – dos humanos para os algoritmos. Assim como a autoridade divina foi legitimada por mitologias religiosas, e a autoridade humana foi justificada pela narrativa liberal, a futura revolução tecnológica poderia estabelecer a autoridade dos algoritmos de Big Data, ao mesmo tempo que solapa a simples ideia da liberdade individual.

A inteligência artificial, conceito construído a partir da ideia de simulacro das capacidades humanas, tende, inexoravelemente, a reproduzir padrões de negócios reflexivos da natureza de quem a criou, para o bem ou para o mal, como exposto por Pedro Domingos:[13] "[...] deixar os robôs aprenderem ética observando humanos pode não ser uma boa ideia. O robô pode ficar bastante confuso ao ver que as ações dos humanos com frequência violam seus princípios éticos".

2. Regras contra a discriminação digital geográfica na União Europeia

A partir da aplicabilidade do Regulamento (UE) 2018/302 e do conjunto de normas correlatas ao domínio do universo digital tem-se a expectativa de que os objetivos traçados pelos legisladores da União Europeia sejam, de fato, assimilados pelos agentes econômicos com a mesma velocidade do avanço dos negócios impulsionados pela Internet tradicional e por sua sucessora, a Internet 4.0 (ou Internet das Coisas).

As mudanças são prementes, devendo ser operadas no ambiente de *eCommerce* e nos seus portais de negócios, em especial no que diz respeito à comunicação das regras definidas pelo novo comando legal. O respeito ao consumidor de produtos e serviços do comércio eletrônico é condição para que o próprio mercado digital consiga avançar tal como planejado pelas organizações representativas da União Europeia.

O dignóstico do *eCommerce* europeu é revelado pelo Regulamento (UE) 2018/302 quando relata nos seus considerandos iniciais:[14]

> Em muitos casos, ambientes jurídicos divergentes, a insegurança jurídica envolvida, os riscos associados no que respeita à legislação aplicável à proteção dos consumidores, a legislação relativa ao ambiente ou à rotulagem, as questões tributárias e fiscais, os custos de entrega ou os requisitos linguísticos, contribuem para a relutância dos comerciantes em encetar relações comerciais com clientes de outros Estados-Membros. Noutros casos, determinados comerciantes

[12] Yuval Noah Harari, *21 lições para o século 21* (São Paulo: Companhia das Letras, edição *Kindle*).
[13] Pedro Domingos, *O algoritmo mestre* (São Paulo: Editora Novatec, 2018), 308.
[14] Regulamento (UE) 2018/302, *Considerando n. 2*.

> segmentam artificialmente o mercado interno ao longo das fronteiras internas e impedem a livre circulação de bens e serviços, restringindo os direitos dos clientes e impedindo-os de beneficiar de uma escolha mais ampla e de melhores condições. Tais práticas discriminatórias são um fator importante que contribui para o nível relativamente baixo de transações transfronteiriças na União, nomeadamente no setor do comércio eletrónico, que impede o pleno aproveitamento do potencial de crescimento do mercado interno.

Como apenas 37% dos fornecedores digitais europeus[15] permitem adquisições por compradores residentes em outro Estado-Membro, o inquérito examinou o lado oculto dessa força econômica, constatando os principais tipos de bens ou serviços bloqueados: os cinco campeões de discriminação geográfica por segmento de mercado são os portais de eletrodomésticos (86% de bloqueio); de eletrônica e hardware de computador (79%); de jogos e software de computador (73%); de roupas, calçados e acessórios (65%); e de cosméticos e produtos de cuidados de saúde (63%).

Natural imaginar, nesse contexto, a profusão de conflitos de consumo, os quais, por certo, logo ultrapassarão as esferas judiciais dos Estados-Membros para serem dirimidos pelo Tribunal de Justiça da União Europeia (TJUE). Em consulta ao site curia.europa.eu[16] não se registrava, até maio de 2019, nenhum processo relativo ao Regulamento (UE) 2018/302.

Sob o prisma da prevalência do primado do direito da União Europeia, espera-se que a discriminação seja combatida com o mesmo ímpeto empregado na luta contra as práticas reais de segregação, conforme leciona Alessandra Silveira ao tecer a trama da construção da cidadania europeia e da defesa dos direitos fundamentais:

> De qualquer forma, o TJUE parece ter encontrado na cidadania europeia o derradeiro *link* para a salvaguarda do nível de proteção mais elevado dos direitos fundamentais que lhe compete assegurar. Assim, se a cidadania europeia (e os direitos que encerra) recai no âmbito de aplicação material do direito da União, isto permite que o padrão de jusfundamentalidade europeu seja invocado autonomamente pelo cidadão europeu, sem qualquer outro nexo com o direito da União para além da própria cidadania. O raciocínio básico subjacente à jurisprudência do TJUE é o seguinte: 1) a situação de um cidadão da união que não fez uso de uma liberdade económica não pode, só por isso, ser considerada como isenta de conexão com o direito da União; 2) o estatuto do cidadão da União "tende a ser o estatuto fundamental dos nacionais dos Estados-Membros" – o que lhe permite invocar, mesmo relativamente ao Estado-Membro de que é nacional, os direitos relativos a tal estatuto; 3) se o órgão jurisdicional nacional considerar que a situação *sub judice* é abrangida pelo direito da União, via cidadania europeia, deveá examinar se estão a ser respeitados os direitos fundamentais tal como a ordem jurídica da União os assegura.[17]

[15] Comissão Europeia, "The European Commission sheds light on territorial restrictions in the online environment".

[16] A Consulta ao formulário de pesquisa de jurisprudência do site do Tribunal de Justiça da União Europeia registrou nenhum resultado para o critério escolhido de pesquisa relativa ao Regulamento (UE) 2018/302, Luxemburgo, acesso em Maio 31, 2019, http://curia.europa.eu/juris/recherche.jsf?language=pt.

[17] Alessandra Silveira, "Cidadania Europeia e Direitos Fundamentais", in *Direito da União Europeia – Elementos de Direito e Políticas da União*, coord. Alessandra Silveira; Mariana Canotilho e Pedro Madeira Froufe. (Coimbra: Edições Almedina, 2016), 48.

Enfrentando os entraves tecnológicos nas relações de consumo digitais, o Regulamento (UE) 2018/302 descreve os traços gerais do *geoblocking*, traduzidos com a finalidade de auxiliar na aplicação da norma sem a pretensão de alcançar todo o seu âmago, uma vez o ritmo das aceleradas microrrevoluções tecnológicas dificulta o alcance de um conceito definitivo. Exige-se, sobretudo, redobrada atenção para entender as transações digitais e suas tipificações regulatórias:

> O bloqueio geográfico refere-se às práticas utilizadas pelos vendedores em linha para restringir as vendas transfronteiras em linha com base na nacionalidade, na residência ou no local de estabelecimento. Essas práticas incluem a recusa de acesso a sítios Web de outros Estados-Membros e/ou situações em que os clientes estrangeiros, embora tenham acesso a um sítio Web, são impedidos de finalizar a compra ou são instados a efetuar o pagamento com um cartão de débito ou de crédito de um determinado país. A «discriminação geográfica» também ocorre nas aquisições de bens e serviços fora de linha quando, por exemplo, os consumidores, embora fisicamente presentes no local do comerciante, não podem ter acesso a um produto ou serviço ou obter condições diferentes em razão da sua nacionalidade ou residência. O regulamento estabelece disposições diretamente aplicáveis que visam prevenir estas práticas em situações específicas em que não exista qualquer justificação objetiva para um tratamento diferenciado com base na nacionalidade, no local de residência ou no local de estabelecimento.[18]

Inês Gouveia detalha os tipos de obstáculos do *eCommerce* "que impedem os consumidores de livremente adquirirem ou acederem a bens de consumo e conteúdos digitais na União Europeia",[19] fatores que, sob certa medida, conduzem à corrosão dos pilares do Mercado Único Digital a cada negativa de transação comercial *on line*, tais como:

> a) bloqueio do acesso ou da compra de bens/conteúdos a utilizadores localizados num Estado-Membro diferente do fornecedor;
>
> b) bloqueio de acesso a determinado websites (acessíveis apenas a utilizadores localizados no território do fornecedor),
>
> *c) rerouting* automático para outro website destinado ao território do utilizador em questão, na impossibilidade de entrega de bens/prestação de serviços ou na recusa de pagamentos, em função da localização do utilizador;
>
> d) limitação de acesso a conteúdos digitais subscritos noutro Estado-Membro ou a impossibilidade de acesso a conteúdos já descarregados noutro Estado-Membro, quando o utilizador em questão se desloca para um EstadoMembro diferente; e
>
> *e) geofiltering* do acesso a bens/conteúdos não limitado em função da localização mas da cobrança de preços ou condições de aquisição diferentes, em função do Estado-Membro de localização do utilizador.

O conceito de discriminação geográfica, como se observa, requer certa aptidão tecnológica para compreender as nuances do *eCommerce*. O *rerouting*, por exemplo, seria algo como entrar na Casa Branca esperando ver Barack Obama e dar de cara com

[18] Comissão Europeia, "Perguntas e respostas sobre o Regulamento Bloqueio Geográfico no contexto do comércio eletrônico", acesso em Maio 31, 2019, https://ec.europa.eu/digital-single-market/en/news/geo-blocking-regulation-questions-and-answers5.

[19] Inês Gouveia, "Geo-blocking na UE - Comissão divulga conclusões preliminares", *Revista Direito Europeu da Concorrência*, n. 24 (abril, 2016), https://www.mlgts.pt/xms/files/v1/Publicacoes/Newsletters_Boletins/2016/Newsletter_Europeu_e_Concorrencia_n.o_24_PT.pdf.

Donald Trump. Talvez, para muitos, possa não ser tão simples perceber as diferenças abissais entre ambos, todavia, confundi-los é quase impossível. Os ambientes de negócios virtuais estão repletos de sites propositalmente dúbios e insondáveis.

Em outros casos, o *rerouting* é tão escandaloso que a tela recarrega em frações de segundo numa sequência vertiginosa, sem qualquer aviso e nenhuma chance de o usuário interromper o tráfego de pacotes de dados na rede de Internet. Geralmente, o *rerouting* está associado a crimes cibernéticos com o fim de furtar dados pessoais.

Dito de outra perspectiva próxima à analogia anterior, o *rerouting* também equivaleria a estar *cochichando* segredos a Trump sem perceber que *sussurrou* ao pé-do-ouvido de Vladimir Putin, mas, na verdade, o ouviente era Kim Jong-Un. Ou seja, não se sabe ao certo com quem se está a tratar ou a contratar.

Ao aprofundar os estudos sobre o *geoblocking*, Carla de Almeida Freitas insere no contexto, com pertinência, o histórico "caminho de igualdade entre todos os cidadãos e residentes na União Europeia",[20] preconizado pelos princípios da não discriminação e da livre circulação de mercadorias e serviços, insculpidos no TFUE.

De acordo com o artigo 18.º do TFUE, é proibida toda e qualquer discriminação em razão da nacionalidade, preceito que se aplica aos países abrangidos pelos Tratados da UE. O art. 26.º propugna enfaticamente que o mercado interno compreende um espaço sem fronteiras internas, no qual a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais é assegurada de acordo com as disposições dos Tratados.

Ora, no atual mercado digital europeu não se pode afiançar que a livre circulação de mercadorias e serviços esteja a ser observada com rigor pelos agentes econômicos. Tal circunstância desafia, assim, a densificação do direito de não ser discriminado fundada em fartíssima jurisprudência do TJUE. "A proibição de discriminação é [...] imperativa e explícita e não necessita, para a sua aplicação, de qualquer intervenção posterior dos Estados-Membros ou das instituições comunitárias", pelo que cria um efeito direto para os particulares", escreve Carla Freitas,[21] complementando:

> Contudo, e apesar do reconhecimento pelo TJUE do efeito direto vertical e horizontal destas normas, o recurso às mesmas não seria a solução permanente para a resolução do bloqueio geográfico, pela delonga e pelos custos que implicariam para o pequeno consumidor. Da mesma forma, as regras da concorrência controlam residualmente o *geoblocking*, mas não foram criadas expressamente para esse fim, nem os EM têm interesse em reforçá-las.
>
> Todavia, é inquestionável que o rumo da UE vai no sentido da eliminação do bloqueio geográfico através da adoção do Regulamento (UE) 2018/302, muito embora tenha no seu prefácio reconhecido que este só se destina a questões discriminatórias injustificadas, ressalvando, portanto, que há e continuarão a existir situações de bloqueio geográfico justificado que os EM, e os indivíduos em particular, têm interesse em manter.

Importa destacar, a propósito, que o Regulamento 2018/302 não impõe aos comerciantes, conforme enfatizado pela Comissão Europeia,[22] uma obrigação de venda nem de entrega em toda a União Europeia. A regra geral adotada como harmônica entre as partes é a do direito à informação mediante descrição clara,

[20] Carla Sofia Azevedo de Almeida Freitas, "O Bloqueio Geográfico (Geo-blocking) e outras formas de discriminação do consumidor no comércio eletrônico" (Mestrado, Faculdade de Direito da Universidade do Porto, 2018), 46-69, https://repositorio-aberto.up.pt/bitstream/10216/117862/2/304425.pdf.
[21] Freitas, "O Bloqueio Geográfico (Geo-blocking)", 67
[22] Cfr. Comissão Europeia, "Perguntas e respostas sobre o Regulamento Bloqueio Geográfico", 23.

compreensível e precisa das condições gerais de contrato, acesso e comércio digital de bens e serviços.

Dito de outra maneira, a teor do art. 4º do próprio Regulamento,[23] "os comerciantes não podem, nas suas operações digitais ou no estabelecimento real, aplicar condições gerais de acesso diferentes aos bens ou serviços, por razões relacionadas com a nacionalidade, com o local de residência ou com o local de estabelecimento do cliente".

O Regulamento 2018/302 não alcança os serviços de transporte, financeiros e audiovisuais, uma vez que há legislação setorial específica. As regras da UE em matéria de transportes já proíbem a discriminação em razão da nacionalidade ou do local de residência para o transporte por via aérea, autocarro ou barco.[24] Do mesmo modo, o consumidor conta com regras específicas quando decide contrair hipoteca ou abrir conta bancária.

Os serviços audiovisuais foram excluídos do Regulamento 2018/302. Todavia, devem ser alcançados pelo reexame da norma previsto[25] para 2020, incluindo também os serviços de transporte. O reexame decidirá se o regulamento será estendido aos serviços prestados por via eletrônica, cuja principal característica seja a oferta de acesso e a utilização de obras protegidas por direitos de autor (como a transferência em contínuo ou o descarregamento de música, livros eletrônicos, descarregamento ou videojogos em linha).

A respeito dos serviços audiovisuais, vislumbra-se previsível dificuldade no reajuste legal que possa, de fato, se harmonizar às diretrizes do Mercado Único Digital e da proteção do consumidor em todos os Estados-Membros, pois, como observa Carla Freitas,

> [...] nem todos os bens e serviços são igualmente afetados pelo bloqueio geográfico injustificado, sendo o mais sensível dos setores o dos serviços de conteúdo digital sujeitos a *copyrights* e prestados por via eletrónica. Embora a Comissão tenha deliberadamente optado por não regular este setor no Regulamento (UE) 2018/302, tem tentado, de forma mais subtil e indireta, contornar os direitos de autor através da promoção de licenças multiterritoriais e da implementação do princípio do "país de origem" aos serviços em linha de radiodifusão, o que não tem gerado consensos.[26]

Livrar-se do *geoblocking* requer vigilância redobrada dos organismos estatais responsáveis por tornar efetivas as disposições antes descritas, além do aprefeiçoamento dos canais de interação com os consumidores para acolher denúncias de práticas que se opõe aos seus legítimos interesses do Mercado Único Digital e dar efetividade ao Regulamento 2018/302.

Tem-se como exemplo complexo e de ampla repercussão o caso da disputa da Comissão Europeia contra seis estúdios norte-americanos de Hollywood e o canal Sky UK, que impediam os clientes britânicos de terem acesso *online* ou via satélite aos serviços de televisão paga fora do Reino Unido e da Irlanda.

A contenda foi encerrada com acordo,[27] celebrado em março de 2019, pelo

[23] Regulamento (UE) 2018/302, art. 4º – Acesso a bens e serviços.
[24] Cfr. Comissão Europeia, "Perguntas e respostas sobre o Regulamento Bloqueio Geográfico", 13.
[25] Regulamento (UE) 2018/302, art. 9º – Cláusula de reexame.
[26] Freitas, "O Bloqueio Geográfico (Geo-blocking)", 68
[27] Comissão Europeia. "Antitrust: Commission accepts commitments by Disney, NBCUniversal, Sony Pictures, Warner Bros. and Sky on cross-border pay-TV services", acesso em Março 8, 2019, http://europa.eu/rapid/press-release_IP-19-1590_en.htm.

qual a Comissão Europeia assumiu os compromissos oferecidos por Disney, NBCUniversal, Sony Pictures, Warner Bros e Sky, ao abrigo das regras antitrustes da UE, relativamente a cláusulas nos contratos de licenciamento de filmes destes estúdios para a televisão por assinatura com a Sky UK.

Antes desse entendimento, o TJUE confirmara, em dezembro de 2018, a decisão da Comissão Europeia de aceitar os compromissos da Paramount (processo T-873/16 Groupe Canal+), quando foi aplicada à disputa judicial o artigo 101.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e o artigo 53.º do Acordo EEE, os quais proíbem os acordos e práticas concertadas que possam afetar o comércio e impedir ou restringir a concorrência.

O acesso *online* ou via satélite aos serviços de televisão paga é um dos muitos temas transfronteiriços de grande repercussão no atual planeta digital a ser contemplado no reexame do Regulamento 2018/302, além do objetivo de avaliar o impacto do combate ao geoblocking e suas variações no mercado europeu e no comércio eletrônico transfronteiriço. A expectativa é de alargamento do alçance da regulação contra a discriminação geográfica.

3. Processos contra *geoblocking* e *geopricing* no Brasil

As novas tecnologias de *eCommerce* continuam a alterar os hábitos de consumo, especialmente daqueles relativos aos serviços de hotelaria e transporte individual. Enquanto no passado estavamos limitado à interveniência direta de profissionais treinados por agências turísticas, no presente cenário de transações virtuais os consumidores conseguem acessar ofertas de viagens por aplicativos concorrentes.

Em instantes, tem-se a prerrogativa de contratar qualquer tipo de transporte e escolher o destino mais vantajoso, desde que o fornecedor não resolva selecionar com base na localização geográfica qual turista deseja receber nem de flutuar o preço de acordo com o perfil de gasto do potencial cliente.

Ao lado do *geoblocking*, a prática congênere do *geopricing* desponta como grave lesão ao patrimônio dos consumidores. Representa a prévia codificação de arranjo digital para alterar o preço de produtos e serviços de acordo com a localização geográfica do interessado ou por outra razão comercial sem amparo de natureza concorrencial. Em suma, o preço varia conforme a origem do freguês. Imporante distinguir, além disso, que no *geoblocking* há impedimento do exercício de compra do bem ou serviço, enquando no *geopricing* a abusividade invade o patrimônio do consumidor.

Fatos característicos dessas duas práticas foram detectados no Brasil por ocasião dos Jogos Olímpicos de 2016, no Rio de Janeiro, naquilo que ficou conhecido, sem muito alarde, como Caso Decolar. A exploração do tema pelos meios de comunicação foi relativamente tímida e veio ao conhecimento público em 2018.

