UNIO
EU LAW JOURNAL

O paradigma da Justiça eletrónica. Atas da Mesa Redonda de Jovens Investigadores na Spring School eUjust

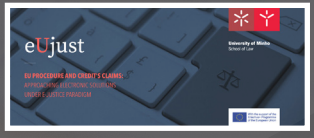
(Coleção UNIO E-book)

Coordenação Científica

Joana Covelo de Abreu
Larissa Coelho
Tiago Sérgio Cabral

Universidade do Minho

With the support of the Erasmus+ Programme of the European Union



INFORMAÇÕES EDITORIAIS

O paradigma da Justiça eletrónica. Atas da Mesa Redonda de Jovens Investigadores na Spring School eUjust
(Coleção UNIO E-book)

Coordenação Científica:
Joana Covelo de Abreu, Larissa Coelho e Tiago Sérgio Cabral

Autores:
Francisco Salvador Gil García | Gonçalo Martins de Matos
Patrícia Pacheco Rodrigues | Pedro Petiz Viana
Samantha Ribeiro Meyer-Pflug Marques

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

Este trabalho é financiado ao abrigo do Módulo *Jean Monnet* "eUjust" – *EU Procedure and credits' claims: approaching electronic solutiosn under e-Justice paradigm*, com o número 611662-EPP-1-2019-1-PT-EPPJMO-MODULE.

ISBN: 978-989-53342-4-7 | DOI: 10.21814/1822.77977

Braga, maio de 2022

ÍNDICE

APRESENTAÇÃO

As atas que agora se publicam correspondem aos trabalhos apresentados e desenvolvidos por investigadores de mestrado e doutoramento, no âmbito da Mesa Redonda de Jovens Investigadores, que decorreu na 3.ª Edição do Curso Intensivo "eUjust: *EU Procedure and credits' claims: approaching electronic solutions under e-Justice paradigm*", promovido sob a forma de *Spring School*, que ocorreu nos dias 14 a 18 de março de 2022, na Escola de Direito da Universidade do Minho, em formato *online*.

A publicação destas atas corresponde a um dos objetivos visados no Módulo *Jean Monnet* com o acrónimo "eUjust" e subordinado ao tema "*EU Procedure and credits' claims: approaching electronic solutions under e-Justice paradigm*", desenvolvido, na Escola de Direito da Universidade do Minho, de setembro de 2019 a agosto de 2022, com a chancela da Comissão Europeia e do Programa ERASMUS+, que conta com a coordenação científica da Prof. Doutora Joana Covelo de Abreu, Professora da mesma instituição, e integrando, na sua equipa, a Prof. Doutora Alessandra Silveira e o Prof. Doutor Pedro Madeira Froufe.

O Módulo eUjust congrega as sensibilidades auscultadas pela equipa que o integra de que, com o estabelecimento de um Mercado Único Digital, a União Europeia começou a votar uma atenção particular às dinâmicas associadas às novas tecnologias de informação e de comunicação ao serviço de uma boa administração da justiça. Tema que ganhou novo fôlego e atualidade com a apresentação, em 2019, do Plano e da Estratégia do Conselho sobre justiça eletrónica europeia, a implementar até 2023.

Por outro lado, apesar de a administração da justiça já se encontrar permeada pelas dinâmicas digitais, ainda se regista um insipiente conhecimento das suas potencialidades, dos seus riscos e das suas vantagens, devendo tal equação partir de um fundamento antropológico, aliás, ínsito ao próprio surgimento e desenvolvimento do direito como ciência autónoma.

Partindo deste mote, a mesa redonda foi um espaço no qual investigadores juniores e seniores tiveram a oportunidade de dialogar e discutir sobre os desafios e paradigmas da justiça eletrónica sob o prisma de diferentes sistemas jurídicos, tendo como escopo os trabalhos de investigação desenvolvidos pelos jovens investigadores.

Deste modo, os trabalhos que agora se apresentam por escrito refletem o tema da justiça eletrónica a partir de uma abordagem tanto teórico-prática, com vista a apontar os desafios que a digitalização tem colocado aos diversos sistemas jurídicos, tendo sido ressaltado, nomeadamente, as relações de consumo e o mercado digital análise feita a partir do sistema jurídico brasileiro, ao passo que no campo europeu as investigações apresentadas tiveram por objeto os desdobramentos da tutela jurisdicional efetiva e o desenvolvimento do sistema e-CODEX; os impactos da inteligência artificial no Direito e da digitalização nas políticas de segurança e os desafios à privacidade.

Joana Covelo de Abreu
Larissa Coelho
Tiago Sérgio Cabral

O adensamento da tutela jurisdicional efetiva operado pela digitalização da justiça como aprofundamento da União de Direito: o papel do e-CODEX

Gonçalo Martins de Matos[*]