Em janeiro daquele ano, o Ministério Público do Rio de Janeiro (MPRJ) ajuizou uma ação civil pública para vedar as práticas de *geoblocking* e *geopricing* pela empresa Decolar.com,[28] com base em investigação instaurada a partir de representação da concorrente Booking.com,[29] cujos fatos teriam se dado no primeiro semestre de

[28] Cfr. Wikipédia, a empresa Decolar.com é a filial brasileira da empresa argentina Despegar.com, maior agência de viagens da América Latina, a qual é controlada pelo fundo de investimento *Tiger Global Management*, de Nova York (EUA), e conta com mais de 4 mil profissionais, com faturamento de aproximadamente US$ 4 bilhões anuais, acesso em Janeiro 15, 2019, https://pt.wikipedia.org/wiki/Decolar.com.

[29] Cfr. Wikipédia, a empresa Booking.com é um site agregador de tarifas de viagem e mecanismo

2016, antes, portanto, das disputas olímpicas na capital carioca, conforme descrito nos autos.

> Aproveitando-se de sua experiência no comércio eletrônico e com o processo de grande quantidade de dados através de processamento eletrônico ('BigData'), a BOOKING.COM identificou que a empresa DECOLAR.COM estava discriminando os consumidores brasileiros através do bloqueio de ofertas em determinados hotéis e da cobrança de preços superiores em hotéis que estavam disponíveis. Diante da identificação de que a empresa DECOLAR.COM estava privilegiando consumidores estrangeiros em detrimento dos consumidores brasileiros, a BOOKING.COM produziu provas contundentes da discriminação por origem geográfica para preços e ofertas ao consumidor, efetuando operações comerciais simultâneas no Brasil e na Argentina no dia 4 de maio de 2016 para a locação de acomodações idênticas. Tais operações foram feitas simultaneamente no Rio de Janeiro e em Buenos Aires por tabeliães de cartórios de notas, a pedido dos advogados da DANNEMANN SIEMSEN ADVOGADOS, sendo certo que os oficiais notariais realizaram tais operações ao mesmo tempo, enquanto mantinham contato telefônico para alinhar suas buscas por hospedagem em horário idêntico. O resultado das operações simultâneas foi uma evidente e manifesta discriminação do consumidor brasileiro diante do consumidor argentino, sendo certo que muitas ofertas foram bloqueadas para brasileiros e liberadas para argentinos. Além disso, quando eram feitas ofertas tanto para brasileiros quanto para argentinos, os preços cobrados aos consumidores brasileiros eram significativamente superiores aos preços ofertados aos argentinos para hotéis e períodos de hospedagem rigorosamente idênticos. Foram caracterizadas de maneira evidente as práticas de bloqueio discriminatório de oferta com base na origem geográfica do consumidor ('*GeoBlocking*') e de preço discriminatório de serviços de hospedagem com base na origem geográfica do consumidor ('*GeoPricing*') por parte da DECOLAR.COM.[30]

Nessa descrição dos fatos a partir de inquérito civil do MPRJ, a empresa argentina teria ajustado seu portal de *eCommerce* para evitar a compra de serviços de hospedagem por consumidores geograficamente localizados no Brasil, de modo a comercializer reservas em hoteis e outros serviços turísticos com a aplicação de tarifas até 30% superiores em relação às tarifas informadas nas consultas feitas a partir da Argentina.

Também foi constatada, na ocasião, a prática do *geoblocking* com base em pesquisas de reservas de hotéis na plataforma Decolar.com que apareciam indisponíveis para consultas a partir do Brasil e retornavam disponíveis quando efetuadas no mesmo momento na Argentina, conforme autos do respectivo processo judicial.

A aversão algorítmica da plataforma aos consumidores localizados no Brasil teria sido confirmada pela investigação do MPRJ também em São Paulo e em Belo Horizonte, capitais de Estados brasileiros próximos à sede carioca dos Jogos Olímpicos. Na ação civil foi informado que o *geoblocking* e o *geopricing* seriam práticas corriqueiras nesse segmento:

---

de metabusca de viagens para reservas de hospedagem, sediada em Amsterdã, sendo que pertence e é operada por *Reservations Holdings*, nos Estados Unidos, acesso em Janeiro 15, 2019, https://en.wikipedia.org/wiki/Booking.com.

[30] Site Consumidor Vencedor RJ, Ação Civil Pública n. 0018051-27.2018.8.19.0001, acesso em Janeiro 20, 2019, https://rj.consumidorvencedor.mp.br/documents/13137/332720/acp.pdf.

> Em audiência administrativa de 29 de março de 2017, a BOOKING.COM reafirmou que seu interesse principal é regular o mercado de reservas online brasileiro, combatendo práticas discriminatórias anticompetitivas, salientando que seus demais concorrentes também praticam 'GeoPricing' e se comprometendo a apresentar evidências a respeito de Expedia, Submarino, Hotel Urbano e Hoteis.com – o que levou a instauração de procedimentos específicos com relação às demais empresas, ainda sem conclusão das demais investigações.[31]

O MPRJ sustentou a jurisprudência do Supremo Tribunal Federal (STF), segundo a qual

> a autonomia privada, que encontra claras limitações de ordem jurídica, não pode ser exercida em detrimento ou com desrespeito aos direitos e garantias de terceiros, especialmente aqueles positivados em sede constitucional, pois a autonomia da vontade não confere aos particulares, no domínio de sua incidência e atuação, o poder de transgredir ou de ignorar as restrições postas e definidas pela própria Constituição, cuja eficácia e força normativa também se impõem, aos particulares, no âmbito de suas relações privadas, em tema de liberdades fundamentais.[32]

A não discriminação constitui direito básico do consumidor consagrado no artigo 6º, II do Código brasileiro de Defesa do Consumidor (CDC),[33] que lhe assegura a liberdade de escolha e igualdade nas contratações. Sob essa previsão legal, o MPRJ identificou a "ocorrência de diversas práticas abusivas levadas a cabo pela DECOLAR.COM", tendo em vista que "o *geoblocking* nada mais é do que a recusa injustificada à prestação do serviço, vedada pelo artigo 39, II e IX, CDC".[34]

Diz o art. 39 do CDC, que é vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: [...] II – recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes; [...] e IX – recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais.

A prática de *geopricing* restou caracterizada na precificação discriminatória também com base no critério da origem geográfica, o que acarretou, segundo o MPRJ, na ocorrência das práticas abusivas previstas no artigo 39, V e X, CDC, segundo os quais, respectivamente, é vedado ao fornecedor exigir do consumidor vantagem manifestamente excessiva e elevar sem justa causa o preço de produtos ou serviços.

Outro aspecto apurado nos autos[35] evidenciou a publicidade contrária ao disposto no artigo 37, §1º do CDC – é enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço

[31] Portal Consumidor Vencedor RJ, Ação Civil Pública n. 0018051-27.2018.8.19.0001, p. 17.
[32] Supremo Tribunal Federal, Recurso Extraordinário RE 201819/RJ, rel. Min. ELLEN GRACIE, rel. p/acórdão Min. GILMAR MENDES, j. 11/10/2005, 2ª T., DJ 27/10/2006, p. 64.
[33] Lei n. 8.078, de 11 de setembro de 1990, Código de Defesa do Consumidor, acesso em Janeiro 21, 2019, http://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm.
[34] Portal Consumidor Vencedor RJ, Ação Civil Pública n. 0018051-27.2018.8.19.0001, p. 18.
[35] Supremo Tribunal Federal, Recurso Extraordinário RE 201819/RJ, rel. Min. ELLEN GRACIE, rel. p/acórdão Min. GILMAR MENDES, j. 11/10/2005, 2ª T., DJ 27/10/2006, p. 64.

e quaisquer outros dados sobre produtos e serviços. Além disso, a empresa teria violado o Marco Civil da Internet (Lei n. 12.965/2014),[36] que assegura ao usuário o direito de acesso à Internet como essencial ao exercício da cidadania.

No plano legislativo, a norma brasileira protege o consumidor contra o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de Internet, exceto se comprovado consentimento livre, expresso e informado nas hipóteses previstas. Os dados pessoais do consumidor podem ser utilizados para finalidades que justifiquem sua coleta e não sejam vedadas pela legislação, além de previstas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet.

O MPRJ entendeu que a empresa Decolar infringiu a ordem econômica brasileira ao discriminar adquirentes ou fornecedores de bens ou serviços por meio da fixação diferenciada de preços, ou de condições operacionais de venda ou prestação de serviço. Em razão dessas violações ao ordenamento legal, requereu o fim das práticas de *geoblocking* ou de *geopricing*, sob pena de multa diária de R$ 10 mil reais, e indenização por danos materiais e morais coletivos de R$ 57 milhões de reais.

O pedido do MPRJ foi indeferido na primeira e segunda instâncias do Poder Judiciário do Rio de Janeiro, além de decretado tramitação em segredo de Justiça. Recorda-se, a propósito, que a petição inicial foi uma ação civil pública. Antes do recesso forense no final de 2018, o Judiciário carioca indeferiu os recursos interpostos pelo órgão ministerial e considerou as provas técnicas insuficientes:

> Agravo de Instrumento. Decisão que indeferiu tutela provisória. Art. 300 do CPC. O deferimento da tutela de urgência demanda a presença da probabilidade do direito e o perigo de dano, assim como risco ao resultado útil do processo. Frágil conjunto probatório carreado aos autos não é demonstrativo dos requisitos para o deferimento da medida liminar pretendida. Decisão do juízo a quo que se mantém. Recurso conhecido e desprovido.[37]

Na sequência do processo judicial, a pretensão do MPRJ também foi negada pelos seguintes fundamentos:

> Agravo interno. Decisão que indeferiu efeito suspensivo ativo em agravo interposto contra decisão que indeferiu liminar pelo juízo de 1º grau. Ausência de demonstração de prática de abusivas de "Geo-Blocking" (bloqueio da oferta com base na origem geográfica do consumidor e de "GeoPricing" (precificação diferenciada da oferta com base na origem geográfica do consumidor). Disputa mercadológica e atuação do MP orientada por concorrente. Ausentes os requisitos indispensáveis para concessão da liminar. Indeferido efeito suspensivo ativo. Decisão que se mantém. Recurso conhecido e desprovido.[38]

Diferente do resultado preliminar do caso no Judiciário carioca, as práticas atribuídas à empresa foram objeto de processo administrativo[39] instaurado pelo Departamento de Proteção e Defesa do Consumidor (DPDC), que atua como esteio

[36] Lei Federal n. 12.965, de 23 de abril de 2014, Marco Civil da Internet brasileira, acesso em Janeiro 21, 2019, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.
[37] Tribunal de Justiça do Rio de Janeiro, Agravo de Instrumento n. 0008914-24.2018.8.19.0000. Processo Originário n. 0018051-27.2018.8.19.0001, acesso em Janeiro 23, 2019, http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=000406C2CABE150B1E5E887CF20609CD30D0C5093840500D&USER=.
[38] Tribunal de Justiça do Rio de Janeiro, Agravo de Instrumento n. 0008914-24.2018.8.19.0000.
[39] Ministério da Justiça, Departamento de Proteção e Defesa do Consumidor. "Decolar.com é multada por prática de geo pricing e geo blocking", acesso em Janeiro 25, 2019, https://www.justica.gov.br/news/collective-nitf-content-51.

da Secretaria Nacional do Consumidor do Ministério da Justiça do Brasil e teve a sua estrutura alterada pelo Decreto Federal n. 9.662/2019.[40]

Em junho de 2018, o DPDC multou a Decolar em R$ 7,5 milhões por diferenciação de preço de acomodações e negativa de oferta de vagas, quando existentes, de acordo com a localização geográfica do consumidor. Para o órgão de defesa do consumidor, ficou caracterizada a prática de *geopricing* pela empresa:

> ao precificar – ou permitir que se precifique – o serviço de acomodação de acordo com a localização geográfica do usuário, a Decolar se conduz de forma a extrapolar o direito de precificar (ou permitir que serviço por ele anunciado seja precificado) de acordo com as práticas do mercado". Além disso, "com efeito, não se justifica nem é prática usual o estabelecimento de preços diferentes de serviços que são prestados no mesmo local e nas mesmas condições a qualquer consumidor que esteja disposto a pagar por esses serviços".[41]

A Decolar.com foi responsabilizada por ter excedido os limites legais ao instituir prática contrária à ordem econômica e ao mercado de consumo, tendo corrompido o

> seu direito de praticar o comércio e de ofertar o produto, prejudicando o consumidor brasileiro, ao não mostrar serviço que não queira vender a determinado consumidor (no caso, o consumidor brasileiro). Isso porque o favorecimento (ou desfavorecimento), bem como a discriminação por conta de etnia, localização geográfica ou qualquer outra característica extrínseca ao ato comercial causa desequilíbrio no mercado e nas relações de consumo.[42]

Em sua defesa, a empresa sustentou não praticar *geoblocking* nem *geopricing* em seu modelo de negócios, tendo sempre operado "com transparência, honestidade, integridade, respeito aos seus clientes, e, principalmente, em conformidade com as leis, normas e regulamentos aplicáveis em todos os países em que atua".[43]

Para descontruir as alegações do MPRJ e do DPDC, a Decolar.com alegou operar como intermediadora entre fornecedores e consumidores "em cada país por meio de um site local", assim, não teria como comandar a referida discriminação digital. Rebateu, ainda, informando seguir as legislações, os regulamentos e as precificações que lhes são próprios no Brasil e na Argentina, razões pelas quais continuará a contestar os processos nas suas respectivas esferas.

4. Conclusões

A harmonização das práticas do mercado digital aos preceitos protetivos do consumidor enfrenta, relativamente ao *geoblocking*, ao *geoprincing* e às discriminações correlatas, o desafio de identificar e obter o conjunto probatório das práticas ilícitas em ambiente virtual, por autoridades competentes de países distintos, para possibilitar

[40] Decreto Federal n. 9.662, de 1º de janeiro de 2019, aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública, acesso em Janeiro 23, 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9662.htm#art11.

[41] Ministério da Justiça, Departamento de Proteção e Defesa do Consumidor. "Nota Técnica n. 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ", acesso em Janeiro 25, 2019, http://www.mpsp.mp.br/portal/page/portal/cao_consumidor/SENACON/SENACON_NOTA_TECNICA/SENACON%20DECIS%C3%83O%20geo%20pricing%20e%20geo%20blocking%20multa.pdf.

[42] Ministério da Justiça, Departamento de Proteção e Defesa do Consumidor. Nota Técnica n.º 92/2018.

[43] Núcleo de Informação e Coordenação do Ponto BR – NIC.br. "Como Decolar.com e outras empresas mudam seus preços de acordo com seus dados", acesso em Junho 30, 2019, https://nic.br/noticia/na-midia/como-decolar-com-e-outras-empresas-mudam-precos-de-acordo-com-seus-dados/.

ao juízo competente a aplicação do princípio da verdade real aos casos concretos.

É perceptível a dificuldade de se comprovar a prática discriminatória. Requer-se, ademais, esgrimir a fundamentação jurídica por meio de diferentes normas como no caso brasileiro, de modo a alcançar a mais ampla dimensão da tutela consumerista.

Nessa breve exposição dos aspectos gerais do Regulamento (UE) 2018/302 da União Europeia e do Caso Decolar no Brasil fica evidente que os códigos ardilosos inseridos nas plataformas de *eCommerce* estão presentes em diferentes mercados digitais. A estratégia empresarial preponderante parece ser a de não assumir o compromisso de transparência a quem não se deseja vender fora da área de cobertura da empresa.

Além disso, parte dos agentes econômicos altera deliberadamente o preço da oferta conforme o potencial de gastos do consumidor de determinada região, demonstrando violação ainda mais grave aos preceitos basilares da concorrência e da proteção ao livre mercado. Trata-se de pura abusividade.

O espaço sem fronteiras físicas e digitais propugnado pela União Europeia tem, no Regulamento (UE) 2018/302, um dispositivo suscetível de se transformar em norma influenciadora do direito internacional, com efeitos na formação do ordenamento de outros países.

Embora sem atuação direta em solo europeu, muitas praticantes do bloqueio geográfico e da precificação manipulável têm negócios conjuntos com agentes parceiros sediados em Estados-Membros da União Europeia. É de se imaginar que o Regulamento (UE) 2018/302 também tenha eficácia na depuração dessas relações de consumo.

Os fatos e decisões administrativas e judiciais trazidos à análise em relação ao caso brasileiro demonstram que o esforço da União Europeia na persecução dos seus principais objetivos da construção do Mercado Único Digital deveria ser estendido à regulação do comércio digital de empresas atuantes em outros continentes.

As autoridades europeias têm como exigir dos agentes econômicos locais o compromisso dos parceiros externos destes a se submeterem ao Regulamento (UE) 2018/302, do contrário se estará tolerando a continuidade da violação transfronteiriça de direitos fundamentais, tal qual o ativista internacional que defende a Floresta Amazônica sentado numa confortável poltrona feita de Castanheira, uma das árvores ameaçadas de extinção da flora brasileira.

Muito há por ser investigado pelas autoridades na defesa do consumidor, para coibir o uso de códigos maliciosos engenhosamente embutidos nas aplicações de *eCommerce*. A vulnerabilidade é latente, mas de difícil comprovação nas esferas administrativo e judicial.

Quer sejam adquirentes ou não de produtos e serviços, os consumidores estão atualmente à mercê dos algoritmos lícitos e ilícitos. Portanto, se o objetivo do Regulamento (UE) 2018/302 é combater a discriminação direta e indireta com base na nacionalidade, no local de residência ou no local de estabelecimento dos clientes, incluindo o bloqueio geográfico injustificado, urge estabelecer estratégias transnacionais com a finalidade de elidir a abusividade nas relações de consumo no mercado digital planetário.

A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados

Tiago Branco da Costa*

RESUMO: O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Nesse contexto, são reconhecidos, aos titulares dos dados pessoais, o direito à ação judicial e o direito a receber uma indemnização, quando considerarem ter havido uma violação dos direitos que lhes assistem, na sequência de um tratamento destes dados à revelia do disposto no Regulamento. O preenchimento dos requisitos legais de que depende o instituto jurídico da responsabilidade civil afigura-se complexo, com particular destaque para a quantificação dos danos. Sendo certo que esta complexidade se agudiza com a necessidade de articulação entre o direito interno de cada Estado-Membro e o Direito da União Europeia, tendo em conta o sentido e o alcance de cada um desses requisitos à luz da autonomia processual dos Estados-Membros e dos princípios-teste da equivalência e da efetividade. Com efeito, o apuramento e a quantificação dos danos resultantes de um tratamento de dados realizado ao arrepio do regime legal emanado pelo RGPD traz à colação o debate em torno da resposta aos desafios do mercado único digital.

PALAVRAS-CHAVE: Interoperabilidade – Mercado Único Digital – Responsabilidade Civil – RGPD

ABSTRACT: The Regulation (EU)2016/679 of the European Parliament and of the Council of 27th April 2016 lays down rules on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In that context, the holders of personal data are granted the right to a legal action and the right to compensation if they consider that there has been a breach of their rights following the processing of such data in breach of Regulation. The fulfillment of the legal requirements that the civil liability legal institute depends appears complex, with particular emphasis on the quantification of damages. It is true that this complexity is exacerbated by the need to establish a link between the internal law of each Member State and European Union law, having regard to the meaning and scope of each of those requirements under Member States procedural autonomy and the principles of equivalence and effectiveness. The establishment and quantification of the damage resulting from data processing carried out in violation of the legal regime established by the GDPR brings to the fore the discussion on the challenges of the digital single market.

KEYWORDS: Interoperability – Digital Single Market – Civil Responsability – GDPR

* Advogado, Mestrando em Direito dos Contratos e da Empresa e Investigador do Centro de Investigação em Justiça e Governação (JusGov) da Escola de Direito da Universidade do Minho.

1. O instituto jurídico da responsabilidade civil no âmbito do Regulamento Geral sobre a Proteção de Dados

O Regulamento Geral sobre a Proteção de Dados (doravante designado apenas por RGPD) atribui a todos os titulares de dados o direito de recorrer à via judicial quando (i) estes considerem ter havido uma violação dos direitos que lhes assistem nos termos do regulamento e (ii) essa violação resulte de um tratamento dos seus dados pessoais efetuado em violação do regulamento.[1] Este meio de tutela dos direitos dos titulares de dados pessoais não contende com o recurso a outros meios legalmente previstos.[2]

Ademais, estabelece-se, no artigo 82.º do RGPD,[3] que qualquer pessoa que tenha sofrido danos, materiais ou imateriais, devido a uma violação do regulamento, tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratado pelos danos sofridos.

Note-se que a responsabilidade do responsável pelo tratamento se verifica quando este esteja envolvido no tratamento de dados, ao passo que a responsabilidade do subcontratado só tem lugar nos casos em que este não cumpra as obrigações decorrentes do regulamento[4] ou se não tiver seguido as instruções lícitas fornecidas pelo responsável pelo tratamento.

Por outro lado, sempre que estejam envolvidos mais do que um responsável pelo tratamento ou subcontratado civilmente responsáveis nos termos do regulamento, é válida a regra da solidariedade, de acordo com a qual ambos poderão responder pela totalidade dos danos (sem prejuízo do direito de regresso que exista entre os responsáveis civis).

Não obstante, o direito a receber uma indemnização, que pretendemos tratar, já tinha sido reconhecido ao titular dos dados, no âmbito da Diretiva 95/46/CE (concretamente no artigo 23.º), embora com contornos diversos, no âmbito do RGPD, o direito de indemnização é concedido a "qualquer pessoa que tenha sofrido danos",[5] ao passo que o direito à ação judicial é atribuído a "todos os titulares de dados". Estas diferenças literais levantam outras questões jurídicas ao nível da legitimidade ativa, no âmbito da ação judicial para tutela dos direitos do titular dos dados.

Por conseguinte, resultam, em abstrato, três interpretações distintas: o artigo 82.º pode ser invocado (i) por todas as pessoas coletivas e singulares; (ii) apenas por pessoas singulares; ou (iii) somente pelos titulares de dados visados.[6]

Se atentarmos ao conteúdo do Considerando 146, podemos verificar que o legislador se referiu apenas aos titulares dos dados.

---

[1] Cfr. artigo 79.º e Considerandos 145 e 147, todos do RGPD.

[2] Conforme resulta do corpo da norma, "sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar relação a uma autoridade de controlo". No mesmo sentido, vd. Alexandre Sousa Pinheiro et. al., *Comentário ao Regulamento Geral de Proteção de Dados* (Coimbra, Almedina, 2018), 629, "o direito de ação, judicial […] não preclude o recurso às vias administrativas, *maxime* a reclamação perante uma autoridade de controlo […], nem é prejudicado pelo facto de estas terem sido utilizadas".

[3] Cfr. Considerando 146 do RGPD.

[4] Deve-se entender as obrigações do RGPD que lhe são especificamente dirigidas, nos termos do artigo 28.º.

[5] Cfr. artigo 82.º do RGPD.

[6] Cfr. A. Barreto Menezes Cordeiro, "Da responsabilidade civil pelo tratamento de dados pessoais", *Blook,* acesso Dezembro 2018, https://blook.pt/publications/publication/2ae6399f13bb/, 9-11.

Por outro lado, o próprio preceito legal que atribui o direito à indemnização aos titulares de dados restringe as ações de responsabilidade civil a danos causados em virtude de um tratamento de dados pessoais, o que acentua a ligação intrínseca entre os danos causados e o titular dos dados. Sendo certo, para além disso, que se faz referência não só a danos patrimoniais como a danos morais, o que parece circunscrever uma vez mais a titularidade (pelo menos) às pessoas singulares.

Neste sentido, entendemos que a legitimidade ativa no âmbito do exercício do direito à ação judicial e do direito à indemnização encontra-se, por regra, atribuída ao titular dos dados, já que estes direitos foram instituídos com o propósito de tutelar os seus direitos.

Do ponto de vista da legitimidade passiva podem figurar na ação judicial o responsável pelo tratamento de dados ou o subcontratado, mas já não o encarregado da proteção de dados.[7]

Ora, o regime da solidariedade que resulta dos termos do RGPD, traduz, no âmbito das obrigações, uma inversão da regra da parciaridade ou conjunção,[8] presente no Código Civil português, no campo da qual cada devedor responde pelas suas obrigações. Só assim não se verifica quando, por força da lei ou da vontade das partes, se institua a solidariedade.[9]

Como é consabido, a solidariedade passiva – perspetiva dos devedores solidários, no âmbito da teoria geral do direito das obrigações, tem como efeito, no domínio das relações externas (isto é, na relação entre os devedores solidários e o credor) a possibilidade de o credor exigir, judicial ou extrajudicialmente, a prestação integral ou parcial de cada um dos devedores solidários.[10]

Por sua vez, no domínio das relações internas (ou seja, na relação entre os devedores solidários), os efeitos da solidariedade concretizam-se no direito de regresso, de acordo com o qual o devedor que satisfizer o direito do credor além da parte que lhe competia tem direito de regresso contra cada um dos codevedores, na parte que as estes competem.

Posto isto, cabe analisar de que forma o direito interno será acionado para ser empregue no âmbito de aplicação do RGPD que nos ocupa.

---

[7] Com efeito, o encarregado da proteção de dados, pode exercer a sua profissão enquanto elemento do pessoal da entidade responsável pelo tratamento ou do subcontratado, tal como pode fazê-lo com base num contrato de prestação de serviços, mas em qualquer um dos casos com base numa relação jurídica estabelecida com o responsável pelo tratamento ou com o subcontratado. Em sentido diverso, vd. Mafalda Miranda Barbosa, "Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil", *Revista de Direito Comercial*, vol., nº 2 (março de 2018): 477, "o encarregado da proteção de dados poderá ser responsabilizado em face do titular dos dados, por violação dos deveres que lhe são impostos no quadro regulamentar".

[8] Cfr. José Carlos Brandão Proença, *Lições de Cumprimento e Não Cumprimento das Obrigações* (Coimbra: Coimbra Editora, 2011), 105.

[9] Cfr. artigo 513.º do Código Civil. Neste sentido, vd. Nuno Manuel Pinto Oliveira, *Princípios de Direito dos Contratos* (Coimbra: Coimbra Editora, 2011), 72, "[e]m regra – se a lei ou o negócio jurídico nada disserem – a obrigações é parciária; excecionalmente – se a lei ou o negócio jurídico o disserem – a obrigação plural é solidária."

[10] Cfr. Oliveira, *Princípios de Direito*, 70 e segs.; e ainda Proença, *Lições de Cumprimento*, 109. Visto que o estudo em causa deslinda-se pela análise da responsabilidade civil aplicada em caso de violação dos princípios constantes no RGPD, faz-se necessário ressaltar que a posição tradicional do credor, no âmbito direito civil, é aqui compreendida como sendo o titular do direito violado, ao passo que a posição do devedor, corresponde ao responsável pelo tratamento ou subcontratado civilmente responsáveis nos termos do regulamento, que têm ao seu encargo a incumbência de zelar pela proteção e não disponibilização dos dados em causa.

2. Pressupostos da responsabilidade civil

O artigo 19.º n.º 1, 2.º parágrafo do Tratado da União Europeia institui o princípio da autonomia processual dos Estados-Membros, cabendo-lhes "a obrigação de criarem as vias recursórias tendentes à tutela dos direitos conferidos pela ordem jurídica da União",[11] em respeito pelos princípios da equivalência e da efetividade, que teremos oportunidade de retratar de seguida.

Neste sentido, a fim de acautelar a tutela jurisdicional efetiva, devem os Estados-Membros gozar da autonomia processual necessária à regulação, no ordenamento jurídico interno, das soluções jurídico-processuais e organizativo-processuais inerentes à efetivação dos direitos e liberdades dos cidadãos reconhecidos pelo direito da União, sem, contudo, estabelecer um sistema processual interno que se repute menos favorável à tramitação de litígios fundados em direito da União quando comparados com litígios puramente internos (teste da equivalência), nem que torne excessivamente difícil ou impossível, na prática, o exercício de tais direitos (teste da efetividade).[12]

Por esta razão, ao enveredarmos pelo estudo do instituto da responsabilidade civil decorrente do RGPD, não podemos deixar de considerar, por um lado, o regime legal constante do Código Civil português na medida em que, por força da autonomia processual dos Estados-Membros, este será o regime mobilizável, no ordenamento jurídico português, que permitirá a efetivação das soluções decorrentes do RGPD.

Por sua vez, também nos cabe ter em consideração os arestos do TJUE, bem como os desenvolvimentos do direito da União, no que a esta matéria diz respeito.

Isto dito, de acordo com a redação constante no artigo 493.º do Código Civil, relativo aos pressupostos inerentes à responsabilidade extracontratual, aquele que, com dolo ou mera culpa, violar, ilicitamente, o direito de outrem ou qualquer outra disposição legal destinada a proteger interesses alheiros, fica obrigado a indemnizar o lesado pelos danos resultantes da violação.

Por sua vez, o artigo 798.º, que se ocupa da responsabilidade civil contratual, prevê, neste regime, que quem faltar culposamente ao cumprimento da obrigação se torna responsável pelo prejuízo que causar ao titular dos dados.

Resulta, assim, necessário o preenchimento dos pressupostos da responsabilidade civil: prática de um facto voluntário, ilicitude, culpa, dano e nexo de causalidade (entre o facto e o dano).[13]

Todavia, no âmbito da responsabilidade civil contratual, o titular do direito violado goza, no que diz respeito ao ónus da prova, de uma presunção de culpa, incumbindo ao agente perpetrador da violação provar que a falta de cumprimento ou o cumprimento defeituoso da obrigação não decorre de culpa que lhe seja imputável.

Porém, no âmbito do RGPD também é possível configurar uma relação jurídica na qual possa verificar-se simultaneamente a responsabilidade civil extracontratual (violação de dados pessoais sem haver relação contratual entre o responsável pelo tratamento e o titular dos dados) do responsável pelo tratamento, bem como a sua responsabilidade civil contratual (lesão de um direito relativo).

No entanto, o concurso de responsabilidades que se venha a verificar neste domínio surge algo facilitada, na medida em que o RGPD não distingue os regimes

[11] Joana Covelo de Abreu, *Tribunais Nacionais e Tutela Jurisdicional Efetiva: da Cooperação à Integração Judiciária no Contencioso da União Europeia* (Coimbra: Almedina, 2019), 11.
[12] Cfr. Alessandra Silveira, *Princípios de Direito da União Europeia* (Lisboa: Quid Juris, 2011), 119-120.
[13] Cfr. Barbosa, *Data controllers,* 440; e Pinheiro et. al., *Comentário ao Regulamento*, 636.

de responsabilidade, antes atribuindo sempre o ónus da prova ao responsável pelo tratamento ou subcontratado.

O titular dos dados beneficia de uma inversão do ónus da prova, favorável aos interesses do lesado, a quem basta demonstrar que os prejuízos sofridos foram causados por uma operação de tratamento da responsabilidade do responsável pelo tratamento ou do subcontratado, cabendo, por sua vez, a este(s) demonstrar que não é(são) responsável(is) pelo evento gerador dos dados, ou seja, que não agiu(ram) com culpa, pelo que o facto não lhe(s) pode ser imputado.[14]

Deste modo, ao responsável pelo tratamento ou ao subcontratado é atribuído um ónus da prova do facto negativo, que é o da sua irresponsabilidade em relação ao evento causador dos danos.

Em termos processuais, este ónus da prova do facto negativo pode consubstanciar uma dificuldade acrescida para a esfera jurídica do responsável pelo tratamento ou do subcontratado. Com efeito, este ónus é, em regra, mais oneroso do que um ónus da prova do facto positivo, sendo certo que, em alguns casos, podemos estar perante uma prova verdadeiramente impossível ou uma prova de factos negativos indeterminados ou indefinidos, como é o caso de uma eventual factualidade negativa subjacente à inexistência de uma ligação entre a conduta lesiva e a atuação do responsável pelo tratamento de dados ou subcontratado.

A título de exemplo, podemos equacionar um tratamento de dados ilícito levado a cabo por um terceiro que, de forma ilegítima, acede aos dados de um titular que se encontram na posse do responsável pelo tratamento.

Nesta situação, para que o responsável pelo tratamento possa afastar a sua responsabilidade, tornar-se-á necessária a mencionada prova do facto negativo, isto é, a prova de que o dano provocado na esfera jurídica do titular dos dados não foi por si causado. O que será possível se este sujeito demonstrar que, para além de ter cumprido com todos os seus deveres, não lhe era exigível outra conduta do que aquela que encetou. Por exemplo, o responsável pelo tratamento de dados deve demonstrar, neste caso, quais os procedimentos de segurança de que dispunha e que, tendo em conta as técnicas e os meios disponíveis, bem como os respetivos custos de aplicação, a natureza, o âmbito, o contexto, as finalidades do tratamento e, ainda, os riscos, de probabilidade e gravidade variável, para os direitos e liberdades do titular dos dados, não lhe era exigível outro comportamento.

Porém, este argumento não foi suficiente para justificar uma distribuição diversa do ónus da prova, tendo o legislador optado por onerar o responsável pelo tratamento, em prol da proteção dos direitos dos titulares de dados pessoais.

2.1. Prática de um ato voluntário

O primeiro dos pressupostos da responsabilidade civil é o facto voluntário, ou seja, a prática de um ato positivo. No entanto, a doutrina[15] e a jurisprudência[16] admitem reiteradamente que, embora se aponte, em regra geral, uma ação, este facto pode também tratar-se de um facto negativo, isto é, de uma abstenção ou de uma

[14] Cfr. Pinheiro et. al., *Comentário ao Regulamento*, 636.

[15] Entre outros, vd. Oliveira, *Princípios de Direito*, 617 e segs.

[16] Cfr. Acórdão do Supremo Tribunal de Justiça, de 01/07/2003, processo 03A1902, relator Azevedo Ramos; Acórdão do Supremo Tribunal Administrativo, de 22/03/2017, processo 01356/14, relatora Teresa de Sousa; Acórdão do Tribunal da Relação de Coimbra, de 04/11/2003, processo 2569/03, relator Jaime Ferreira, todos disponíveis em http://www.dgsi.pt/.

omissão.

No âmbito da proteção de dados pessoais e do regime constante do RGPD, deve-se verificar a prática de um ato voluntário que se consubstancia num facto positivo (ação) ou num facto negativo (omissão), por parte do responsável pelo tratamento de dados ou do subcontratado.

2.2. Ilicitude

Conforme resulta da análise do direito ao recurso à via judicial atribuído aos titulares de dados pessoais, este direito baseia-se em dois pressupostos essenciais: (i) a existência de uma violação dos direitos dos titulares dos dados; e (ii) que a violação desses direitos resulte de um tratamento de dados pessoais efetuado ao arrepio do regulamento.

Deste modo, deve-se verificar não só uma violação aos direitos dos titulares de dados, o que resulta desde logo numa violação ao RGPD, mas é também necessário que essa violação decorra de um tratamento de dados pessoais efetuado em violação ao RGPD, ou seja que incumpra também ele os ditames dele decorrentes.

Por sua vez, o artigo 82.º do RGPD, que se refere especificamente ao direito de indemnização, alude apenas à produção de danos, materiais ou imateriais, devido a uma violação do regulamento.

Para que seja possível falar-se da ilicitude, deve-se verificar uma desconformidade em relação ao regime legal constante do RGPD, optando-se, assim, por uma interpretação extensiva do conceito de «ilicitude». Com efeito, o ato lesivo cuja prática é da responsabilidade do responsável pelo tratamento de dados ou do subcontratado pode violar qualquer um dos preceitos legais do RGPD, não se limitando, portanto, a uma ilicitude relativa aos fundamentos para o tratamento de dados.[17]

Assim sendo, quando um dos requisitos de que depende o direito à indemnização se encontre preenchido, o requisito da ilicitude encontrar-se-á preenchido igualmente, uma vez que uma violação ao direito dos titulares de dados consubstancia uma violação ao RGPD o que resulta, por conseguinte, na sua ilicitude. Do mesmo modo, um tratamento de dados violador do RGPD resulta na sua ilicitude, já que é violador do regime jurídico aplicável.

2.3. Culpa

Nos termos do n.º 3 do artigo 82.º do RGPD, o responsável pelo tratamento ou o subcontratado ficam isentos de responsabilidade se provarem que não são, de modo algum, responsáveis pelo evento que deu origem aos danos. Significa isto que se demanda que o responsável pelo tratamento de dados ou o subcontratado não tenham atuado com dolo ou negligência.[18] Estamos, portanto, perante uma causa de exclusão da culpabilidade nos casos em que o responsável pelo tratamento ou o subcontratado não tenham dado origem, dolosa ou negligentemente, à situação de violação.

A este respeito cumpre chamar à colação os princípios relativos ao tratamento de dados pessoais, *maxime* o princípio da integralidade e da confidencialidade, de acordo com o qual os dados pessoais devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando-se, para o efeito,

[17] Cf. resulta do artigo 6.º do RGPD.

[18] Vd. a respeito dos conceitos de dolo e de negligência, Oliveira, *Princípios de Direito*, 428 e segs.

as medidas técnicas ou organizativas adequadas.

Mais adiante, no âmbito do RGPD, este artigo é concretizado por outros preceitos que se debruçam sobre os deveres que recaem sobre o responsável pelo tratamento de dados ou o subcontratado, no sentido de adotarem medidas técnicas e organizativas que zelem pela segurança dos dados pessoais do titular. Todavia, o nível de segurança alcançado com estas medidas deve ser adequado ao risco,[19] considerando-se as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, os riscos de probabilidade e gravidade variável para os direitos e liberdades das pessoas singulares.

Ademais, a adoção destas medidas técnicas e organizativas deve incluir, consoante o que se afigurar adequado à situação, a pseudonimização e cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Estabelece-se, ainda, a este respeito, uma importante salvaguarda no que diz respeito à segurança da informação no seio da organização do responsável pelo tratamento de dados ou do subcontratado, exigindo-se que estes adotem medidas adequadas a assegurar que qualquer pessoa singular que, agindo sob a sua autoridade, tenha acesso a dados pessoais, só procede ao seu tratamento mediante as suas instruções.

Para que o responsável pelo tratamento de dados ou o subcontratado possam demonstrar a exclusão de culpabilidade é necessário comprovar primeiramente o cumprimento de todos os deveres que lhes são impostos por força do regulamento, no que à segurança dos dados pessoais diz respeito.

Pense-se, por exemplo, numa situação de violação de dados pessoais, o que de acordo com o disposto no n.º 12 do artigo 4.º do RGPD, se traduz numa violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Neste caso, o responsável pelo tratamento de dados ou o subcontratado podem, efetivamente, não ter contribuído, a título de dolo ou negligência, para a verificação da violação.

Todavia, para que tal se verifique é necessário assegurar previamente o cumprimento dos deveres de segurança a que estes sujeitos se encontravam adstritos. Se o responsável pelo tratamento não tiver adotado as medidas que estavam ao seu alcance e que eram adequadas ao caso, então, pelo menos, de forma negligente, o responsável pelo tratamento de dados não cumpriu os deveres a que estava vinculado, não podendo, assim, optar-se pela exclusão da culpa.