0. Introdução

A União Europeia (UE) é perspetivada, nos dias que correm, como uma União de Direito, onde os poderes públicos das instituições europeias se sujeitam ao direito por esta criado. Desta forma, é natural que na UE vigore um princípio estrito de legalidade, impondo-se aos órgãos competentes uma reação adequada contra qualquer sujeito de direito que atente contra as normas de direito da União. Assim, ao submeter as suas instituições ao princípio da legalidade, e garantindo a proteção dos direitos dos particulares, é natural que a UE se organize no sentido de promover meios destinados a garantir uma proteção jurisdicional efetiva dos direitos conferidos aos cidadãos pelo direito da União. Neste contexto, é natural que a ideia de União de Direito seja indissociável da garantia de tutela jurisdicional efetiva, consagrada como princípio fundamental basilar da UE pelo Tratado da União Europeia (TUE) e pela Carta dos Direitos Fundamentais da União Europeia (CDFUE). Este princípio pode ser resumido pela ideia de que a cada direito deve corresponder um meio jurisdicional de o efetivar. Complementarmente, pela própria natureza da integração europeia, uma noção ampla de contencioso da UE leva a que se entendam todos os meios jurisdicionais ao dispor dos sujeitos titulares de direitos como partes integrantes da tutela jurisdicional efetiva consagrada pelo direito da União, a par da integração dos tribunais nacionais, enquanto tribunais funcionalmente europeus, e dos tribunais organicamente europeus numa mesma ordem jurídica europeia.

Num mundo em constante desenvolvimento, é natural que a par de novas situações surjam novos direitos, e com estes a necessidade de os tutelar efetivamente. Olhamos, particularmente, para o novo paradigma preconizado pela justiça eletrónica europeia. As ferramentas inovadoras que a digitalização da justiça oferece permitem-nos explorar de forma absolutamente inédita novas fórmulas de resolução de velhos problemas, entre os quais a questão sempre premente de tutela jurisdicional efetiva. Uma destas mudanças é a corporizada pela criação do sistema e-CODEX, que, como o próprio website indicia, visa "promover o fácil acesso dos cidadãos à justiça transfronteiriça". É através destas novas ferramentas que se torna possível um adensamento sem precedentes da tutela jurisdicional efetiva no seio da UE. E, através deste, a própria conceção de União de Direito sai reforçada, garantindo-se a sua plenitude e aprofundamento na construção de uma sociedade mais justa, livre e igualitária.

[*] Mestrando em Direito Judiciário na Escola de Direito da Universidade do Minho.

Assim, é no intuito de explorar estas questões que damos início ao presente trabalho. Neste, começaremos por abordar em que consiste a verificação de uma tutela jurisdicional efetiva no contexto alargado de uma União de Direito, partindo de seguida para a dissecação das realidades enquadráveis em ambos os conceitos. Num momento posterior, iremos analisar de que forma se concretizam estas realidades através das ferramentas de justiça eletrónica criadas e utilizadas pela UE, com especial enfoque no sistema e-CODEX. Para tanto, iremos abordar o contexto e a evolução das estratégias europeias para a justiça eletrónica e o contexto e evolução da ferramenta e-CODEX, para além de observar os desenvolvimentos mais recentes relativamente a estes dois tópicos.

1. A tutela jurisdicional efetiva no contexto da União de Direito e a sua concretização no contencioso da União Europeia

Com a "*renovação de largo significado para a evolução futura do processo de integração europeia*"[1] operada pela entrada em vigor do Tratado de Lisboa saiu reforçada a ideia de que os Tratados Europeus "*criaram uma ordem jurídica própria, integrada nos sistemas jurídicos dos Estados-Membros e que se impõe aos respetivos órgãos jurisdicionais, cujos sujeitos são […] também os seus nacionais*".[2] Esta perceção da natureza da UE resulta não apenas dos indícios que o processo de integração europeia vai deixando à interpretação da doutrina, mas principalmente dos contributos dos Tribunal de Justiça da União Europeia (TJUE), que tem afirmado que, para além de uma ordem jurídica autónoma, a UE se comporta como uma verdadeira União de Direito, "*na medida em que nem os seus Estados-membros nem as suas instituições estão isentos da fiscalização da conformidade dos seus actos com a carta constitucional de base que é o Tratado*"[3] (na altura, o TJUE referia-se ao Tratado que institui a Comunidade Económica Europeia). Esta citação é retirada diretamente do considerando 23 do emblemático Acórdão *Les Verts*, jurisprudência na qual se detetam as "*bases do reconhecimento da (atual) União Europeia enquanto União de direito e dos tratados constitutivos como a Constituição da União",*[4] *e a partir da qual se tem erigido o princípio da União de Direito, "construído […] como uma norma que fornece um i) limite à atuação das instituições europeias e dos Estados-Membros nos domínios abrangidos pelo direito da União, bem como uma ii) garantia aos direitos dos particulares afetados por disposições europeias*".[5] Isto assim é porque, para além de critério fundamental aplicável aos Estados-Membros, que o devem observar, a limitação do poder pelo Direito deve conformar a conduta da própria União, uma vez que a sua atuação é suscetível de interferir com os direitos e interesses dos particulares ou dos próprios Estados.

Sendo a UE uma União de Direito, é natural que ela se reja por um princípio estrito de legalidade, que "*impõe aos órgãos competentes uma reação adequada contra qualquer*

---

[1] Maria Luísa Duarte, *União Europeia: Estática e Dinâmica da Ordem Jurídica Eurocomunitária*, v. I (Coimbra: Almedina, 2011), 78.

[2] João Mota de Campos, António Pinto Pereira e João Luiz Mota de Campos, *O direito processual da União Europeia: contencioso comunitário* (Lisboa: Fundação Calouste Gulbenkian, 2014), 515.

[3] Acórdão TJUE *Partido Ecologista "Os Verdes" contra Parlamento Europeu*, 23 de abril de 1986, processo C-294/83.