2.4. Dano

De acordo com o disposto no Considerando 146 do RGPD, o conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do TJUE, de uma

[19] Nos termos do disposto no n.º 2 do artigo 32.º do RGPD, "Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

forma que reflita plenamente os objetivos do regulamento.

Para além de não constar do RGPD qualquer definição de dano, verifica-se, nos vários sistemas jurídicos, que é complexa a quantificação dos danos e que recai sobre a competência jurisdicional dos tribunais dos Estados-Membros a resolução destes litígios, o que pode intensificar esta dificuldade.

Com efeito, pese embora não exista (ainda?) um direito privado europeu, não podia optar-se por outra solução, sob pena de se entorpecer a tutela efetiva dos direitos dos titulares de dados junto dos tribunais de cada Estado-Membro e a observância da autonomia processual dos Estados-Membros como princípio geral do direito da União.

Não obstante, tal não obstruirá o recurso prejudicial dos tribunais dos Estados-Membros ao TJUE com o propósito de aferir da conformidade do direito nacional com o direito da União, nem significará a inobservância da jurisprudência do TJUE, sob pena de se frustrar a almejada interoperabilidade no seio do Mercado Único Digital.

Conforme assinala A. Barreto Menezes Cordeiro,[20] "[e]m matéria de responsabilidade civil, o TJUE há muito que impõe, aos tribunais dos Estados-Membros, o cumprimento de dois princípios nucleares: o da equivalência e o da efetividade".

O princípio da equivalência exige aos Estados-Membros que, ao designarem os órgãos jurisdicionais competentes e ao regularem as modalidades processuais das ações destinadas a garantir a salvaguarda dos direitos que decorrem, para os cidadãos, do Direito da União Europeia, não tornem essas modalidades menos favoráveis do que as das ações análogas de natureza interna.

Por sua vez, o princípio da efetividade exige aos Estados-Membros, na esteira do que se discorreu acerca do princípio da equivalência, que essa regulação interna não torne praticamente impossível ou excessivamente difícil o exercício dos direitos conferidos pela ordem jurídica da União.[21]

No que concerne diretamente aos danos, seguindo a tese de A. Barreto Menezes Cordeiro,[22] podemos identificar um conjunto alargado de situações, de entre as quais se contam, a título de danos patrimoniais,

> (i) o aumento dos custos finais cobrados por um serviço prestado, na decorrência da transmissão ilícita de dados por um terceiro para o prestador; (ii) a não celebração de um contrato de trabalho ou o despedimento na decorrência da recolha ilícita de dados pessoais, pela entidade patronal, relativos ao candidato; (iii) a utilização ilícita de dados pessoais por entidades financeiras, com um impacto negativo nas condições apresentadas ao titular, por exemplo nos juros cobrados ou no valor do prémio do seguro; e (iv) a não retificação (artigo 16.º) ou o não apagamento de dados (artigo 17.º).

Por sua vez, no que respeita aos danos não patrimoniais, o facto (positivo ou negativo) encetado pelo responsável pelo tratamento de dados ou pelo subcontratado pode resultar na exposição pública não desejada do titular dos dados, o pejo, a

[20] Cfr. Cordeiro, "Da responsabilidade civil", 6.

[21] Vd., a este respeito, entre outros, acórdão Aprile do TJUE, de 17 de novembro de 1998, processo C-228/96; acórdãos Courage e Crehan do TJUE, de 20 de setembro de 2001, processo C-453/99; acórdão Târsia do TJUE, de 06 de outubro de 2015, processo C-69/14; acórdão Santoro do TJUE, de 07 de março de 2018, processo C-494/16; acórdão XC do TJUE, de 24 de outubro de 2018, processo C-234/17; acórdão Syndicat do TJUE, de 11 de abril de 2019, processo C-254/18.

[22] Cf. Cordeiro, "Da responsabilidade civil", 7.

ansiedade, a perturbação da intimidade e a limitação do livre desenvolvimento da personalidade, a discriminação, a depressão, etc. o que, nas palavras de A. Barreto Menezes Cordeiro, pode consubstanciar a objetivação do ser humano, enquanto mero dado.[23]

De entre os danos patrimoniais e os danos não patrimoniais, estes últimos afiguram-se de mais difícil quantificação, tal como já se verifica ao nível do direito interno, sobretudo pelo facto de o conceito de privacidade de cada indivíduo assumir um valor consideravelmente diferente, bem como pela própria natureza imensurável dos danos.

2.5. Nexo de causalidade

Por fim, a responsabilidade civil por violação do RGPD apenas poderá ocorrer se entre esta violação e os danos produzidos na esfera jurídica do lesado existir um nexo de causalidade adequada entre o facto e o dano, "de acordo com a natureza geral e o curso normal das coisas".[24] Trata-se, então, de aferir da idoneidade do facto para a produção daquele dano.

Embora não resulte expressamente do regulamento, o conceito de causalidade deve igualmente "ser interpretado (pelos tribunais dos Estados-Membros) em sentido lato e à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do RGPD".[25]

A jurisprudência do TJUE tem vindo a admitir o afastamento do preenchimento do nexo de causalidade direto entre o dano e o facto, mormente em respeito dos princípios da efetividade e da equivalência a que supra aludimos.[26]

Reiteramos, assim, a ideia da necessidade de articulação entre os vários direitos nacionais dos Estados-Membros e o Direito da União na interpretação e na aplicação do instituto jurídico da responsabilidade civil, tendo em vista a uniformização desejada no seio do Mercado Único Digital.

3. Conclusão

A evolução desaforada da tecnologia contribuiu, significativamente, para um aumento do tráfego dos dados pessoais no mercado interno, e até fora dele, e para uma aproximação (virtual) dos cidadãos na União Europeia e no mundo em geral.

O RGPD assinalou uma apropinquação da regulamentação da proteção de dados pessoais no contexto do mercado único digital e permitiu a confirmação de um direito com contornos mais definidos.

No âmbito deste regime legal, instituído pelo RGPD, reafirmou-se um conjunto alargado de direitos, de entre os quais o direito à ação judicial e o direito à indemnização. Estes direitos chamam, assim, à colação o instituto da responsabilidade civil, embora relegando para os Estados-Membros a sua efetivação e aplicação ao caso concreto, em respeito pelo princípio da autonomia processual dos Estados-Membros, bem como pelos princípios da efetividade e da equivalência.

São várias as questões que nos assaltam neste domínio, mormente no que respeita à legitimidade, à quantificação dos danos causados na esfera jurídica do

[23] Cfr. Cordeiro, "Da responsabilidade civil", 8.
[24] Vd. entre outros, acórdão do Supremo Tribunal de Justiça, de 14/02/2017, processo 528/09.7TCFUN.L2.S1, relator Alexandre Reis, disponível em http://www.dgsi.pt.
[25] Cf. Cordeiro, "Da responsabilidade civil", 8.
[26] Ibidem.

lesado e ao nexo de causalidade. Por conseguinte, caberá, em breve, aos tribunais nacionais e ao TJUE a aclaração e a concretização de todos estes domínios.

Apesar de se verificar a necessidade de preenchimento de todos os requisitos de que depende a responsabilidade civil, estabeleceu-se, no RGPD, uma inversão do ónus da prova relativamente à culpa do responsável pelo tratamento ou do subcontratado, o que se traduz numa proteção acrescida do titular do lesado. Ao mesmo tempo, o ónus da prova do facto negativo que recai sobre o responsável pelo tratamento ou subcontratado pode, na prática, revelar-se uma prova de difícil concretização, o que implicará, nestes casos, a responsabilização do responsável pelo tratamento ou do subcontratado.

Não obstante, verifica-se necessário e salutar, na aplicação deste instituto jurídico, no domínio do RGPD, a articulação entre os ordenamentos jurídicos dos Estados-Membros e o Direito da União e os seus princípios fundamentais. Pois, só desta forma, será possível alcançar a almejada interoperabilidade no contexto do Mercado Único Digital, cujas prioridades principais são a melhoria do acesso a bens e serviços digitais, a criação de um ambiente onde a oferta digital (redes, bens e serviços) possa prosperar, e a perceção do "digital" como um condutor para o crescimento,[27] observando o elevado grau de proteção de dados pessoais no contexto da União.

[27] Joana Covelo de Abreu, "O Mercado Único Digital e o seu desígnio político-constitucional: o impacto da Agenda Eletrónica Europeia nas soluções de interoperabilidade", *UNIO – EU Law Journal*, Volume 3, n.º 1, (janeiro de 2017), http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%203/UNIO%203%20PT/Novo%20Joana%20Abreu.pdf.

O papel da tecnologia na busca pela conformidade com o RGPD

Leandra Dias*

RESUMO: Não é admissível cair na tentação fácil de considerar que a tecnologia define, per si, se uma organização está em conformidade com o RGPD, porque, para além de um trabalho em contínua execução, abrange diferentes dimensões. Esta conformidade é um fenómeno transversal, mas é inegável o papel facilitador da tecnologia. Medidas técnicas como encriptação, pseudonomização ou cifragem de dados auxiliarão na demonstração da conformidade e a evitar as várias responsabilidades previstas. A centralização da informação e desmaterialização associadas à transformação digital facilitam a resposta ao exercício dos direitos dos titulares dos dados em menor tempo e custos. A inteligência artificial torna a tecnologia mais eficaz na prevenção de falhas de segurança, diminuindo o risco de exposição, podendo até orientar o utilizador na adoção do comportamento correto face ao RGPD. A conformidade só é concretizável se as organizações tornarem o seu negócio seguro/confiável e simultaneamente produtivo e, neste ponto, a tecnologia é central.

PALAVRAS-CHAVE: Conformidade demonstrada – Tecnologia – Inteligência artificial – Produtividade – Ética

ABSTRACT: We need to avoid the temptation to consider that technology itself is enough to define whether an organization is compliant with the GDPR or not. Compliance requires continuous work and it branches out, touching different fields. Although it is undeniable that technology plays a facilitating role, compliance with the GDPR is a crosscutting phenomenon. Technical measures such as pseudonymization or data encryption can help provide proof of compliance and minimize liability. The centralization and dematerialization of information associated with the digital transformation allows organizations to respond to data holder claims/provide support for data holder rights faster and with less costs. Artificial intelligence also makes technology more effective by preventing security breaches and reducing the risk of exposure, and even being able to guide users into adopting correct behaviors in light of the GDPR. Organizations can achieve success by leveraging the potential of technology for compliance with the GDPR while at the same time making their business more secure, reliable and productive.

KEYWORDS: Proof of compliance – Technology – Artificial intelligence – Productivity – Ethics

* Leandra Daniela da Silva Dias, Licenciada em Direito pela Escola de Direito da Universidade do Minho, Mestre em Direito Judiciário pela Escola de Direito da Universidade do Minho, Jurista, Product Owner de soluções de gestão na área de Recursos Humanos, Formadora em Direito Laboral e Privacidade e Proteção de Dados.

1. Introdução

Em 2015, Satya Nadella, Diretor Executivo da Microsoft, dirigindo-se aos delegados na conferência anual da empresa, nos Estados Unidos, afirmou "Every business will be a software business". Este foi o mote para o presente estudo, sendo que, apesar de concordarmos, parece-nos que esta afirmação deve ser feita no presente do indicativo. Com isto, defendemos que, para que uma organização seja competitiva no contexto atual, é necessário que tenha ou traga a tecnologia para o centro do seu negócio. É comumente aceite e consensual que a tecnologia é sinónimo de digitalização, simplificação, aceleração, produtividade, potenciando a afirmação e expansão das relações comerciais, da satisfação de clientes, da fácil interação com fornecedores e outros agentes que se relacionam com as organizações.[1]

A questão que nos assolou o espírito foi a de tentar perceber se a tecnologia pode trazer essas reconhecidas vantagens para o campo da conformidade com o Regulamento Geral de Proteção de Dados (RGPD)[2] e, em caso afirmativo, em que medida pode fazê-lo? Como? Com que objetivo e com que benefícios/dificuldades?

2. Conformidade demonstrada: a tecnologia é um elemento chave ou um elemento da equação?

Cremos que se impõe desmistificar a ideia de que "software conforme" significa organização conforme. Por um lado, deve esclarecer-se que a conformidade com o RGPD é algo exigido à organização, enquanto o software/tecnologia deve, no que para estes efeitos importa, incorporar conceitos, processos, funcionalidades que auxiliem na conformidade da organização não podendo, de forma alguma, impedir ou dificultar esse objetivo.

Longe terá de estar a tentação fácil de considerar que uma organização está em conformidade com o RGPD se, no seu leque de software/sistemas/tecnologias, estiverem incluídas ferramentas mais ou menos direcionadas para as necessidades criadas ou exponenciadas pelo RGPD[3].

Na verdade, a conformidade com o RGPD é um trabalho em contínuo progresso, pois que novas dúvidas, desafios, novas necessidades surgem quase que diariamente. Esta conformidade abrange diferentes dimensões e não se limita ou resume à tecnologia.

Numa base de melhoria contínua é necessário implementar, rever ou revisitar processos como a catalogação/classificação de dados pessoais no poder de uma organização; a recolha e tratamento de dados pessoais; a política de segurança e privacidade de dados pessoais; as avaliações de impacto; as auditorias internas e externas, assim como consciencializar e formar os colaboradores que lidam ou possam contactar com dados pessoais, fomentando a mudança de comportamentos quando necessário. Também não pode ficar esquecida, a título de exemplo, a importância de verificar as garantias de conformidade dadas pelos subcontratados e fornecedores a que a organização recorre e verificar as condições de segurança das aplicações internas ou de terceiros usadas dentro da organização.

---

[1] Leandra Dias, "O papel da Tecnologia na conformidade com o RGPD", *Fiscalidade e Legalidade*, (2019), https://pt.primaverabss.com/pt/blog/como-a-tecnologia-suporta-a-implementacao-do-rgpd/.

[2] 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 e que revoga a Diretiva 95/46/CE.

[3] Dias, "O papel da Tecnologia".

Desta forma, teremos de concluir pela transversalidade da conformidade com o RGPD, que se alicerça em diferentes dimensões – pessoas (consciencialização, formação,[4] preparação para a mudança, sendo que muito do risco e vulnerabilidades está no fator humano);[5] processos (como os atrás referidos); sistemas e ferramentas que facilitem a operacionalização do exercício dos direitos por parte dos titulares de dados, assim como de gestão de consentimento e outros fundamentos de legitimação da recolha e uso dos dados pessoais, etc.

No entanto, e apesar de a tecnologia ser apenas um elemento desta equação complexa, cremos que será inegável o papel facilitador, agilizador e diferenciador que a tecnologia pode ter neste processo.

A este respeito o art.º 32.º do RGPD refere que devem ser implementadas medidas técnicas e organizativas adequadas para assegurar um nível de segurança ajustado ao risco tendo em conta as técnicas mais avançadas, os custos de aplicação face aos riscos, a probabilidade e a gravidade variável em cada situação. Exemplifica, ainda, algumas dessas medidas referindo a pseudonimização e cifragem de dados pessoais; medidas que tenham a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; ou processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. Podemos perceber a importância da adoção destas medidas quando vemos a exceção descrita na alínea a) do n.º 3 do art.º 34.º do RGPD quando nos diz que, em caso de violação de dados pessoais, a comunicação ao titular dos dados não é exigida quando "o responsável pelo tratamento tiver aplicado medidas de proteção adequadas tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como cifragem" (sublinhado nosso).

A cifragem de dados, ao tornar os dados incompreensíveis e sem sentido para terceiros, permite que, numa situação em que ocorra incidente de violação de dados, se possa prescindir da notificação ao(s) titular(es) dos dados, o que pode fazer toda a diferença, evitando o dano reputacional da organização e a perda da confiança por parte de quem com ela, de alguma forma, se relaciona.[6]

A tecnologia pode ainda contribuir de forma positiva com cuidados aparentemente simples e com os quais as organizações estão mais familiarizadas, cuidados esses que auxiliam neste processo de busca pela conformidade. Veja-se o

[4] Para além da formação nos moldes mais tradicionais devem, ainda, ser incluídos exercícios de simulação de ataques, testes de penetração e implementar, por exemplo, conceitos como o de engenharia social.

[5] Neste sentido, na conferência *Ciber Crime: da prevenção à resposta forense*, organizada pela Ernest & Young e pelo ECO em 06/05/2019 na CCIP afirmava Sérgio Martins que "O mercado da cibersegurança tem mudado muito, mas continuam a existir muitas vulnerabilidades, particularmente na parte humana. É o elo mais fraco". Já Adriano Squilacce, na mesma conferência, defendeu que o "phishing, associado ao erro humano […] é uma das grandes ameaças às empresas", por Ana Sofia Franco, "Cibersegurança: ´Chega de investir tanto em tecnologia. É preciso começar a olhar para as pessoas`", *MSN Notícias*, Maio 06, 2019, https://www.msn.com/pt-pt/noticias/newsscienceandtechnology/cibersegurança-"chega-de-investir-tanto-em-tecnologia-é-preciso-começar-a-olhar-para-as-pessoas"/ar-AAAYSfR?li=BBoPEwF.

[6] Dias, "O papel da Tecnologia".

exemplo dos programas de antivírus, de sistemas de bloqueio de downloads de fontes desconhecidas ou suspeitas, de uma política de atualização regular das palavras chave, de mecanismos que permitam a recuperação de dados.

Também a execução de testes de penetração, testes de engenharia social, assim como a realização de auditorias internas e externas serão exemplos de trabalho desenvolvido rumo à responsabilidade demonstrada e à potencial conformidade.

Isto dito, e para definir qual o papel da tecnologia na busca pela conformidade com o RGPD, traríamos o aforismo que define o lema dos Jogos Olímpicos – ***Citius, Altius, Fortius*** (mais rápido, mais alto, mais forte).

A tecnologia é um facilitador/simplificador para a meta da conformidade, pois permite executar um conjunto de tarefas associadas ao cumprimento de obrigações impostas pelo RGPD de forma menos penosa. Veja-se uma organização confrontada com o exercício do direito à informação e de acesso por um titular de dados que obrigaria a percorrer todas as aplicações e locais de armazenamento de dados onde o titular dos mesmos pudesse constar. Se essa pesquisa tivesse de ser efetuada manualmente, para além de bastante mais morosa, estaria mais sujeita a erros e teria um custo administrativo superior. Agora, imagine-se o mesmo cenário, mas em que o exercício desse direito foi manifestado por vários titulares em simultâneo. Sem o auxílio da tecnologia dificilmente se conseguiria executar em tempo útil esta tarefa ou isso acarretaria um gasto de tempo substancialmente superior, significando menor produtividade e eficiência.

Assim, poderá também ser reconhecido à tecnologia um papel acelerador e otimizador de recursos.

Cremos que a tecnologia pode ter um papel relevante para facilitar a prevenção e antecipação de deteção de falhas de segurança e violações de dados, contribuindo para a diminuição do risco de exposição dos dados.

Através da incorporação da encriptação de palavras-chave e de ficheiros; da definição de perfis e de níveis de acesso à informação e de categorias de informação; da existência do histórico de operações (Log) pode-se chegar mais longe. Neste último caso, permite-se detetar *quem*, *quando*, *onde*, *a quê* e *o quê* consultou/executou sobre determinados dados, o que permite, não raras vezes, detetar a origem e a responsabilidade por incidentes de violação de dados.

Todos estes exemplos servem para a construção de evidências de conformidade, que permitem demonstrá-la de forma mais fácil estando centralizadas e com rápido acesso em caso de auditoria ou inspeção.