[4] Alessandra Silveira *et al.*, "União de direito para além do direito da União – as garantias de independência judicial no acórdão *Associação Sindical dos Juízes Portugueses*", *JULGAR Online* (2018): 2, http://julgar.pt/uniao-de-direito-para-alem-do-direito-da-uniao-as-garantias-de-independencia-judicial-no-acordao-associacao-sindical-dos-juizes-portugueses/.

[5] Silveira *et al.*, "União de direito", 4.

sujeito de direito que atente contra as regras do direito da União".[6] É neste contexto que se fala de um princípio de tutela jurisdicional efetiva inerente à UE. Com efeito, o §2.º do n.º 1 do artigo 19.º do TUE dispõe expressamente que os Estados-Membros estabelecem as vias de recurso necessárias para assegurar uma tutela jurisdicional efetiva nos domínios abrangidos pelo direito da União, positivando, desta forma, no direito originário da UE a constatação extraída pelo TJUE, no Acórdão *Les Verts*, da natureza do processo de integração. Aproveitamos para acrescentar, igualmente, que estes princípios são realidades extraídas jurisprudencialmente do espírito do processo de integração europeia, pelo que são complementares e interrelacionáveis, pressupondo-se mutuamente, não existindo estre estes princípios uma "ordem" ou "decorrência". Complementarmente, o artigo 6.º da Convenção Europeia dos Direitos do Homem (CEDH) e o artigo 47.º da CDFUE consagram o direito a uma ação perante um tribunal imparcial e independente para defesa dos seus direitos e liberdades, que constitui não só um princípio geral de Direito da União,[7] mas igualmente um direito fundamental dos cidadãos da UE.[8]

Mas em que consiste, então, a tutela jurisdicional efetiva, no contexto do direito da UE? Se adotarmos a noção de tutela jurisdicional efetiva como "*sucessão lógica […] de direitos que […] visa garantir que tanto a objetiva legalidade europeia como os direitos subjetivos e interesses legítimos, maxime fundamentais, conferidos […] aos particulares pela ordem jurídica da União, sejam […], através da atividade levada a cabo pelos tribunais, devidamente assegurados e protegidos*",[9] depressa constatamos que o princípio da tutela jurisdicional efetiva comporta uma natureza complexa, que se desdobra num conjunto de subprincípios que o materializam. Sucintamente, a tutela jurisdicional efetiva pode desdobrar-se em: direito à ação; direito de acesso ao Direito e a tribunais imparciais; direito a um processo justo e equitativo; direito à obtenção de uma decisão judicial em prazo célere e razoável; direito à efetividade das decisões judiciais; e direito à defesa e assistência judiciária. Destes subprincípios, focar-nos-emos no direito de acesso ao Direito, pela sua relevância no contexto do presente estudo.

Cumpre, no entanto, enquadrar brevemente o direito de acesso ao Direito no contexto mais abrangente do direito à ação. Retira-se da formulação "direito à ação" a faculdade de os "particulares poderem fazer valer judicialmente os direitos conferidos pelo direito comunitário e correspondente direito ao controlo jurisdicional".[10] No contexto do artigo 47.º da CDFUE, a expressão "direito à ação" indicia, de forma mais ampla,[11] um direito a um recurso jurisdicional efetivo, articulando o direito a remédios e formas de tutela efetivos que os interessados visam obter do órgão jurisdicional, "no sentido de um tipo de atuação «*remedial*» que permita assegurar uma plena proteção do

---

[6] Mota de Campos, Pereira e Mota de Campos, *O direito processual*, 515.

[7] Acórdão TJUE *Marguerite Johnston contra Chief Constable of the Royal Ulster Constabulary*, 15 de maio de 1986, processo 222/84, considerando 18.

[8] Acórdão TJUE *Unión de Pequeños Agricultores contra Conselho da União Europeia*, 25 de julho de 2002, processo C-50/00 P, considerando 41.

[9] Carlos Carranho Proença, *Tutela jurisdicional efetiva no Direito da União Europeia – Dimensões teoréticas e práticas* (Lisboa: Petrony, 2017), 61-62.

10 Maria José Rangel de Mesquita, "Anotação ao artigo 47.º", in *Carta dos Direitos Fundamentais da União Europeia Comentada*, coord. Alessandra Silveira e Mariana Canotilho (Coimbra: Almedina, 2013), 538.

[11] Estes indícios resultam da redação francesa – *droit à un recours effectif* – e inglesa – *right to na effective remedy* – do mesmo artigo, complementadas pela jurisprudência do TJUE assente no já referido acórdão *Johnston* (*vide* considerando 19), in: Joana Covelo de Abreu, "Princípio da tutela jurisdicional efetiva", in *Enciclopédia da União Europeia*, coord. Ana Paula Brandão *et al.* (Lisboa: Petrony, 2017), 331.

direito em causa",[12] assim como o correspondente direito a meios processuais efetivos de ação e defesa,[13] quer por via de uma ação principal, quer por via de medidas provisórias.[14] Naturalmente, o direito à ação implica, necessariamente, um direito de acesso ao Direito, ou, dito por outras palavras, o direito de acesso à justiça e aos tribunais. Por lógica, a existência de direitos fundamentais inerentes aos cidadãos leva a que deva ser garantida a estes a possibilidade de se dirigirem aos tribunais para a "*declaração e a efetivação dos seus direitos não só perante outros particulares, mas também perante o Estado e quaisquer entidades públicas*".[15] Se partimos do pressuposto que "*ubi ius, ibi remedium*",[16] ou seja, de que a cada direito corresponde uma forma de o efetivar em juízo, então deve operar-se uma "*compreensão unitária da relação entre direitos materiais e direitos processuais, entre direitos fundamentais e organização e processo de protecção e garantia*",[17] levando a que se estabeleçam, *v. g.*, tipos de ações ou recursos adequados aos direitos a proteger e tipos de sentenças apropriadas às pretensões sob tutela.

Tecidas estas considerações, cumpre analisar sumariamente a concretização da tutela jurisdicional efetiva no contencioso da UE. A expressão "contencioso da UE" pode assumir dois sentidos: um sentido orgânico e um sentido material. Entendido num sentido orgânico, o contencioso da UE será o estudo da jurisdição e da competência do TJUE e dos meios jurisdicionais que perante ele se podem exercer, ou seja, "do *sistema jurisdicional de garantia* da Ordem Jurídica da União Europeia".[18] Num sentido material, o contencioso da UE será o estudo da aplicação do direito da UE pelos órgãos jurisdicionais nacionais e da própria União. Ora, sendo a UE perspetivada como uma União de Direito, na medida em que estabelece "*um sistema completo de vias de recurso e de procedimentos destinado a confiar ao Tribunal de Justiça a fiscalização da legalidade dos actos das instituições*",[19] dotando-se assim de um sistema jurisdicional complexo, é natural que esta conte com os "*tribunais nacionais enquanto tribunais funcionalmente europeus (quando aplicam o direito da União) e os tribunais organicamente europeus que integram o TJUE*".[20]

É precisamente desta "*interação reflexiva entre ordens jurisdicionais que convivem no mesmo espaço jurídico*"[21] que a tutela jurisdicional efetiva se concretiza enquanto

---

[12] Patrícia Fragoso Martins, *Tribunais Nacionais e Direito da União Europeia – questões e jurisprudência essenciais* (Lisboa: Universidade Católica Editora, 2020), 40.

[13] Filipa Fernandes, *O direito fundamental à ação e as suas implicações no contencioso da União Europeia pós-Tratado de Lisboa* (Cascais: Principia, 2015), 21.

[14] Rangel de Mesquita, "Anotação", 542.

[15] Jorge Miranda, *Manual de direito constitucional*, Tomo IV, 5.ª ed. (Coimbra: Coimbra Editora, 2012), 354-355.

[16] Martins, *Tribunais*, 40.

[17] J.J. Gomes Canotilho e Vital Moreira, *Constituição da República Portuguesa Anotada, Volume I: Artigos 1º a 107º*, 4.ª ed. (Coimbra: Coimbra Editora, 2007), 416.

[18] Maria José Rangel de Mesquita, *Introdução ao contencioso da União Europeia – Lições*, 3.ª ed. (Coimbra: Almedina, 2018), 15.

[19] Acórdão *Les Verts*, considerando 23.

[20] Covelo de Abreu, "Princípio", 330.

[21] Joana Covelo de Abreu, "O acórdão do Tribunal Constitucional português n.º 591/2016 em matéria de concessão de apoio judiciário a pessoas coletivas com fins lucrativos e a jurisprudência do Tribunal de Justiça – reflexões prospetivas à luz da interjurisdicionalidade", in *UNIO E-book – Workshop CEDU/UNISC 2016: Interjusfundamentalidade, Internormatividade e Interjurisdicionalidade*, coord. Alessandra Silveira (Braga: CEDU/EDUM, 2016), 147, http://repositorium.sdum.uminho.pt/handle/1822/53733. O conceito que traduz esta ideia de interação reflexiva é a chamada interjurisdicionalidade, que se inspira na interconstitucionalidade de Gomes Canotilho e cuja definição a mesma Autora oferece no mesmo trabalho. *Vide*: *Idem*, 141-142.

princípio da ordem jurídica da UE. Outro entendimento não seria possível, uma vez que a UE continua a criar direitos e obrigações "*sem especificar como é que estes serão observados na prática, pelo que é fundamental a articulação entre os sistemas jurisdicionais nacionais e o TJUE*".[22] Se são criados direitos e obrigações numa União que se diz de Direito, então devem corresponder a estes meios jurisdicionais de os fazer valer em juízo. Mas, mais do que isso, cumpre garantir igualmente que os interessados tenham efetivo acesso a estes meios de tutela jurisdicional, pelo que a ordem jurídica da UE apenas pode ser concebível através da articulação entre o TJUE e os tribunais nacionais, que atuam numa veste de "*tribunais comuns do Direito da União – não só por via da execução do Direito da União pelos Estados membros, mas também pela sua aplicação ao nível nacional implicando a suscetibilidade da sua invocação perante […] as jurisdições nacionais que têm o dever de tutelar direitos decorrentes da Ordem Jurídica da União*".[23]

Portanto, e em suma, o direito-garantia a uma tutela jurisdicional efetiva concretiza-se, no quadro do contencioso da UE, numa rede integrada pelos meios jurisdicionais estabelecidos pelo direito da UE e a sua aplicação perante os órgãos jurisdicionais da ordem jurídica da União, composta pelos tribunais organicamente (TJUE) e funcionalmente (tribunais nacionais) europeus.