3. O contributo da inteligência artificial e *machine learning* para a conformidade

Não existe fórum de debate tecnológico onde os conceitos de *inteligência artificial* e *machine learnig* não sejam abordados ou tratados ainda que lateral ou subsidiariamente. Por isso, na discussão da problemática em causa não podemos deixar de considerar estas realidades que, apesar de não serem propriamente uma novidade, ganharam maior interesse e visibilidade nos últimos anos atentos os progressos alcançados.

Nesse sentido,

> A Inteligência Artificial tem que lidar com o desafio de desenvolver comportamentos inteligentes em computadores com o objetivo de emular os humanos na realização de tarefas do quotidiano, tais como a capacidade de compreender e utilizar uma linguagem, o reconhecimento de figuras, a

aprendizagem ou a resolução de problemas.[7]

Pretende-se, através da inteligência artificial, poder atribuir às máquinas as capacidades de raciocínio, conhecimento, planeamento, aprendizagem, comunicação, perceção e a capacidade para mover ou manipular objetos[8].

Poderemos então afirmar que o uso de inteligência artificial e *machine learning* trazem benefícios importantes nos domínios da conformidade com as exigências do RGPD? De que forma podem promover o objetivo da conformidade?

Em primeiro lugar, através da identificação de padrões ou a construção dos mesmos pode permitir-se uma rápida identificação de novos dados como dados pessoais, assim como proceder à sua catalogação de forma quase imediata e automática. Esses padrões poderão também ajudar a bloquear um potencial *malware*.

Também aqui poder-se-á beneficiar do fator "antecipação" dado que se poderá "ensinar" a máquina, por exemplo, a reconhecer e aplicar os prazos legais de manutenção/conservação dos dados pessoais, deixando que depois promova o alerta aquando da chegada do fim desses prazos para, de seguida, e após validação humana, operacionalizar o princípio da minimização de dados ou até o esquecimento dos mesmos. Com esse binómio - ensino/aprendizagem pela máquina -, mais facilitadas ficariam a prevenção e deteção de falhas de segurança e violações de dados, pois a máquina iria procurá-los.

Na verdade, do que se fala é da criação de um sistema de apoio à decisão como acontece, há vários anos, noutras áreas. Deste tipo de iniciativas são exemplo o *Expertius* (sistema mexicano de apoio à tomada de decisão judicial no âmbito do Direito da Família), auxiliando juízes a determinar se o requerente deve ou não obter pensão de alimentos e, em caso afirmativo, qual o montante que a mesma deve assumir; o *Smartsettle* (sistema de apoio à negociação com vista a solucionar conflitos satisfazendo as necessidades identificadas pelas partes) e o *Family Winner* (sistema de apoio à decisão no âmbito da Direito da Família na Austrália) também numa base de negociação atendendo àquilo que é mais e menos valorizado pelas partes. [9]

Atendendo à evolução que tem existido neste âmbito e que se espera acontecer, antecipa-se que os agentes inteligentes de *software* "venham a ser capazes de mediar conflitos, o que implica que sejam capazes de percecionar o seu ambiente (que compreenderá as partes, as características e domínio do problema, o direito e outros parâmetros)".[10]

Não se podem retirar desta equação as capacidades de comunicação, de fazer raciocínios dedutivos e indutivos, de concluir, de compreender a linguagem natural. Estando essas premissas garantidas, os agentes inteligentes de *software* poderão assumir o papel de "mediadores ou árbitros, replicando o comportamento dos peritos humanos".[11]

Estes agentes inteligentes de *software* poderão ser uma mais-valia no auxílio das organizações na verificação de falhas e na avaliação da sua conformidade no âmbito de auditorias internas? Poderão também auxiliar as autoridades de controlo

[7] Francisco Carneiro Pacheco Andrade (*et al.*), "A inteligência artificial na resolução de conflitos em linha", *Scientia Iuridica*, Tomo LIX, n.° 321 (2010): 19, http://repositorium.sdum.uminho.pt/bitstream/1822/19388/1/4%20-%202010b%20-%20Journal%20Scientia%20Ivridica.pdf.

[8] Stuart Russell e Peter Norvig, *Artificial Intelligence: A Modern Approach* citado por Francisco Carneiro Pacheco Andrade et al., *A inteligência artificial*, 19.

[9] *Ibidem,* p. 27-28.

[10] *Ibidem*, p. 27-28.

[11] *Ibidem*, p. 27-28.

em inspeções às organizações?

Atente-se que, muito recentemente, já depois de 25 de maio de 2018, a Organização Europeia de Consumidores usou inteligência artificial (algoritmo **Claudette)**[12] para analisar as políticas de privacidade de 14 empresas de tecnologia. Ou seja, com o objetivo de avaliar a conformidade com o RGPD das políticas de privacidade de entidades como a Google, Facebook (e Instagram), Amazon, Apple, Microsoft, WhatsApp, Twitter, Uber, AirBnB, Booking.com, Skyscanner, Netflix, Steam e Epic Games de forma automática, recorreu-se à inteligência artificial, colocando-a ao serviço da sociedade civil.[13]

Compõem estes 14 documentos cerca de 80.000 palavras (!), o que implicaria vários dias de análise de um humano, que ficaria exausto após algum deste tempo, e que necessitaria de descansar e de prover a outras necessidades físicas. Por outro lado, era difícil garantir exatamente o mesmo nível de concentração durante essa análise. Poderia uma máquina apoiar na deteção de falhas ou insuficiências de um texto face a exigências legais? Muito provavelmente sim.[14]

Na verdade, o algoritmo *Claudette* constitui uma prova de conceito de que é possível usar, com bons resultados, a inteligência artificial através do *machine learning*. Nestes domínios pelo menos; já que permitiu detetar que um terço das cláusulas analisadas era "potencialmente problemático" ou continha "informação insuficiente" e mais de 11 por cento continham termos pouco claros.[15]

Conseguiu-se, desta forma, otimizar a análise (efetuada em muito menos tempo do que seria se fosse efetuada por um humano), aplicando-se exatamente os mesmos critérios de análise a cada um dos textos, o que aumenta a justiça da análise em si e dos resultados obtidos.

Por outro lado, pode-se dizer que a análise efetuada pelo algoritmo é mais isenta e imparcial dado que não sofre influência de preconcebimentos no sentido em que todas as políticas de privacidade analisadas seguiram o mesmo processo e critérios, tornando-se mais impermeável a ideias pré-concebidas.

Assim, poder-se-á concluir que esta tecnologia pode auxiliar num conjunto de diferentes frentes.[16] Poderá, por exemplo, ser usada no desenvolvimento de ferramentas de análise ao serviço das Autoridades de Controlo e, bem assim, das associações de defesa dos consumidores, possibilitando detetar falhas e incoerências na atuação dos responsáveis pelo tratamento.

Também os consumidores finais, os cidadãos comuns, terão a tarefa mais facilitada. Com recurso a uma *app* ou um sistema simples, por exemplo, não teriam de ler/analisar um texto longo de acordo com critérios de análise que podem não conhecer, e, de forma simples e rápida, conseguiriam perceber que categorias de dados estão a ser recolhidos/tratados, quais os fundamentos invocados, para que finalidades, qual o período de manutenção desses dados e se os mesmos são ou não partilhados com terceiros. Uma aplicação desse tipo dará mais informação e

[12] Automated CLAUse DETeCTER", http://claudette.eui.eu.

[13] Giuseppe Contissa et al., *CLAUDETTE MEETS GDPR – Automating the Evaluation of Privacy Policies using Artificial Inteligence* (Florence, Bologna, Reggio Emilia: BEUC, 2018), 1, https://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf.

[14] Giuseppe Contissa et al., *CLAUDETTE: an Automated Detector of Potentially Unfair Clauses in Online Terms of Service* (2019), https://arxiv.org/pdf/1805.01217.pdf.

[15] *Ibidem*, p. 56-57.

[16] Neste sentido, Contissa, *CLAUDETTE MEETS GDPR*.

autonomia ao cidadão.[17/18]

Nesta mesma linha, as atividades de tratamento poderiam ser submetidas a um rastreio de conformidade onde a inteligência artificial fosse usada para, por exemplo, ajudar cada organização a perceber, através de notificações, se existem não conformidades, permitindo-lhe tomar conhecimento da sua existência e adotar medidas adequadas a minimizá-las ou eliminá-las. Ferramentas deste tipo seriam um importante apoio e facilitador das funções do Encarregado de Proteção de Dados, tal como seria se pudessem auxiliá-lo na decisão da necessidade ou não de realizar uma avaliação de impacto com base em *inputs* previamente fornecidos. Ter-se-ia, neste caso, um verdadeiro sistema de apoio à decisão como já existe noutras áreas do Direito em diferentes localizações.

No entanto, e não obstante todos os benefícios que se reconhece ao uso da inteligência artificial nestes domínios, não podemos deixar de defender que a mesma só pode ser usada dentro dos limites legais e éticos e isso só será possível através de uma cooperação estreita entre tecnólogos e juristas.[19]

Seguimos de perto Kriti Sharma[20] quando afirma que se deve "[…] garantir que há um grupo diversificado de pessoas a criar a tecnologia, não apenas tecnólogos […] mas também pessoas que compreendem a sociedade, as leis, a política." E acrescenta "[…] quando desenhamos IA temos de pensar na ética desde o princípio. Que valores queremos? Da mesma forma que temos regras para os humanos que trabalham em diferentes áreas, as máquinas devem seguir regras e não ter preconceitos ou ser discriminatórias".

Surgem aqui outras questões – no caso em que a aprendizagem da máquina se baseie em decisões humanas anteriores, então essa aprendizagem trará consigo os preconceitos que os humanos veicularam nessa decisão.[21]

Tendo em conta estas preocupações, a Comissão Europeia disponibilizou a versão final de um guia de princípios éticos que devem nortear o desenvolvimento da inteligência artificial.[22] De notar que estes princípios não são Leis, nem podem ser considerados *soft law*, o que os fragiliza e pode discutir-se quem deve e como regular a ética na Inteligência Artificial: se os governos, se as instituições supranacionais, se a indústria ou se uma força conjunta, considerando que esta última hipótese será a mais produtiva, importando agregar os contributos de diferentes áreas.[23]

Defendemos, ainda, que nestes processos dominados pela máquina tem de existir alguma intervenção humana, principalmente quando se tratem de sistemas de apoio à decisão. Para além do controlo dos algoritmos por algoritmos, teremos de

---

[17] *Ibidem*, p. 56 e 57.

[18] Leandra Dias, "A inteligência artificial ao serviço do RGPD", *Inovação e Tecnologia*, (junho 4, 2019), https://pt.primaverabss.com/pt/blog/como-aplicar-a-inteligencia-artificial-ao-rgpd/.

[19] Leandra Dias, "A inteligência artificial".

[20] Kriti Sharma, "Jovens de hoje vão fazer trabalhos que ainda não existem", *Jornal de Notícias*, Caderno Dinheiro Vivo, 2019, 10.

[21] Neste sentido recentemente se pronunciou Eduardo Magrani na conferência *Brazil Legal Symposium* na Faculdade de Direito de Harvard em abril de 2019.

[22] High-Level Expert Group on Artificial Intelligence, *Ethics guidelines for trustworthy AI* (Brussels: European Comission, 2019), https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[23] Veja-se o exemplo identificado por Kriti Sharma (em *Jovens de hoje vão fazer trabalhos que ainda não existem*) relativamente ao Reino Unido, em que o governo criou um organismo independente, o Centro para a Ética e Inovação dos Dados, que trabalha com legisladores, indústria, governo, tecnólogos com o objetivo de criar padrões e garantias.

ter a intervenção humana. Não poderíamos aceitar que a aplicação de uma coima por não cumprimento do RGPD fosse aplicada por uma autoridade de controlo baseada em exclusivo nos resultados apresentados por um algoritmo. Nesse caso poderíamos dizer que estávamos perante uma decisão automatizada, vedada pelo RGPD?[24]

Importa investir verdadeiramente em literacia digital ética para que os avanços tecnológicos sirvam bons propósitos e todos possamos deles beneficiar.

4. Conclusões

A conformidade com o RGPD engloba várias áreas, sendo uma questão transversal dentro das organizações.

Essa conformidade só é concretizável se as organizações fizerem do seu negócio uma realidade segura e confiável, garantindo ao mesmo tempo a produtividade. É neste ponto que a tecnologia tem um papel facilitador, acelerador, distintivo e otimizador, levando-nos mais longe nesta busca pela conformidade.

A inteligência artificial e o *machine learning* podem ser colocados ao serviço das Autoridades de Controlo, das associações de defesa dos consumidores, dos encarregados de proteção de dados e, principalmente, dos cidadãos, tornando o cumprimento, verificação e conhecimento do RGPD mais simples e com resultados otimizados.

Claro está que não é possível deixar os limites legais e a ética fora desta equação, sendo o fiel que garantirá o seu bom uso e permitirá o benefício global. O investimento em literacia digital ética é urgente e os padrões éticos deverão ser o resultado de uma atuação conjunta ente legisladores e a indústria e entre tecnólogos e juristas.

[24] De acordo com o art.º 22.º, n.º 1 do RGPD "O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado […] que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Princípio da integração ambiental: um guia a direcionar projetos de cidades inteligentes na União Europeia

Nataly Carvalho Machado*

RESUMO: *Num contexto mundial, em que espaços urbanos e alterações climáticas são alvos de constantes questionamentos acerca de possíveis soluções para os problemas que a atividade humana pode afetar direta ou indiretamente o ambiente, a agenda da União Europeia (UE) demonstra grande preocupação em integrar a tecnologia na construção de cidades inteligentes. Para tanto, considerações ambientais, no que concerne ao respeito dos princípios fundamentais do Direito do Ambiente, devem estar em conformidade com a aplicação das políticas da UE em prol de resultados eficazes na criação, exempli gratia, de um dos sistemas energéticos mais sustent*áveis *do mundo. E como alicerce desse projeto, o princípio da integração ambiental aparece como protagonista no estabelecimento de metas e ações que visam à transformação de espaços urbanos da comunidade europeia em ambientes mais sustentáveis, ao utilizar as soluções tecnológicas que o mundo digital pode proporcionar.*

*PALAVRAS-CHAVES: Princípio da Integraç*ão *– Cidades inteligentes – Tecnologia – Ambiente – Sustentável*

ABSTRACT: In a global context, where urban spaces and climate change are the subject of constant questions concerning possible solutions to problems that human activity may directly or indirectly affect the environment, the European Union (EU) agenda shows great concern about integrating technology in the construction of intelligent cities. Therefore, environmental considerations must respect the fundamental principles of environmental law and must be in line with the implementation of EU policies for effective results in the creation of, exempli gratia, one of the most sustainable energy systems in the world. And as a cornerstone of this project, the principle of environmental integration appears as the protagonist in establishing goals and actions that aim to transform urban spaces of the European community into more sustainable environments by using the technological solutions that the digital world can provide.

KEYWORDS: Integration Principle – Smart cities – Technology – Environment – Sustainable development

* Mestranda em Direito da União Europeia na Universidade do Minho.

1. Considerações introdutórias

A necessidade de se dar maior atenção à degradação ambiental decorre do surgimento de desastres ambientais paradigmáticos[1] que, de certa forma, direcionam acordos internacionais[2] que visam à consecução de ações que possam conciliar a atividade humana e um ambiente sustentável.

Por esse ângulo, a União Europeia tem como um dos seus grandes intentos, a longo prazo, viabilizar projetos com conceito de desenvolvimento sustentável e permitir uma unidade indissociável entre o crescimento econômico e a proteção dos equilíbrios sociais e ambientais.[3]

Nos grandes centros urbanos, a preocupação dos Estados-Membros em encontrar e aplicar soluções que possam diminuir o impacto humano negativo sobre o meio ambiente se sobressai, através do princípio da integração ambiental, nos planos de construção de cidades inteligentes e sustentáveis.

No entanto, há de se ter em conta que o uso das tecnologias de comunicação e informação (TIC) nos projetos das referidas cidades poderá, ao mesmo tempo que confere, aos cidadãos, ferramentas tecnológicas e inovadoras que facilitam a integração entre o social e a sustentabilidade, acarretar desafios, nesse mesmo sistema de inovações em prol do melhoramento dos centros urbanos atinentes à proteção dos dados pessoais, que se terá de pautar à luz do Regulamento de Proteção de Dados Pessoais (RGPD)[4] vigente na União Europeia.

Nesse sentido, o enfoque dessa pesquisa destina-se a entender como surgiu e como é aplicado o princípio da integração ambiental dentro da União Europeia, indicando seu papel transversal desde o planejamento até a aplicabilidade das políticas da União, nomeadamente quando se fala na construção de cidades inteligentes (*smart cities*). Ainda, será questionado como o projeto das referidas cidades poderá ser pensado numa perspectiva de proteção de dados pessoais, dada a interoperabilidade dos sistemas digitais que norteiam uma *smart city*.

---

[1] Como o desastre ocorrido com o Torrey Canyon, navio liberiano que encalhou perto das ilhas Scilly (Reino Unido), no ano de 1967, e que derramou perto de 120 000 toneladas de petróleo bruto, atingindo o litoral da Bretanha (oeste de França), in "Maré negra: principais desastres desde 1967", *Correio do Minho*, Maio 29, 2010, https://correiodominho.pt/noticias/mare-negra-principais-desastres-desde-1967/29114.

[2] O Protocolo de Quioto, adotado em dezembro de 1997 em complemento à Convenção-Quadro das Nações Unidas sobre Alterações Climáticas (CQNUAC), salienta a atitude da comunidade internacional relativamente ao fenômeno das alterações climáticas. O Protocolo entrou em vigor em 2005. Ao abrigo do primeiro período de compromisso do Protocolo de Quioto, os países industrializados comprometeram-se a reduzir em 5%, em média, as emissões respetivas de seis gases com efeito de estufa (dióxido de carbono, metano, óxido nitroso, hidrofluorocarbonetos, perfluorocarbonetos e hexafluoreto de enxofre) durante o período 2008-2012, relativamente aos níveis de 1990. A UE e 15 países da UE (os respetivos membros aquando da adoção do Protocolo) comprometeram-se a reduzir em 8% as respetivas emissões como um todo. Informação disponível em: https://eur-lex.europa.eu/summary/glossary/kyoto_protocol.html?locale=pt.

[3] Definido no Relatório Brundtland de 1987 "O Nosso Futuro Comum" da Comissão Mundial para o Ambiente e o Desenvolvimento como "desenvolvimento que responde às necessidades do presente sem comprometer a capacidade de resposta das gerações futuras às suas próprias necessidades", o desenvolvimento sustentável tornou-se formalmente um dos objetivos, a longo prazo, da União Europeia com a introdução do artigo 3.º, n.º 3, do Tratado da União Europeia, disponível em: https://eur-lex.europa.eu/summary/glossary/sustainable_development.html?locale=pt.

[4] 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

2. O princípio da integração ambiental no ordenamento europeu

O desenvolvimento da política ambiental na União Europeia[5] iniciou-se, ainda que com uma perspectiva de proteção ambiental, como um pressuposto para projetos de cunho econômico.[6]

A noção de consciência ambiental aparece na década de 1960, com a publicação do livro "Primavera Silenciosa", de Rachel Carson, com sua consequente expansão na década seguinte, com o advento da Conferência das Nações Unidas sobre o Meio Ambiente Humano, celebrada em Estocolmo, no ano de 1972.

E foi em função desta referida Conferência que o Direito do Ambiente se tornou eco constante na pauta não mais somente econômica, mas também na sócio-político-jurídica da União Europeia, com um papel consolidado na prossecução da preservação ambiental[7] e da qualidade de vida populacional dos Estados-Membros.