2. A tutela jurisdicional efetiva à luz do novo paradigma da justiça eletrónica europeia

Baseando-se na transformação sem precedentes que as tecnologias de informação e comunicação representam para a economia mundial, a UE cedo percebeu que teria de se adaptar à rápida digitalização da economia se quisesse agarrar as oportunidades para a inovação, o crescimento e o emprego que surgem com estas transformações. Por isso mesmo, a Comissão Europeia "*estabeleceu como uma das suas prioridades-chave a criação de um Mercado Único Digital*", que consistiria num mercado "*inclusivo em que os cidadãos e as empresas tenham as competências necessárias e possam beneficiar de serviços eletrónicos interligados e multilingues, desde a administração pública em linha, a justiça eletrónica, a saúde em linha, a energia em linha ou o transporte eletrónico*".[24]

É com este pano de fundo que a Comissão Europeia apresenta o seu Plano de ação (2016-2020) para a administração pública em linha (*e-Government*), no âmbito do qual a Comissão refere a necessidade de aprofundar a digitalização da justiça, promovendo "*esforços significativos de modernização digital com impacto significativo na justiça, alinhando-se com as demandas decorrentes do Plano Plurianual de Justiça Eletrónica em vigor, nomeadamente apostando num reforço das valências do Portal Europeu de Justiça como*

[22] Covelo de Abreu, "Princípio", 330.

[23] Rangel de Mesquita, *Introdução*, 18. A ideia dos tribunais nacionais como tribunais comuns da UE é recorrente na literatura, podendo ser citados, entre outros: Fausto de Quadros e Ana Maria Guerra Martins, *Contencioso da União Europeia*, 2.ª ed. (Coimbra: Almedina, 2009), 23; Joana Covelo de Abreu, "Tribunal de Justiça da União Europeia", in *Instituições, Órgãos e Organismos da União Europeia*, coords. Joana Covelo de Abreu e Liliana Reis (Coimbra: Almedina, 2020), 74; Ana Maria Guerra Martins, *Manual de direito da União Europeia* (Coimbra: Almedina, 2012), 539-540; Koen Lenaerts, Ignace Maselis e Kathleen Gutman, *EU Procedural Law* (Oxford: Oxford University Press, 2014), 3; e Mota de Campos, Pereira e Mota de Campos, *O direito processual*, 27.

[24] Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Estratégia para o Mercado Único Digital na Europa, COM(2015) 192 final, Bruxelas, 6.5.2015, 18, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A52015DC0192.

balcão único de informações sobre justiça europeia".[25] Todos estes planos de ação vinham na senda da *e-Justice*, definida já em 2008 pela Comissão como "*o recurso às tecnologias da informação e da comunicação com o objectivo de melhorar o acesso dos cidadãos à justiça e a eficácia da acção judiciária*". [26]

Neste contexto, o Conselho apresenta três planos plurianuais de ação sobre a justiça eletrónica europeia, encontrando-se atualmente em vigência o Plano de ação (2019-2023) para a justiça eletrónica europeia.[27] Tendo como objetivo geral "*melhorar o acesso à justiça num contexto pan-europeu*", procura-se "*desenvolver e integrar tecnologias da informação e comunicação para o acesso à informação jurídica e o funcionamento dos sistemas judiciais*",[28] visando-se "*facilitar o acesso à justiça e o funcionamento dos sistemas de justiça, nomeadamente em processos transfronteiras, para os cidadãos, os profissionais da justiça e as autoridades, tendo em conta a independência do poder judicial e a separação de poderes*".[29] Este objetivo, acrescenta o Conselho, "*é concretizado através da simplificação e digitalização das comunicações, do acesso aos procedimentos e à informação jurídica e da ligação aos sistemas nacionais, bem como entre eles, num contexto transfronteiras*".[30]

Outro objetivo fundamental associado à justiça eletrónica europeia é o do aprofundamento e consolidação da interoperabilidade entre os sistemas judiciais dos Estados-Membros. Por interoperabilidade deve entender-se 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*",[31] consoante a definição fornecida pela Comissão Europeia. Assim, com a estratégia do Conselho visa-se assegurar a "*compatibilidade dos vários aspetos técnicos, organizativos, jurídicos e semânticos selecionados para as aplicações do sistema judicial*"[32] mediante a "*implementação técnica e a gestão dos sistemas nacionais de justiça eletrónica necessários para facilitar a interligação e a interoperabilidade*".[33]

Portanto, a finalidade que retiramos de todos os planos, comunicações e resoluções destas instituições europeias é a de operacionalizar a justiça eletrónica, e o novo paradigma que esta representa ao nível da justiça europeia, ao serviço da tutela

---

[25] Joana Covelo de Abreu, "O desígnio da justiça eletrónica europeia de 2019 a 2023 à luz do contencioso da União – reflexões antecipatórias", in *Direito e pessoa no mundo digital algumas questões*, coord. Luís Couto Gonçalves *et al.* (Braga: Escola de Direito da Universidade do Minho, 2019), 29.

[26] Comissão das Comunidades Europeias, Comunicação da Comissão ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu – Rumo a uma estratégia europeia em matéria de e-Justice, COM(2008) 329 final, Bruxelas, 30.5.2008, 3, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52008DC0329.