Com a assinatura do Ato Único Europeu (AUE), em 1986,[8] foi promovida a primeira modificação substancial ao Tratado de Roma quanto ao alargamento dos poderes da União, inclusive no domínio da proteção do ambiente, no qual foi introduzido um novo título "Ambiente", através do qual foi concebida, numa perspectiva comum aos Estados-Membros, a base jurídica ambiental que dispõe sobre a preservação da qualidade do ambiente, a proteção da saúde humana e a garantia da utilização racional dos recursos naturais.[9]

Mais adiante, o desígnio em tela foi previsto no princípio n.º 4 da Declaração de Princípios e no capítulo 8.º da Agenda 21, ambos firmados durante a Conferência das Nações Unidas sobre Meio Ambiente e Desenvolvimento, realizada no Rio de Janeiro (Brasil) em 1992.[10]

---

[5] Ludwig Krämer, "The European Union is the only region in the world which had fixed itself the objectives of economic growth and sustainable development which ensures the protection of the environment", in *Eu Environmental Law*, Ludwig Krämer (London: Sweet & Maxwell, 2012), vii.

[6] Vide Declaration of the Council of the European Communities and of the representatives of the Governments of the Member States meeting in the Council of 22 November 1973 on the programme of action of the European Communities on the environment - JO 1973 C 112/1 - , a qual dispõe, em seu preâmbulo, que "nos termos do artigo 2.º do Tratado que a institui, a Comunidade Económica Europeia tem nomeadamente a missão de promover o desenvolvimento harmonioso de atividades económicas no conjunto da Comunidade e uma expansão contínua e equilibrada, o que não se pode conceber, doravante, sem uma luta eficaz contra as poluições e perturbações e sem a melhoria da qualidade de vida e da proteção do ambiente".

[7] Philippe Pomier Layrargues, "Do ecodesenvolvimento ao desenvolvimento sustentável: evolução de um conceito?" (1997) *apud* Heline Sivini Ferreira, "Do desenvolvimento ao desenvolvimento sustentável: um dos desafios lançados ao estado de direito ambiental", in *Repensando o Estado de Direito Ambiental*, org. José Rubens Morato Leite, Heline Sivini Ferreira e Matheus Almeida Caetano (Florianópolis: FUNJAB, 2012), 132.

[8] O Ato Único Europeu apenas entrou em vigor em 1 de julho de 1987, com seis meses de atraso, devido a um recurso interposto junto dos tribunais irlandeses por um particular. Informação disponível em: http://www.europarl.europa.eu/factsheets/pt/sheet/2/a-evolucao-conducente-ao-ato-unico-europeu.

[9] Informações sobre a política ambiental da União Europeia, relativa aos princípios gerais e quadro de base, disponível em: http://www.europarl.europa.eu/factsheets/pt/sheet/71/politica-ambiental-principios-gerais-e-quadro-de-base.

[10] Ocorre que estes documentos internacionais, segundo a doutrina tradicional, não têm força vinculativa, uma vez que não preenchem os requisitos de validade de um tratado multilateral, constituindo o chamado *soft law*, embora sejam dotados de relevância jurídica e crescente importância no direito internacional. No entanto, a aceitação da *soft law* como obrigatória é cada vez mais crescente, como enfatiza a Professora da George Washington University Law School, Dinah Shelton: "Soft law instruments adopted subsequent

Com a entrada em vigor do Tratado de Amesterdão, no ano de 1999, o qual modificou o Tratado da União Europeia, foi declarado, no art. 6º, que "as exigências em matéria de proteção do ambiente devem ser integradas na definição e execução das políticas e ações da Comunidade [...], em especial com o objetivo de promover um desenvolvimento sustentável".

Vale lembrar, outrossim, que foi desde a chamada *Iniciativa Cardiff,*[11] à mesma época dos negociações do Tratado de Amesterdão, que o componente ambiental teve uma presença longa e importante dentro da União Europeia, e a sua ligação à estratégia então comunitária e hoje europeia para o desenvolvimento sustentável[12] permaneceu até os dias atuais.

Finalmente, com o Tratado sobre o Funcionamento da União Europeia (TFUE), o art. 6º do Tratado de Amesterdão passa a estar incluído no art. 11º daquele ato de direito originário, refletindo, principalmente, a necessidade de abordar o desenvolvimento social, pondo-se no mesmo plano de valoração a dimensão ambiental e as questões econômicas e sociais.

Imperioso destacar, ainda, que o princípio da integração ambiental está explícito no art. 37º da Carta dos Direitos Fundamentais da União Europeia (CDFUE) dispondo que "todas as políticas da União devem integrar um elevado nível de proteção do ambiente e a melhoria da sua qualidade, e assegurá-los de acordo com o princípio do desenvolvimento sustentável".

Sobre o princípio, comenta Alexandra Aragão que:

> A consagração da proteção do ambiente na Carta dos Direitos Fundamentais da União Europeia não nos deve fazer esquecer que a proteção ambiental está igualmente presente nos sistemas nacionais de proteção dos direitos fundamentais. Esta é uma das políticas da União que mais tem crescido, tanto em importância quantitativa como qualitativa. A interpretação do conteúdo do art. 37º não pode ser feita senão nesse contexto europeu alargado. [...] Ora, no panorama dos direitos fundamentais da União Europeia, as condições são totalmente diferentes. Primeiro, porque o dever de proteção ambiental foi consagrado expressamente entre os doze direitos de solidariedade; depois, porque foi consagrado com uma relevância e uma abrangência tais, que seria difícil, com outra fórmula, dizer tanto com tão poucas palavras. Referimo-nos, por um lado, à exigência de assegurar um nível elevado de proteção e por outro ao dever de reconhecer a proteção ambiental, como objetivo secundário, de *todas* as políticas da União.[13]

---

to a treaty are useful in allowing treaty parties to authoritatively resolve ambiguities in the binding text or fill in gaps, without the cumbersome and lengthy process of treaty amendment. This is part of an increasingly complex international system with variations in forms of instruments, means, and standards of measurement that interact intensely and frequently, with the common purpose of regulating behavior within a rule of law framework" , cf. Dinah Shelton, "Law, Non-Law and the Problem of 'Soft Law'", in *The Role of Non-Binding Norms in the International Legal System*, ed. Dinah Shelton (New York: Oxford University Press, 2000), 17.

[11] "A integração das preocupações ambientais noutros domínios de intervenção da União Europeia passou a ser um conceito importante da política comunitária desde que surgiu, pela primeira vez, com uma iniciativa do Conselho Europeu, que teve lugar em Cardiff, em 1998", informação disponível em: http://www.europarl.europa.eu/factsheets/pt/sheet/71/politica-ambiental-principios-gerais-e-quadro-de-base.

[12] Enrique Leff, *Saber ambiental* (Petrópolis: Editora Vozes Ltda, 2001), 17.

[13] Alexandra Aragão, "Artigo 37º - Proteção do ambiente", in *Carta dos Direitos Fundamentais da União Europeia: comentada,* coord. Alessandra Silveira e Mariana Canotilho (Coimbra: Almedina, 2013),

No âmbito europeu, o princípio em liça é considerado um dos vetores do direito ambiental, dada a sua transversalidade na aplicação das políticas da União.[14/15] Ou seja, a questão ambiental deve ser levada em conta, por exemplo, no planejamento, execução e manutenção de aeroportos, haja vista o seu impacto direto no meio ambiente, de modo a garantir um elevado nível de proteção ambiental.[16]

Importa ter em conta ainda, que, "*nos procedimentos deliberativos ambientalmente relevantes, deve ser cumprido o dever de promover a efetiva e tempestiva participação do público*".[17] Neste caso, trata-se da Convenção de Aarhus, um acordo ambiental multilateral sob os auspícios da Comissão Económica das Nações Unidas para a Europa (UNECE), que entrou em vigor em 2001, e da qual são partes a União Europeia e os seus Estados-Membros. O caráter inovador da Convenção estabelece relações entre os direitos ambientais e os direitos humanos, uma vez que garante o envolvimento dos cidadãos[18] na participação democrática das decisões relacionadas ao meio ambiente, ao acesso às informações em posse da administração pública, bem como ao acesso à justiça, quando aqueles dois direitos não tenham sido considerados.[19]

Ora, com uma base jurídica sólida, o princípio da integração do ambiente, na União Europeia, deve permear toda e qualquer política pública, sem sobreposição ou concorrência entre os demais princípios norteadores do Direito Europeu.

Sobre a elaboração e a implementação das políticas ambientais, comenta Ludwig Krämer:

> The provision states that environmental considerations be fully taken into account in the elaboration and implementation of other Union policies. It is based on the concept that environmental requirements and, subsequently, environmental policy cannot be seen as an isolated green policy which groups specific actions on the protection of water, air, soil, fauna and flora. Rather, the environment is affected by other policies such as on transport, energy and agriculture, for example. art.11 TFUE therefore calls for a permanent, continuous "greening" of all Union policies. As mentioned above, though, art.11 TFUE does not allow priority to be given to environmental requirements over other requirements; rather, the different objectives of the Treaties rankat the same level and the policy must endeavour to achieve all of them; this is also

Arquivo Kindle, loc. 11708, loc. 11713, loc. 11732.

[14] Carla Amado Gomes e Tiago Antunes, "O ambiente no Tratado de Lisboa: uma relação sustentada", in *Textos Dispersos de Direito do Ambiente*, ed. Carla Amado Gomes, vol. III (Lisboa: AAFDL, 2010), 355-394.

[15] José Joaquim Gomes Canotilho e Vital Moreira, *Constituição da República Portuguesa Anotada*, vol. I., 4.ª ed. (Coimbra: Coimbra Editora, 2014), 851-852.

[16] Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à avaliação dos efeitos de determinados projetos públicos e privados no ambiente que, por sua vez, é conhecida como "Diretiva AIA (Avaliação dos efeitos de projetos no ambiente)", ao objetivar a garantia de um elevado nível de proteção do ambiente, bem como a garantia da integração das preocupações ambientais na preparação de projetos. Informações disponíveis em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:ev0032.

[17] Aragão, "Artigo 37º - Proteção do ambiente", loc. 11847.

[18] Vide Acórdão do TJUE *Lesoochranárske zoskupenie*, 8 de março de 2011, Processo C-240/09, no qual foi feito um pedido de reenvio prejudicial acerca do acesso à informação, participação pública no processo de tomada de decisão e acesso à justiça em matéria ambiental, celebrada em 25 de Junho de 1998 e aprovada pela Comunidade Europeia por Decisão do Conselho, de 17 de Fevereiro de 2005 (JO L 124, p. 1).

[19] Informação disponível em: http://www.europarl.europa.eu/factsheets/pt/sheet/71/politica-ambiental-principios-gerais-e-quadro-de-base.

the meaning of art.7 TFUE .[20]

Assim, o princípio em questão, fundamental do Direito Ambiental, trata-se de "*reconhecer o caráter transversal do meio ambiente*",[21] bem como de "*ter em consideração*"[22] o próprio ambiente.

Nesse contexto, a construção de cidades inteligentes (*smart cities*), projeto com um elevado grau de integração ambiental, de caráter transversal, em conjunto com a interoperabilidade pelo uso de tecnologias de informação e comunicação (TIC), tem sido um dos empenhos da União Europeia.[23]

3. O fortalecimento da sustentabilidade nas cidades inteligentes

Em alguns países, designadamente os Estados-Membros da União Europeia, o processo de industrialização estimulou as populações rurais a migrarem em direção aos centros urbanos[24] em busca de melhores retribuições. Tal situação exacerba problemas como distribuição de energia e água, infraestrutura das zonas de saneamento e de transporte, mobilidade urbana e conservação do ambiente.[25]

Ora, a prossecução do desenvolvimento sustentável[26] tem sido um dos planos estratégicos da agenda da União para minimizar e/ou eliminar alguns dos problemas como os supramencionados.

E pensar em sustentabilidade remete para a ideia de se dar mais atenção à degradação do ambiente na mesma dimensão das questões sociais. Quanto a estas, a concentração urbana da população europeia, nos últimos anos, tem se tornado objeto de projetos que possam conciliar o uso das tecnologias digitais com a construção de um novo conceito de cidade, na qual o uso de tecnologias pode transformar as redes e serviços tradicionais que conhecemos noutros mais eficientes. Tais projetos são as cidades inteligentes.

Inicialmente, é imprescindível ter a noção de que um complexo urbano pode ser qualificado como inteligente quando investimentos feitos em capital humano, em aspectos sociais, em infraestruturas energéticas, tecnologias de comunicação e infraestruturas de transporte contemplam e proporcionam uma elevada qualidade de vida e, no mesmo nível de importância, promovem o desenvolvimento econômico-ambiental sustentável, governança participativa, gestão prudente e reflexiva dos recursos naturais[27].

---

[20] Krämer, *Eu Environmental Law*, 20.

[21] Aragão, Artigo 37º - "Proteção do ambiente", loc. 11793.

[22] Ibidem, loc. 11823.

[23] Informações a respeito dos projetos da União Europeia referentes às *smart cities* em: https://smart-cities-infosystem.eu/.

[24] Para mais informações sobre a urbanização da população e perspectivas até o ano de 2050, consultar relatório anual de 2018 da Organização das Nações Unidas - ONU, disponível em: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html.

[25] A. Zucaro, M. Ripa, S. Mellino, M. Ascione e S. Ulgiati, "Urban resource use and environmental performance indicators. An application of decomposition analysis", *Ecological Indicators*, 47 (2014): 16-25.

[26] O conceito de desenvolvimento sustentável foi apresentado pela primeira vez no relatório Brundtland, no ano de 1987, também nomeado de relatório "Nosso Futuro Comum", preparado pela Comissão Mundial sobre o Meio Ambiente e o Desenvolvimento. O conceito definia desenvolvimento sustentável como "[d]esenvolvimento que atenda às necessidades do presente sem comprometer a capacidade das gerações futuras de atender suas próprias necessidades", disponível em: https://www.apambiente.pt/index.php?ref=16&subref=140.

[27] A. Caragliu e P. Nijkamp, "An Advanced Triple-Helix Network Model for Smart Cities Performance", *Research Memorandum, Faculty of Economics and Business Administration* (2011).

A *smart city,* termo em inglês que remete para a tradução portuguesa de "cidade inteligente", engloba, na sua gênese, a utilização de tecnologias digitais de informação e de comunicação[28] para a consecução do desenvolvimento econômico, da sustentabilidade ambiental e da qualidade de vida dos cidadãos, ao conciliar as dimensões da economia inteligente, da população inteligente, da governança inteligente, da mobilidade inteligente e do meio ambiente inteligente.[29]

E quando se fala em melhor qualidade de vida dos cidadãos, não há como se olvidar a necessidade de melhorar, cada vez mais, a aplicação das políticas ambientais da União[30] em todos os Estados-Membros, tendo-se por base, sempre, o princípio da integração ambiental.

Nos projetos de cidades inteligentes, o grande desafio está na aplicabilidade das políticas supracitadas, uma vez que, ao conseguir conciliar o domínio do ambiente com os planejamentos tecnológicos de melhoramento dos serviços urbanos, a essência de uma *smart city,*[31-32] que é a de crescimento econômico sustentável, terá sido alcançada.

O referido crescimento econômico sustentável parte da ideia de incluir a eficiência na utilização dos recursos naturais, a proteção do ambiente e equilíbrio dos ecossistemas, a gestão da água e dos resíduos, a eficiência energética e a utilização de energias renováveis, a construção sustentável, a mobilidade, a qualidade do ar, biodiversidade. Ou seja, todas as áreas que, de certa forma, permeiam a vida humana[33] direta ou indiretamente.

Para tanto, vários são os setores abarcados pela aplicabilidade das TIC,[34] através do princípio da integração ambiental, e a favor de soluções urbanas inteligentes que possam conciliar a qualidade de vida da população com um ambiente sustentável. Quais sejam, uma melhor gestão do uso dos transportes, da água e dos resíduos, da monitorização do consumo de energia, da iluminação pública,[35] com lâmpadas

[28] R. Hollands, "Will the Real Smart City please Stand up?", *City*, vol. 12, nº 3 (2008): 303-320.

[29] Rudolf Giffinger e Haindlmaier Gudrun, "Smart cities ranking: an effective instrument for the positioning of the cities?", *ACE: Architecture, City and Environment*, vol. 4, nº 12 (2010): 7-26.

[30] Vide página da Comissão Europeia, na internet, dedicada a informar sobre as políticas ambientais da União Europeia disponível em: http://ec.europa.eu/environment/index_en.htm.

[31] Segundo Wolfram, "the idea of the 'smart city' emerges from linking the ontological and epistemological perspectives of the innovation system with those of the digital city. Hence, a 'smart city' is conceived of as a specific type of innovation system, namely one that is deeply rooted in urban spaces, their institutions and actor networks, while also fostering the use of novel web-based ICT applications to support the pertinent interaction processes, learning and creativity", em Marc Wolfram, "Deconstructing Smart Cities: An Intertextual Reading of Concepts and Practices for Integrated Urban and ICT Development", *Re-Mixing The City Towards Sustainability and Resilience Proceedings Tagungsban*, eds. Manfred Schrenk, Vasily V. Popovich, Peter Zeile, Pietro Elisei, (Vienna: RealCorp, 2012), 174.

[32] O conceito de *smart* city segundo Andrea Caragliu, Chiara Del Bo & Peter Nijkamp : "[…] when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance" cf. Andrea Caragliu, Chiara Del Bo e Peter Nijkamp, "Smart Cities in Europe", *Journal of Urban Technology*, vol. 18, issue 2 (2011): 65-82, DOI: 10.1080/10630732.2011.601117.

[33] H. Couclelis, "The construction of the digital city", *Environment and Planning: Planning and Design*, vol. 21 (2004): 5–19.

[34] Caragliu, Del Bo e Nijkamp, "Smart cities in Europe", 65–82.

[35] A Navigant Research, empresa de consultoria e pesquisa de mercado que fornece uma análise detalhada de energia limpa, inteligente, móvel e distribuída, estima que o mercado global de iluminação de rua inteligente atinja o valor de 837,4 milhões de dólares em 2018. Espera-se um crescimento da receita anual proveniente da área de iluminação de rua inteligente para cerca de 8,3 mil milhões de dólares

que consomem menos energia, da redução de partículas contaminadoras do ar atmosférico, etc., enfim, medidas aplicadoras de políticas ambientais dentro de um contexto tecnológico proporcionado pelas cidades inteligentes.

Todavia, há de ser levada em consideração que a iniciativa de construção de cidades inteligentes tem, no mesmo plano de criar um ambiente socioeconomicamente sustentável, a necessidade de se ter uma fonte potencial de dados.

4. A interoperabilidade da cidade inteligente na dimensão da proteção de dados pessoais

Muito embora a ideia de cidade inteligente permeie a política ambiental da União há algum tempo[36], apenas recentemente, com o advento do RGPD da União Europeia – Regulamento (EU) 2016/679 -, os planejadores urbanos, designadamente ao se tratar da construção das *smart cities*, se puseram a pensar sobre o impacto da inovação tecnológica na privacidade e na proteção de dados pessoais.

É bem verdade que não existe um único conceito para definir cidades inteligentes. No entanto, o ponto comum visto nas definições diz respeito à utilização das TIC na implementação ou no aperfeiçoamento de serviços nas cidades. Ou seja, um retrato característico de *smart city* aponta uma interligação perceptível de uma sequência de aplicações tecnológicas, com o fito de incrementar o gerenciamento dos recursos de interesse para a cidade e para os cidadãos[37]. É a chamada interoperabilidade.

Ou seja, deve-se levar em consideração que, por trás de uma tentativa de conceituar a cidade inteligente, a ideia de interoperabilidade tecnológica deve estar presente, tendo em conta a necessidade de se conectarem os diversos sistemas de informação que uma cidade possa ter em sua rede de comunicação.