[27] Conselho, Estratégia de justiça eletrónica para 2019-2023, 2019/C 96/04, 13.3.2019, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52019XG0313(01) e Plano de ação para a justiça eletrónica europeia para 2019-2023, 2019/C 96/05, 13.3.2019, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52019XG0313(02).

[28] Conselho, Estratégia de justiça eletrónica para 2019-2023, § 1.

[29] *Idem*, § 12.

[30] *Idem*.

[31] Decisão (UE) 2015/2240 do Parlamento Europeu e do Conselho, de 25.11.2015, 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, *JO L 318* de 4.12.2015, 1-16 entretanto revogada pelo Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29.4.2021 que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240, *JO L 166* de 11.5.2021, 1-34 .

[32] Conselho, Estratégia de justiça eletrónica para 2019-2023, § 24.

[33] *Idem*.

jurisdicional efetiva. Esta intenção é bem patente nos objetivos de aproximação dos cidadãos à justiça e ao direito (através da digitalização e simplificação das comunicações e do acesso digital à informação jurídica) e da efetivação do sistema judicial europeu (através da ligação entre os diversos sistemas judiciais nacionais numa lógica transfronteiriça). A dupla vertente de direito à ação e acesso ao Direito que a realidade preconizada pela tutela jurisdicional efetiva representa parece-nos, atendendo a tudo isto, devidamente acautelada. Efetivamente, as ferramentas digitais podem reforçar a tutela jurisdicional efetiva, aproximando os cidadãos da justiça e do Direito, através de processos digitais e da utilização de linguagem simplificada e acessível, e promovendo a interoperabilidade entre os diversos sistemas judiciais nacionais, concretizando a articulação entre os tribunais organicamente e funcionalmente europeus desejada por uma União de Direito.

3. O e-CODEX como ferramenta de densificação da tutela jurisdicional efetiva

Inserido na Estratégia de justiça eletrónica para 2019-2023 encontramos o objetivo de "*proporcionar um acesso mais simples e rápido aos tribunais e facilitar o recurso aos procedimentos extrajudiciais através da utilização de ferramentas de comunicação eletrónicas seguras […] em situações transfronteiras*",[34] para além do objetivo de "*facilitar a interação e a comunicação eletrónicas entre as autoridades judiciárias, bem como a comunicação com os cidadãos e os profissionais nos processos judiciais (através […] de intercâmbios seguros de dados eletrónicos, por exemplo*)",[35] sugerindo o Conselho que, para tal, se recorra à tecnologia e-CODEX. Para além disto, o e-CODEX representa um enorme potencial no aprofundamento da interoperabilidade entre sistemas nacionais.[36] Cumpre, portanto, apresentar sumariamente a tecnologia e-CODEX, de forma a podermos, por fim, perceber de que forma pode esta ferramenta contribuir para a densificação da tutela jurisdicional efetiva na UE.

O e-CODEX (*e-Justice Communication via On-line Data Exchange*) foi lançado em dezembro de 2010,[37] "*ao abrigo do plano de ação plurianual 2009-2013 do portal da Justiça, sobretudo para promover a digitalização dos processos judiciais transnacionais e facilitar a comunicação entre as autoridades judiciárias dos Estados-Membros*".[38] O seu objetivo é o de facilitar a "*comunicação segura nos processos cíveis e penais através de uma solução personalizada de intercâmbio transnacional de mensagens eletrónicas no domínio da cooperação judiciária*", sendo composto por "*um conjunto de produtos informáticos (software) que podem ser utilizados para criar um ponto de acesso para comunicações seguras*" com outros pontos de acesso pela Internet, "*através de um conjunto de protocolos comuns, sem que esteja envolvido qualquer tipo de sistema central*".[39] Sendo o e-CODEX "*um instrumento especificamente concebido para facilitar o intercâmbio eletrónico transnacional de mensagens no domínio da justiça*",[40] procura-se com a sua implementação a garantia

[34] Conselho, Estratégia de justiça eletrónica para 2019-2023, §19.
[35] *Idem*, §20.
[36] Conselho, Plano de ação para a justiça eletrónica europeia para 2019-2023, §18.
[37] e-CODEX, "December 2010: Start of e-CODEX", Journey, https://www.e-codex.eu/journey.
[38] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um sistema informatizado de comunicação em processos cíveis e penais transnacionais (sistema e-CODEX) e que altera o Regulamento (UE) 2018/1726, COM(2020) 712 final, Bruxelas, 2.12.2020, 1, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020PC0712.
[39] *Idem*.
[40] Considerando 1 da Proposta de Regulamento.

de um acesso eficaz dos cidadãos e das empresas à justiça e a facilitação da cooperação judiciária entre os Estados-Membros, que "*constituem alguns dos principais objetivos do Espaço de Liberdade, Segurança e Justiça da UE consagrados no Tratado sobre o Funcionamento da União Europeia*".[41]

Explicando muito sucintamente o funcionamento do e-CODEX e a sua gestão operacional, este sistema é composto por dois elementos de *software*: o *software* Domibus Gateway, para o intercâmbio de mensagens com outras portas de ligação, e o *software* Domibus Connector, que possibilita diversas funcionalidades relacionadas com a transmissão de mensagens entre sistemas nacionais. A porta de ligação baseia-se no módulo eDelivery mantido pela Comissão, tornando o *software* conector possíveis "*funções como a verificação de assinaturas eletrónicas através de uma biblioteca de segurança e notificações de receção de mensagens*".[42] Atualmente, a gestão operacional encontra-se a cargo de um consórcio de Estados-Membros e de organizações com financiamento proveniente dos programas da União. No entanto, é intenção da Comissão a atribuição da gestão operacional do e-CODEX à Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala (eu-LISA), adaptando para o efeito as responsabilidades do seu Conselho de Administração, e criando um Grupo Consultivo do e-CODEX.[43]