Sobre a conceituação de interoperabilidade, não existe uma definição singular, mas pode ser considerada como a "capacidade de suportar diferentes tecnologias, dispositivos e mecanismos de captura de informações e padrões de comunicação, assim como outros sistemas de informação internos/corporativos/e (ou) externos"[38].

No contexto da União Europeia, a Decisão (UE) 2015/2240[39], que institui o

---

a nível global até 2027. Informações disponíveis em: https://www.signify.com/pt-pt/our-company/news/press-releases/2018/20180719-navigant-research-ranks-signify-global-leader-for-smart-street-lighting.

[36] A política europeia do ambiente remonta a 1972 – Cimeira em Paris, França – quando os Chefes de Estado e de Governo definiram novos domínios de ação comunitária, nomeadamente, a necessidade de uma política ambiental comunitária que acompanhasse a expansão econômica e apelaram à elaboração de um programa de ação.

[37] Comentário retirado do artigo "Um panorama de proteção de dados para as cidades inteligentes", *AB2L*, Julho 26, 2018, https://www.ab2l.org.br/um-panorama-de-protecao-de-dados-para-as-cidades-inteligentes/.

[38] Conceito retirado da "Plataforma Integral de Ciudad Inteligente" que dispõe sobre a "Norma UNE 178104 - Sistemas Integrales de Gestión de la Ciudad Inteligente: edición de la norma em España, orientada a definir las capacidades, componentes y requisitos de una Plataforma Integral de Ciudad como sistema centralizado de información y sus requisitos de interoperabilidad, en la que se establece la necesidad de una plataforma o sistema operativo de la ciudad que permita facilitar los servicios a los ciudadanos, a la vez que procurar la máxima eficiencia y una fácil integración em el entorno", disponível em: https://onesaitplatform.atlassian.net/wiki/spaces/OP/pages/30638098/Soporte+de+norma+AENOR+UNE-178104+de+Plataforma+Integral+de+Ciudad+Inteligente e https://www.esmartcity.es/2017/07/14/norma-une-178104-interoperabilidad-plataformas-de-ciudades-inteligentes-informacion-publica. (tradução livre)

[39] Decisão (UE) 2015/2240 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações

"Programa ISA²",[40] prevê "facilitar a cooperação entre os Estados-Membros através da aplicação de soluções de interoperabilidade transfronteiriças e intersetoriais que permitam tornar os serviços públicos mais eficientes e mais seguros".[41]

Nesse sentido, Alessandra Silveira e Joana Covelo de Abreu apresentam as três diferentes dimensões que a doutrina[42] concebeu acerca do conceito de interoperabilidade, ao abrigo da Decisão (UE) 2015/2240. Vejamos:

> The definition of interoperability adopted under the Decision aims to accommodate three different dimensions that doctrine was able to devise:
> 1) 'Technical Interoperability': to illustrate '[t]echnological characteristics and elements that link information systems, such as interconnection services, data integration services, and communication protocols';
> 2) 'Semantic Interoperability': to explain that different organizations are able to understand the meaning of the exchanged information – '[i]t is usually associated with classification systems, ontologies, and data formats'; and
> 3) 'Organizational Interoperability': to stress the need to settle and ascertain common goals between integrated services.[43]
>
> Na mesma linha, Joana Covelo de Abreu aponta que:
>
> In this context, interoperability stands for *"the ability of disparate and diverse organizations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between organizations, through the business processes they support, by means of the exchange of data between their respective ICT systems"*. It demands and implies an effective interconnection between digital components where standardization *"has an essential role to play in increasing the interoperability of new technologies within"* the Digital Single Market. It aims to facilitate access to data and services in a protected and interoperable environment, promoting fair competition and data protection.[44]

Em síntese, nota-se que o entrosamento de sistemas de informação e dos serviços de dados, designadamente das Administrações Públicas dos Estados-Membros[45], bem como a "*abordagem intersectorial, ligações além-fronteiras, não só entre as*

---

públicas, as empresas e os cidadãos europeus (Programa ISA2) como um meio para modernizar o setor público (Texto relevante para efeitos do EEE).

[40] A propósito, "O Programa ISA² apoia o desenvolvimento de soluções digitais que permitem às administrações públicas, empresas e cidadãos da Europa beneficiarem de serviços públicos transfronteiriços e intersetoriais interoperáveis", conceito retirado de: https://ec.europa.eu/isa2/isa2_en (tradução livre).

[41] Vide Considerando (1) da Decisão (UE) 2015/2240 em: https://eur-lex.europa.eu/eli/dec/2015/2240/oj.

[42] Cfr. Carlos E. Jiménez-Gómez and Mila Gascó-Hernández, *Achieving open justice through citizen participation and transparency* (New York: Hershey, 2017), 160, citado por Alessandra Silveira e Joana Covelo Abreu, "Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Governance paradigm", *European Journal of Law and Technology*, vol. 9, n. 1 (may. 2018), http://ejlt.org/article/view/590/827.

[43] Vide Silveira e Abreu, "Interoperability solutions under Digital Single Market".

[44] Cfr. Joana Covelo de Abreu, "Digital Single Market under EU political and constitutional calling: European electronic agenda's impact on interoperability solutions", *UNIO – EU Law Journal*, vol. 3, n. 1 (2017), 127, http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%203/UNIO%203%20EN/Joana%20Covelo%20de%20Abreu%20(1).pdf.

[45] Cfr. Joana Covelo de Abreu, "O Mercado Único Digital e a interoperabilidade administrativa: a proteção de dados pessoais na articulação entre administrações públicas nacionais e as instituições e órgãos da União Europeia – reflexões prospectivas", *O Direito Administrativo nos 30 anos da Constituição Brasileira de 1988 - Um diálogo luso-brasileiro,* coord. Carla Amado Gomes, Ana Fernanda Neves, Eurico Bitencourt

administrações públicas, mas também entre estas e os cidadãos e as empresas, mais eficientes",[46] são elementos necessários para a garantia da interoperabilidade pretendida pela União no caso da efetivação dos projetos de cidades inteligentes.

Todavia, a grande preocupação é de que forma os dados pessoais dos cidadãos, em um sistema de *smart city*, estariam protegidos, tendo em conta o alto risco do cruzamento de dados alicerçados numa estrutura de plataformas digitais unificadas, ao por em ameaça a expectativa de privacidade dos dados pessoais.[47]

Ora, impensável deve ser a construção de uma cidade inteligente sem a percepção da criação de padrões de interoperabilidade e que incluam soluções de segurança da informação.

Ademais, provedores de soluções de cidades inteligentes, fornecedores, funcionários da administração pública dos Estados-Membros e desenvolvedores precisarão eventualmente responder às perguntas centrais: quem será o proprietário dos dados? Quem tem acesso aos dados? O que pode ser feito com os dados?

Para tanto, a resposta a essas perguntas, dentro da comunidade europeia, deverá seguir as atuais regras do RGPD, onde define, já no Considerando nº 1(um), que:

> A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, nº 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

Vê-se que há a necessidade de se partir da definição de padrões e critérios que levem em conta a privacidade e segurança da informação para sistemas a serem implementados com cautela, dentro dos projetos das cidades inteligentes.

Do ponto do projeto de uma cidade inteligente, esta deve estar em conformidade, então, com o RGPD, posto que, diante de um imenso catálogo de dados que as administrações públicas, privadas, bem como parcerias público-privadas[48] têm e terão, tal regulamento, vanguarda em seus dispositivos, norteará cada projeto de cidade inteligente, o qual será avaliado para identificar quaisquer riscos de gerenciamento de dados pessoais e estratégias de mitigação necessárias antes do início do projeto.

As avaliações de impacto em relação à proteção de dados deverão ser conduzidas logo na gênese dos projetos das *smart cities*, cujos dados coletados para a interoperabilidade dos sistemas devem ter, de forma transparente, um propósito em benefício do cidadão e da cidade, em conformidade com o RGPD.

Nesse panorama, tem de se ponderar que a apreciação sistemática dos aspectos

---

Neto e Fabricio Motta (Lisboa: ICJP/CIDP, 2019), 213-214, https://www.icjp.pt/publicacoes/pub/1/17698/view.

[46] Cfr. Sophie Perez Fernandez, "Mercado Único Digital e coordenação dos sistemas de segurança social – soluções de interoperabilidade ao serviço da proteção social", *UNIO - EU Law Journal*, vol. 4, n. 2 (Julho, 2018): 24, http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Sophie%20Perez%20Fernandes.pdf.

[47] Vide Danilo Doneda, "Um panorama de proteção de dados para as cidades inteligentes", *Jota*, (Julho, 2018), https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/um-panorama-de-protecao-de-dados-para-as-cidades-inteligentes-04072018.

[48] Um exemplo de abordagem de parceria público-privada é o projeto em curso da Sidewalk Labs com o governo da cidade de Toronto/CA. O projeto trata-se do Sidewalk Toronto que "combinará o design urbano com visão de futuro e a nova tecnologia digital para criar bairros centrados nas pessoas que alcançam níveis de sustentabilidade, acessibilidade, mobilidade e oportunidades econômicas" (tradução livre), disponível em: https://sidewalktoronto.ca/.

das pessoas singulares,[49] quando da coleta de dados pessoais, e possivelmente utilizados pelas novas tecnologias no âmbito da construção de cidades inteligentes, deve estar inteiramente em conformidade com os pressupostos da avaliação dispostos no artigo 35º, nº 7, do RGPD.[50]

Aliás, a fim de se evitar o uso indevido dos dados pessoais, há de ser plenamente observado o princípio da transparência[51] por parte dos sujeitos – sejam públicos, sejam privados – responsáveis pelo tratamento desses dados, haja vista necessidade do diálogo entre tais sujeitos e as autoridades de controle (constitucional, organizacional e administrativa) nos Estados-Membros.[52]

Assim, ao pensar num projeto de cidade inteligente no âmbito europeu, há de se ter em conta que, alicerçado no princípio da integração ambiental, o qual norteia a aplicação das políticas ambientais da União, visando ao desenvolvimento econômico, social e ambiental, não se pode ir na contramão, outrossim, da nova legislação europeia, designadamente o RGPD, ao unir soluções tecnológicas e soluções sustentáveis para a construção de espaços urbanos.

5. Considerações finais

A edificação das políticas ambientais da União Europeia, através da transversalidade do princípio da integração ambiental, tem delineado a construção de cidades inteligentes nos diversos Estados-Membros, com cunho de sustentabilidade e união das tecnologias digitais e da informação para a execução de projetos que direcionem uma melhor qualidade de vida para a população e, na mesma dimensão, um ambiente equilibrado.

Embora não seja uma realidade de toda a população europeia, a operação de planos de espaços urbanos inteligentes, em benefício da ampliação do desenvolvimento econômico e socioambiental dos Estados-Membros, ainda enfrenta desafios em adaptar e harmonizar os serviços das administrações públicas no desígnio da construção de uma *smart city* em relação aos direitos dos cidadãos. Ou seja, o uso de dados e de ferramentas digitais em sistemas de informação interoperáveis – pilares de uma cidade inteligente -, a fim de evitar violações de direitos, tais como a proteção de dados pessoais.

Além disso, há de se ter em vista que, para alcançar a viabilidade prática das *smart cities*, é necessário, ao menos, um equilíbrio entre interesses individual e coletivo no planejamento, monitoramento e tratamento de dados pessoais. Para tanto, tem de se acatar, no cumprimento dos atos administrativos público-privados, o princípio da

[49] Cfr. Artigo 35º do RGPD.

[50] Artigo 35º, nº 7, do RGPD: A avaliação inclui, pelo menos: a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento; b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos; c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.o 1; e d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

[51] A propósito, vide informações sobre condições e tratamento de dados pessoais em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_pt.

[52] Cfr. Considerandos nºs 36, 117 e 119 do RGPD.

transparência, a garantia da publicidade ("*a publicidade é requisito de eficácia e moralidade*")[53] pelas autoridades de controle e o acesso de dados pessoais aplicados ao território inteligente, uma vez que o cumprimento desses padrões dependerá, em certa medida, do respeito aos direitos tanto coletivos, como individuais.

Dessarte, o princípio da integração ambiental, na aplicação das políticas da União, está intrinsicamente ligado à ideia de construção das cidades inteligentes, onde são criados conceitos, dimensões e modelos que incorporam, de certa forma, o caráter transversal da sustentabilidade. E mais: ainda através do uso de instrumentos tecnológicos digitais e de comunicação, dentro de um conceito de interoperabilidade, não se pode descuidar da conciliação entres as ideias de sustentabilidade e de privacidade dos dados coletados, na tentativa de reunir o equilíbrio entre colher os benefícios das oportunidades de inovação em movimento rápido e entregar esses benefícios de longo prazo a todos os cidadãos.

[53] Segundo Hely Lopes Meirelles, *Direito administrativo brasileiro* (São Paulo: Malheiros Editores, 1993), 86 *apud* José Afonso da Silva, *Curso de Direito Constitucional Positivo* (São Paulo: Malheiros, 2006), 670.

A inteligência artificial e a questão constitucional

Larissa Coelho*

RESUMO: A tecnologia no futuro será uma fonte de poder ou um meio para o exercício do poder? Esta é a questão que nos guia neste artigo, tendo como ponto de partida a leitura de dois teóricos da sociologia constitucional, Gunther Teubner e Ferdinand Lassalle, que embora tenham um século de distância entre os seus estudos dedicam-se à análise das metamorfoses sociais e do poder. Assim, objetiva-se examinar, no quadro dos novos problemas constitucionais, se a tecnologia em específico, com referência à inteligência artificial, pode ser associada ao conceito de fator de poder, num período dominado pela digitalização, privatização e globalização subjacente ao pensamento da constitucionalização da sociedade numa perspetiva multinível e em virtude das modificações que a revolução digital vem causando na organização social.

PALAVRAS-CHAVE: *Fatores de poder – Constitucionalismo – Tecnologia – Inteligência artificial – Gunther Teubner – Ferdinand Lassalle*

ABSTRACT: Will the technology be a source of power in the future or a means to the exercise of power? This is the question that guides us in this article, starting with the reading of two theorists of constitutional sociology, Gunther Teubner and Ferdinand Lassalle. Despite their studies being a century apart, they are dedicated to the analysis of the social metamorphoses and the power. Thus, the objective is to examine, within the framework of the new constitutional problems, whether specific technology, regarding artificial intelligence, can be associated with the concept of power factor, in a period dominated by the digitization, privatization and globalization underlying the thought of the constitutionalisation of the society in a multilevel perspective and due to the changes that the digital revolution has been causing in social organization.

KEYWORDS: Power factors – Constitutionalism – Technology – Artificial intelligence – Gunther Teubner – Ferdinand Lassalle

* Doutoranda em Ciências Jurídicas Públicas pela Universidade do Minho. Investigadora do Centro de Investigação em Justiça e Governação (JusGov). Bolsista pela Fundação para a Ciência e a Tecnologia – FCT. Este texto tem por inspiração os debates decorridos no Grupo de Leitura Às Margens do Texto – GLMAT, da Escola de Investigadores do JusGov/UMinho, a que tive a honra de coordenar no primeiro semestre do ano de 2019.

O século XXI inicia-se exigindo um reexame do paradigma constitucional. Perto de completar cerca de 245 anos de existência, o constitucionalismo clássico, fruto das revoluções do século XVIII, depara-se com uma série de mudanças no âmbito político, económico e social que obrigam a que este seja pensado para além da figura do Estado-Nação. A este processo soma-se um novo fator que passa por demarcar o espaço e a confrontar o constitucionalismo: a revolução tecnológica, que se acopla ao remo da globalização, promovendo mudanças na forma do homem estar e atuar na sociedade.

Face a este cenário questionamos se a tecnologia, no futuro, será uma fonte de poder ou um meio para o exercício do poder, tendo como ponto de partida a leitura de dois teóricos da sociologia constitucional, Gunther Teubner e Ferdinand Lassalle, que embora tenham um século de distância entre seus estudos, dedicam-se à análise das metamorfoses sociais e do poder. Justificando-se este aporte teórico no fato de Lassalle ser o cérebro que desenvolve a conceção sociológica da constituição, para a qual relevam os "[…] fatores sociais que condicionam o exercício do poder",[1] enquanto Teubner desponta como um dos principais nomes a desenvolver esta teoria na atualidade, sobretudo e em função das atuais tendências multiníveis e da descentralização do poder que rondam o constitucionalismo. Assim, objetiva-se examinar, no quadro dos novos problemas constitucionais, se a tecnologia em específico, com referência à inteligência artificial, pode ser associada ao conceito do fator de poder, num período dominado pela digitalização, privatização e globalização subjacente ao pensamento da constitucionalização da sociedade numa perspetiva multinível e em virtude das modificações que a revolução digital vem causando na organização social.

Sendo certo que o constitucionalismo clássico fora outrora também, ele próprio, um marco na história do homem, por moldar a forma deste ser e estar em sociedade, é considerado por Maurizio Fioravanti como um dos períodos "mais decisivos na história do constitucionalismo" por inaugurar um "novo conceito e uma nova prática",[2] ilustrado numa constituição escrita, garante dos direitos fundamentais, da separação de poderes, do governo representativo, da limitação do poder governamental, da responsabilidade política e pela independência dos tribunais, herança da Declaração de Direitos da Virgínia de 1776 e que hoje completa cerca de 245 anos.

Para Horst Dippel, os princípios do constitucionalismo moderno tiveram origem na pergunta: como a liberdade individual poderia assegurar-se permanentemente contra as intervenções do governo? E durante esse período, pelo menos no mundo ocidental, nenhuma Constituição se atreveu a questionar ou a desafiar os princípios do constitucionalismo clássico. Pelo contrário, a sua incorporação nos diversos textos constitucionais transforma o constitucionalismo moderno, ou melhor, os elementos do constitucionalismo moderno, de uma ideia franco-americana num fenómeno transnacional, cuja repercussão se dá globalmente.[3]

E diante de tais observações Dippel conclui que, apesar dos estudos sobre o constitucionalismo no geral e o seu impacto em diversos países, estamos no tempo em que é necessário reescrever-se a história do constitucionalismo, nas suas palavras, uma "história do constitucionalismo moderno [que] deliberadamente se torna alheia

[1] Cfr. Jorge Miranda, *Manual de direito constitucional*, 7ª ed., Tomo II (Coimbra: Coimbra Editora, 2013), 71.
[2] Cfr. Maurizio Fioravanti, *Costituzione* (Bolonia: Il Mulino, 1999), 102.
[3] Cfr. Horst Dippel, "Constitucionalismo moderno. Introducción a una história que necessita ser escrita", *Historia Constitucional*, n.º 6 (septiember, 2005): 183-190.

aos passos da história do constitucionalismo nacional e se inicia numa perspectiva global". Sendo que "[…] [t]udo o que necessitamos é de uma nova leitura, que promete abrir um enorme espaço, de novos panoramas".[4]

E é neste seguimento, na busca por se deslindar novos panoramas, consoante afirma Dippel, ou dos novos desenhos constitucionais como escreve Gomes Canotilho,[5] que os atuais movimentos constitucionais, como o constitucionalismo multinível, a interconstitucionalidade, o constitucionalismo societário, o constitucionalismo cooperativo e o transconstitucionalismo visam dar respostas aos novos problemas constitucionais.[6]

Problemas esses que surgem: i) das mudanças sociais, ii) das transformações do globo promovida pelo homem, como por exemplo as questões ambientais, iii) nas mudanças do próprio homem em função das transformações do globo, no qual podemos citar a problemática dos refugiados ambientais, iv) nos problemas que advêm do desenvolvimento geoestratégico como as migrações, as políticas de segurança e os conflitos armados, v) das interações e intervenções económico-financeiras e iv) do desenvolvimento tecnológico, base esta para uma nova revolução: *a revolução digital*, que permite o *upgrade* do próprio homem, enquanto *homo digitalis* e que abre a porta para o emergir de uma nova escrita da história do constitucionalismo, sob o signo dos direitos fundamentais na era digital. Isto porque, como salienta Klaus Schwab, a revolução tecnológica apresenta desafios e transforma toda a sociedade, visto que altera a maneira como "[…] vivemos, trabalhamos e nos relacionamos", e conforme argumenta o autor, encontramo-nos perante a fusão dos mundos "físico, digital e biológico",[7] consequentemente novos paradigmas passam a ser anunciados e questões são colocadas aos até então existentes.