A justiça, numa União de Direito, quer-se sem fronteiras. Isto porque *"[c]riar uma Europa mais justa e segura é […] fundamental para atingir um verdadeiro Mercado Único*".[44] E o acesso à justiça por parte dos cidadãos "*não deve ser desencorajado pela complexa variedade dos […] diferentes sistemas jurídicos" nacionais, como por exemplo no que toca a ações transfronteiriças de pequeno montante ou a assuntos criminais.*[45] Pela sua potencialidade para promover uma "*transmissão segura de dados eletrónicos nos processos cíveis e penais transnacionais*",[46] a par da cooperação judicial transfronteiriça que este sistema preconiza, o e-CODEX "*torna os processos judiciais mais transparentes, eficientes e económicos*", simultaneamente facilitando "*aos cidadãos, empresas, administrações e profissionais da justiça um acesso fácil à justiça*".[47]

Atendendo àquelas que são as dimensões fundamentais de uma tutela jurisdicional efetiva enquadrada num contencioso amplo e dinâmico de uma União de Direito, é natural que nos saltem à vista as potencialidades da *e-Justice* e, especificamente, do sistema e-CODEX. Nomeadamente, no potencial de concretização da rede articulada de meios e órgãos jurisdicionais da ordem jurídica europeia. Dos dois aspetos fundamentais da tutela jurisdicional efetiva que destacamos, verificamos que o e-CODEX ajuda a cumprir e a sedimentar o direito de acesso ao Direito, nomeadamente de acesso aos tribunais (funcionalmente e organicamente) europeus e aos meios jurisdicionais adequados a fazer valer as suas pretensões. As soluções representadas pela integração das ferramentas digitais na justiça e na governação a nível europeu exponenciam consideravelmente a concretização de uma verdadeira ordem jurídica europeia garante de uma tutela jurisdicional efetiva, criadora de direitos para os seus cidadãos e de meios jurisdicionais de os efetivar, cumprindo assim os desígnios de uma verdadeira, justa e ampla União de Direito.

---

[41] Comissão Europeia, Proposta de Regulamento, 1.
[42] Considerando 5 da Proposta de Regulamento.
[43] Considerandos 7 e 8 da Proposta de Regulamento.
[44] e-CODEX, "A more just and secure Europe", About, https://www.e-codex.eu/about. No mesmo texto, afirma-se perentoriamente que "Justice is borderless" (A justiça não tem fronteiras).
[45] e-CODEX, "A more just and secure Europe".
[46] Comissão, Proposta de Regulamento, 3.
[47] e-CODEX, "Safer and legally protected", About.

O consumo e potenciais problemas concorrenciais nos mercados digitais

Samantha Ribeiro Meyer-Pflug Marques[*]
Patrícia Pacheco Rodrigues[**]

1. Introito

O cenário atual é o de uma população mundial de mais de sete bilhões e recursos naturais limitados, o que enfatiza a necessidade premente de se agir com responsabilidade, pois o que se faz hoje tem impacto futuro na vida das pessoas e próprio planeta. A Educação para o Desenvolvimento Sustentável ajudaria a alcançar um futuro possível para se integrar o desenvolvimento sustentável ao ensino e à aprendizagem, inclusivo e de equitativa qualidade. No plano internacional global, há diversos Tratados Internacionais e Declarações sobre proteção dos Direitos Humanos, e todos em questão procuram limitar o poder, merecendo destaque na atual conjuntura o poder empresarial, ainda mais quando se fala na eficácia horizontal dos direitos fundamentais.[1] Nesse mesmo sentido está a Carta dos Direitos Digitais Fundamentais da União Europeia, que tem por objetivo afirmar a União Europeia como líder no estabelecimento de regras para o respeito pelos direitos digitais individuais na busca de uma Democracia Digital, centrada na defesa da democracia, sustentabilidade e ética.[2]

Busca-se nesse artigo ressaltar as mudanças no mercado de consumo devido ao amplo uso e desenvolvimento da tecnologia, que tornou o potencial de economia globalizada em escala mundial uma característica da sociedade contemporânea, trazendo novas utilidades para o consumidor e o aprimoramento diuturno de produtos e serviços. A importância deste trabalho justifica-se pela dicotomia entre o interesse público e o privado, pois as transformações tecnológicas recentes vêm criando novas categorias de sociabilidades nas formas de produção, relações de trabalho e de consumo, que implicam, ao mesmo tempo, um Direito mais ágil e adaptado a estas transformações, ainda mais quando fundado no referencial teórico do Capitalismo Humanista.[3]

Objetiva-se assim demonstrar que, no atual cenário, os consumidores são impactados de diversas maneiras, face ao alto volume de dados por eles fornecidos às