E em razão destas transformações, ou, para utilizarmos a expressão de Ulrich Beck, *metamorfose,*[8] muitas são as questões que se levantam[9], as quais ainda não conseguimos dar respostas. E, com o intuito de contribuir para o desenvolvimento científico desta matéria é que apresentamos a seguinte questão: poderíamos considerar que a tecnologia no futuro será uma *fonte de poder* ou apenas um *meio* para o exercício do poder? Isto porque, a revolução digital iniciada entre as décadas de 1970-80 do século passado "[…] não se refere apenas a máquinas e sistemas inteligentes e conectados. O seu alcance é muito mais vasto". Assim, a "segunda era da máquina"[10]

---

[4] Cfr. Dippel, "Constitucionalismo moderno", 199 (tradução nossa).

[5] Cfr. J. J. Gomes Canotilho, *Direito Constitucional e Teoria da Constituição*, 7ª ed. (Coimbra: Almedina, 2003).

[6] Sobre os movimentos constitucionais ver: Larissa A. Coelho, "O constitucionalismo para o século XXI", in *Encontro de Investigadores EDUM 2018*, org. Larissa Coelho, Ana Carolina Cohen, Maria João Lourenço e Raphaela Toledo (Braga: Escola de Direito da Universidade do Minho, 2019), 81-92 e Larissa A. Coelho, "O ensino do direito constitucional na era da globalização", in *Desafios do ensino jurídico no século XXI*, org. Fabrício Veiga Costa, Ivan Dias da Motta, Sérgio Henrique Zandona Freitas (Maringá, Pr: IDDM, 2018), 361-387.

[7] Cfr. Klaus Schwab, *A quarta revolução industrial* (Oeiras: Levoir, 2017), 5.

[8] Cfr. Ulrich Beck, *A metamorfose do mundo*, trad. Pedro Elói Duarte (Lisboa: Edições 70, 2017).

[9] A título de exemplo, Klaus Schwab (*A quarta revolução*, 6-7) apresenta uma série de questões que tem assolados os cientistas das mais variadas áreas, dentre eles os cientistas do direito, que têm por base sobremaneira as seguintes interrogações: "como é que a tecnologia está a mudar as nossas vidas e as das gerações futuras" e/ou "como é que [a tecnologia] está a reformular o contexto económico, social, cultural e humano em que vivemos". Isto porque, justifica o autor, "[e]sta revolução não está apenas a mudar o ´que` fazemos e o ´como` fazemos mas também ´quem` somos".

[10] Cfr. Erik Brynjolfsson e Andrew MacAfee, *The Second Machine Age: Work, Progress and Prosperity in a Time of Brilliant Technologies* (New York: W.W. Norton & Company, 2014).

apresenta uma tecnologia ainda mais sofisticada e integrada, na qual os *hardwares* e os *softwares* "transformam as sociedades e a economia global".[11]

Dentre os vários desenvolvimentos atuais da tecnologia,[12] importa-nos para o presente estudo destacar a *inteligência artificial*, considerada pela Comissão Europeia como a "[…] tecnologia mais estratégica do século XXI".[13] A inteligência artificial, popularmente conhecida pela sua sigla IA, foi definida no documento apresentado em abril de 2019, pelo Grupo de Peritos de Alto Nível sobre Inteligência Artificial (GPAN IA), criado pela Comissão Europeia, como sendo um "[…] sistema de software (e eventualmente também de hardware) concebido por seres humanos […]" que recebem um objetivo complexo, atuando "[…] numa dimensão física ou digital […]" com vista à "[…] aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido".[14]

Simplificando sua definição, a inteligência artificial consiste num sistema que apresenta "[…] um comportamento inteligente, analisando o seu ambiente e tomando medidas – com um determinado nível de autonomia – para atingir objetivos específicos".[15] A sua aplicação tem sido observada, principalmente, na criação de veículos autónomos, assistentes virtuais, motores de busca na internet, drones e *softwares* de tradução, que têm na sua base a capacidade para processar e disponibilizar uma grande quantidade de dados,[16] mas que, embora tenha sido criada pelo homem, não depende deste para a prossecução dos seus fins, pelo contrário, "[m]uitos destes algoritmos aprendem a partir de pistas com 'migalhas' de dados que nós deixamos no mundo digital", uma vez que fundamentam-se na "[…] 'aprendizagem automática' e detecção automatizada que permitem a computadores e robôs 'inteligentes' autoprogramar-se […]" com a finalidade de "[...] encontrar as melhores soluções a partir de princípios iniciais".[17]

Em função deste entendimento, quanto à capacidade desses *softwares* de recolherem e tratarem os dados autonomamente, a partir da aplicação da aprendizagem automática, é que questionamos se não estaríamos a desenvolver uma tecnologia com

[11] Cfr. Schwab, *A quarta revolução*, 10.

[12] Podemos citar como ilustração aos novos desenvolvimentos da tecnologia o sequenciamento genético, a nanotecnologia, as energias renováveis, a computação quântica, a inteligência artificial e a aprendizagem automática. Essas são as principais matérias que compõe a Revolução 4.0 que suplanta a descoberta dos computadores (Terceira Revolução Industrial); da produção em massa (Segunda Revolução Industrial) e dos caminhos de ferro e da máquina a vapor (Primeira Revolução Industrial). A tecnologia do século XXI caracteriza-se pela capacidade de criar "[…] objectos que são continuamente mutáveis e adaptáveis" cf. Schwab, *A quarta revolução*, 9-13.

[13] Cfr. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Inteligência artificial para a Europa.* 25.04.2018 (COM (2018) 237 final), 2, https://ec.europa.eu/transparency/regdoc/rep/1/2018/PT/COM-2018-237-F1-PT-MAIN-PART-1.PDF.

[14] Cfr. Grupo de Peritos de Alto Nível sobre a Inteligência Artificial – GPAN IA, *Orientações éticas para uma IA de confiança* (Bruxelas: Comissão Europeia, 2019), 47, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[15] Cfr. Comissão Europeia, COM (2018) 237 final, 1.

[16] Cfr. Schwab, *A quarta revolução*, 13. Para além da aplicação descrita acima, a inteligência artificial tem sido empregue no tratamento de doenças crónicas, nos serviços de emergências médicas, na redução das taxas de mortalidade em acidente de viação, na agricultura e pecuária, na luta contra as alterações climáticas e na prevenção a ameaças à cibersegurança, cf. Comissão Europeia, COM (2018) 237 final, 1.

[17] Cfr. Schwab, *A quarta revolução*, 13-14.

capacidades tais de exercer o poder, ou ainda, se de tornar um meio para o exercício do poder, o que em linguagem jurídico-constitucional significa ser esta tecnologia um ator que influencia a interpretação e a criação de normas constitucionais, o que a doutrina classifica como fator social de poder, colocando-nos no âmbito das mudanças promovidas por fontes constitucionais não formais.[18]

E esta questão coloca-se na esteira do cruzamento do estudo de dois teóricos do constitucionalismo que perfazem uma análise sociológica da constituição, Gunther Teubner e Ferdinand Lassalle, visto que afastam a análise de uma visão purista do Direito, com objetivo de observar a confluência de fatores sociais e jurídicos.[19]

E, desenvolvendo a questão, Lassalle, em seu discurso Über *Verfassungswesen*, proferido em Berlim, no ano de 1862, em referência aos acontecimentos decorrentes da Revolução de Março de 1848 e da Constituição alemã de 1850, além de tecer críticas ao sistema antidemocrático da Constituição prussiana, identificava que uma Constituição, para que não seja uma folha de papel, deve refletir a *soma dos fatores reais de poder*.[20] Isto porque, para Lassalle, os problemas constitucionais são problemas de poder e, para o autor, os fatores reais de poder são capazes de modificar a sociedade, ou seja, são os sujeitos ou as instituições que influenciam a sociedade e a sua organização, como também, o sentido a ser dado à interpretação da Constituição, visto que são esses fatores que nos permitem identificar *quem* detém o poder, bem como os seus interesses no âmbito económico, social e político. Nas palavras do autor, os fatores reais de poder "[…] que vigoram no seio de cada sociedade constituem essa força activa e eficaz que informa todas as leis e instituições jurídicas da sociedade […]".[21] No contexto desta obra esses fatores correspondiam à monarquia, à aristocracia, à grande burguesia, aos banqueiros e à classe operária.[22]

Atualmente, observarmos o discurso de Gunther Teubner sobre a tese do constitucionalismo societário, cujo estudo desenvolve-se com base em David Sciulli, que pretendia construir um "[…] quadro conceitual que permitisse analisar e compreender as organizações e instituições da sociedade que influenciam o sentido das mudanças sociais, no contexto de um Estado […]".[23] Trazendo esta tónica para o campo jurídico, Teubner identifica que vivenciamos um período em que há uma transferência do poder político para atores privados, no qual se transmite para diversas instituições que atuam fora do domínio público certas políticas dos Estados. Comportamento que se fundamenta na busca por respostas aos três grandes problemas atuais, quais sejam, a digitalização, a privatização e as redes globais, o

[18] Cfr. Carlos de Cabo Martín, *Contra el consenso: estúdios sobre el estado constitucional y el constitucionalismo del Estado Social* (Ciudad de México: Universidad Nacional Autónoma de México, 1997), 189.

[19] Sobre a sociologia constitucional consultar também: Chris Thornhill, *A Sociology of Constitutions: Constitutions and State Legitimacy in Historical-Sociological Perspective* (New York: Cambridge University Press, 2011); Chris Thornhill, "Towards a historical sociology of constitutional legitimacy", *Theory and Society*, vol. 37, n.º 2, (2008): 161-197. Sobre a sociologia constitucional transnacional consultar: Chris Thornhill, *A sociology of Transnational Constitutions: social foundations of the post-national legal structure* (London: Cambrigde, 2016); Marcelo Neves e Maurício Palma, *Sociologia constitucional e governança global* (Rio de Janeiro: Lumen Juris, 2018) e Alberto Febbrajo, *Sociologia do constitucionalismo: constituição e teoria dos sistemas* (São Paulo: Juruá, 2016).

[20] Cfr. Ferdinand Lassalle, *O que é uma Constituição?* (Lisboa: Escolar Editora, 2013).

[21] Cfr. Lassalle, *O que é uma Constituição*, 76.

[22] Cfr. Lassalle, *O que é uma Constituição*, 77-82.

[23] Cfr. Mariana Rodrigues Canotilho, "O princípio do nível mais elevado de protecção em matéria de direitos fundamentais" (Dissertação de Mestrado, Universidade de Coimbra, 2008), 53 e David Sciulli, *Theory of Societal constitutionalism* (Cambridge: Cambridge University Press, 1992).

que nos coloca diante de uma *nova questão constitucional*, visto que convivemos com a descentralização da política no contexto da sociedade mundial.[24]

Para Teubner, esses atores correspondem à economia, ciência e tecnologia, educação, organizações não governamentais, grupos financeiros, empresas multi e transnacionais e corporações, em que cada ator, ou nas palavras do autor, subsistema, teria a sua própria constituição – constituição civil parcial – que em conjunto conformaria a constituição civil global, na qual se congrega as decisões de política global, posto que, conforme argumenta Teubner devemos "[…] repensar la constitución en dirección a la globalidad política, teniendo en cuenta el proceso interestatal […]".[25]

Ora, os *atores privados* identificados por Teubner seriam, a nosso ver, uma atualização da leitura dos *fatores sociais* apontados por Lassalle, que passam, por sua vez, a deter ou partilhar o poder e, consequentemente, a influenciar a interpretação da Constituição e da organização social. Neste sentido, Teubner reconhece a tecnologia enquanto fator de poder ao afirmar que os embates advindos das tentativas de regulação estatal em função da ciberanarquia e do mercado digital, são conflitos político-constitucionais de primeira categoria, cujo desenvolvimento lentamente afirma uma organização a que classifica como de um direito a uma constituição digital.[26] Como exemplo desta realidade podemos citar o Regulamento Geral de Proteção de Dados[27] enquanto implemento jusconstitucional no Mercado Único Digital por parte da União Europeia no que diz respeito ao tratamento de dados pessoais e a circulação desses dados promovida tanto por agentes públicos, como por privados.

Assim, neste cenário, verificamos que a tecnologia, e em específico, a inteligência artificial, vem modificando a forma do homem *estar* e *atuar* na sociedade, muitas vezes substituindo-se a este ou interagindo com ele e, ao mesmo tempo, gerando uma nova divisão social entre os *infoincluídos* e os *infoexcluídos*, o que nos coloca novamente (como há cerca de 200 anos atrás) diante de um *novo conceito* e de uma *nova prática constitucional*.

No que toca à interação entre essa tecnologia e os direitos fundamentais acompanhamos uma célere e direta aproximação. Para tanto, numa rápida consulta pelo programa mais popular da inteligência artificial, o *Google*, encontramos blogueiros,

---

[24] Cfr. Gunther Teubner, "Globalización y constitucionalismo social: alternativas a la teoria constitucional centrada en el Estado", *AFDUAM*, nº 9 (2005): 200-202.

[25] Cfr. Teubner, "Globalización y constitucionalismo social", 202. Para uma melhor compreensão da tese defendida do Gunther Teubner ver os desenvolvimentos sobre a teoria do constitucionalismo societário em: Gunther Teubner, "Globale Zivilverfassungen: Alternativen zur staatszentrierten", *Verfassungstheorie. Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV)*, vol. 63 (2003), http://www.zaoerv.de/63_2003/63_2003_1_a_1_28.pdf e Gunther Teubner, "Reflexões sobre a constitucionalização do sistema de poder mundial", *Revista Brasileira de Sociologia do Direito*, vol. 5, n.º 1, (jan/abr., 2018), http://dx.doi.org/10.21910/rbsd.v5n1.2018.231.

[26] Cfr. Teubner, "Globalización y constitucionalismo social", 204. Ver também: David R. Johnson e David Post, "The New 'Civic Virtue' of the Internet", *First Monday*, vol. 3, n.º 1 (jan., 1998) https://doi.org/10.5210/fm.v3i1.570. Sobre o desenvolvimento de uma política constitucional europeia no âmbito tecnológico ver Joana Covelo de Abreu, "Digital Single Market under EU political and constitutional calling: European electronic agenda's impact on interoperability solutions", *UNIO - EU Law Jounal*, vol. 3, n.º 1 (January, 2017): 123-140, https://doi.org/10.21814/unio.3.1.13.

[27] 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 e que revoga a Diretiva 95/46/CE, *OJ L* 119, 4.5.2016, p. 1–88.

ativistas e académicos com uma visão positiva sobre essa relação, que se fundamenta no fato de um programa de inteligência artificial poder ajudar a gestão da *res pública*, sobretudo potencializando um aumento no índice de satisfação dos cidadãos quando associado à gestão das políticas públicas, por consentir o processamento *exabytes* de informação e a possibilidade de transformar essa informação em indicadores que permitam aos governos perceber o que necessita a sua população, promovendo uma política redistributiva real e equitativa, uma vez que a inteligência artificial dá lugar à resolução dos problemas de alocação dos recursos através do cruzamento de dados.

Por outro lado, num claro exemplo da aplicação da inteligência artificial no âmbito das políticas de liberdade, acompanhamos uma crescente implementação deste sistema nos diversos setores do poder judiciário, que não se restringe apenas a colher e distribuir informações acerca do conteúdo de decisões judiciais, mas especialmente tem sido aplicada para tornar mais célere os processos judiciais, chegando mesmo a uma espécie de substituição do juiz em certas demandas. Sobre esta realidade, David Wilkins explica que, nos Estados Unidos, se tem difundido a utilização da inteligência artificial em substituição aos julgamentos para a determinação da fiança. Segundo Wilkins, o programa decide com base no "[…] aprendizado da máquina sobre todas as decisões anteriores que foram feitas por juízes"[28] para decidir sobre a instauração ou não de audiência.

No entanto, Wilkins chama a atenção para o fato de que, pelo menos nos Estados Unidos, "muitas das decisões anteriores foram resultados de um viés racial" e, especialmente quanto a fiança, afirma ser notório que a sua aplicação se fundamenta em quesitos raciais, logo, conclui que se "[...] construirmos um algoritmo baseado em performances anteriores, vamos levar todo o viés racial para o sistema".[29] Neste mesmo sentido, Jamie Bartlett disserta que um sistema que se alimenta da recolha de dados potencialmente torna-se um caminho para a manipulação, distração e uma progressiva perda da liberdade de escolha e autonomia, defendo que a tecnologia irá destruir a ordem social e a democracia tal qual nós a conhecemos.[30]

Deste modo, ao permitirmos que um *computador inteligente* aprenda, guarde e replique informações, na busca por soluções ótimas, qual será o produto da maturação do arcabouço das informações jurídicas a que tenha contato, especialmente, qual a leitura que fará esse algoritmo dos últimos 200 anos de constitucionalismo? O que aprenderá essa máquina?

Neste cenário, ainda que utópico, alguns dirão que as soluções ótimas do algoritmo refletirão a evolução no campo da proteção dos direitos fundamentais. Porém, lembremos que essa leitura, essa aprendizagem, terá por base não apenas as promessas legislativas, mas a prática, a norma aplicada ou a falta dela, o espírito presente em todas as sentenças judiciais, o que nos poderá mostrar que vivemos sob um sistema corrompido que, em *nome* do Direito e da proteção de direitos fundamentais, se cometem mais atrocidades, que se privilegiam determinadas classes

[28] Entrevista feita a David Wilkins por Mariana Oliveira, "A advocacia vai continuar um negócio de capital humanos, diz vice-reitor de Harvard", *Revista Consultor Jurídico* (2019), https://www.conjur.com.br/2019-mar-30/entrevista-david-wilkins-vice-reitor-direito-harvard. Sobre a utilização de inteligência artificial para a resolução de conflitos jurídicos ver Francisco Carneiro Pacheco Andrade, Davide Carneiro e Paulo Novais, "A inteligência artificial na resolução de conflitos em linha", *Scientia Iuridica*, Tomo LIX, n.º 321 (2010).

[29] Cfr. Oliveira, "A advocacia vai continuar um negócio".

[30] Cfr. Jamie Bartlett, *The People vs Tech: how the internet is killing democracy (and how we save it)* (London: Ebury Press, 2018), 1-11.

ou em que se ignoram as vítimas.

E mais, sabemos que o programa se torna cada vez mais autónomo quanto mais se alimenta, aprende, e assim, como poderemos garantir nossa liberdade face às suas possíveis intervenções? Por isso, e em relação ao exposto, visto que vai-se tornando cada vez mais visível que a revolução digital modifica a forma do homem estar em sociedade é que perguntamos: a tecnologia no futuro será uma *fonte de poder* ou apenas um *meio para o exercício do poder*?

UNIO
EU LAW JOURNAL

APS
ASSOCIAÇÃO PENSAMENTO SÁBIO

Universidade do Minho
Escola de Direito

Cofinanciado pelo
Programa Erasmus+
da União Europeia