---

[*] Doutora e Mestre em Direito – PUC/São Paulo, Profa. Titular do Programa de Doutorado e Mestrado em Direito da UNINOVE-Brasil.
[**] Doutoranda e Mestre em Direito pela UNINOVE-Brasil, Comissária de Polícia Civil em São Paulo.
[1] Marcelo Benacchio e Diogo Basílio Vailatti, "Empresas transnacionais, globalização e direitos humanos", in *A sustentabilidade da relação entre empresas transnacionais e direitos humanos*, ed. Marcelo Benacchio *et al.* (Curitiba: CRV, 2016), 19-20.
[2] "Charta der Digital en Grundrechteder Europäischen Union", acesso em 20.03.2022, https://digitalcharta.eu/intiatorinnen-und-initiatoren/.
[3] Ricardo Sayeg e Wagner Balera, *Capitalismo humanista a dimensão econômica dos direitos humanos, fator Caph* (São Paulo: Max Limonad, 2020), Edição Kindle.

plataformas, com potenciais violações de privacidade e a necessidade de proteção de dados em geral[4], além do aumento na quantidade de anúncios em buscas e nas redes sociais nas perspectivas do Marketing 4.0 e 5.0.

Foi utilizado o método dedutivo e a pesquisa documental, para se concluir que o poder de mercado de plataformas digitais pode se manifestar de formas distintas nos mercados digitais e não há um único fator a ser analisado. Contudo, a economia comportamental é fundamental para se entender as dinâmicas concorrenciais, pois as plataformas exploram tendências comportamentais para manter a sua posição dominante.

2. Considerações gerais sobre mercados digitais em consumo e concorrência

Em conformidade com a Política Nacional das Relações de Consumo, do artigo 4.º do Código de Defesa do Consumidor Brasileiro, deve-se reconhecer a vulnerabilidade do consumidor no atual mercado de consumo que surge com a revolução tecnológica da Quarta Revolução Industrial, Revolução 4.0 ou Revolução Digital que, dentre outras coisas, vem impactando as indústrias e os negócios com redução de custos para o aumento da produtividade e dos lucros. Desde a reforma trabalhista no Brasil em 2017, houve mudança significativa na Consolidação das Leis do Trabalho pela Lei Federal n.º 13.467 de 2017, que trouxe flexibilização para as condições de trabalho neste mundo globalizado, cada vez mais competitivo, extremamente dinâmico e economicamente agressivo.

Ficaram consignados, na revisão, pelo Departamento de Estudos Econômicos,[5] dos relatórios especializados emitidos por autoridades e centros de pesquisa ao redor do mundo, os principais danos diretos e indiretos aos consumidores na concorrência em mercados digitais e também mencionam, de forma um tanto genérica, muitos benefícios gerados pela digitalização dos mercados.Nesse cenário, em que consumidores podem ser impactados de diversas maneiras, com *"o alto volume de dados fornecidos às plataformas, potenciais violações de privacidade e proteção de dados em geral e o aumento na quantidade de anúncios em buscas e redes sociais"*.[6] Para os problemas apresentados, as possíveis soluções por parte das autoridades antitruste seria de maior proatividade na promoção e manutenção da rivalidade nestes mercados, corrigindo as distorções identificadas, mas *"isso, porém, não significa que a competição é impossível-remédios antitruste e regulatórios podem endereçar as fontes de poder de mercado e assegurar uma melhor dinâmica competitiva que beneficie consumidores"*.[7]

Assim, a proteção do consumidor, diante desse novo paradigma tecnológico, não reside exclusivamente nas normas do Direito do Consumidor, mas na compreensão destas em comum com outras legislações, até mesmo de Direito Comparado. No Brasil, o Conselho Administrativo de Defesa Econômica (Cade), definido no artigo 4.º da

[4] Lei Federal n.º 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), acesso em 10.03.2022, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[5] Cfr. a Lei Federal n.º 12.529 de 30 de novembro 2011, é órgão que compõe o Sistema Brasileiro de Defesa da Concorrência, acesso em 10.03.2022, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm.

[6] Departamento de Estudos Econômicos, "Concorrência em mercados digitais: uma revisão dos relatórios especializados", in *Documento de Trabalho n.º 005/2020*, ed. Filippo Maria Lancieri *et al.* (Brasília: Conselho Administrativo de Defesa Econômica, 2020), 37-38.

[7] Departamento de Estudos Econômicos, "Concorrência em mercados digitais", 99.

Lei Federal n.º12.529, de 30 de novembro de 2011, que estrutura o Sistema Brasileiro de Defesa da Concorrência, vem reconhecendo esta nova conjuntura das autoridades antitruste ao redor do mundo, promovendo estudos para mapear os desafios à ampla e livre concorrência em uma economia digital.[8]

Para o Cade, em uma visão geral da estrutura destes mercados, segundo os relatórios analisados, cujo conteúdo se mostrou de especial importância, seja pelo renome das autoridades responsáveis ou pelo foco específico em importantes mercados digitais, esses mercados não convergem para uma definição única do que são plataformas digitais, mas quase todos destacam a importância dos dados para estes mercados digitais. De igual modo, nos relatórios analisados, a *Competition and Markets Authority* (CMA), reguladora da concorrência no Reino Unido, também destacou as diferentes formas e intensidades em que plataformas coletam dados de usuários. Assim, a economia comportamental vem como chave para entender dinâmicas concorrenciais, pois, conforme o Departamento de Estudos Econômicos Brasileiro, as plataformas exploram conhecidos vieses comportamentais para solidificar sua posição dominante: *"De fato, quanto mais mudanças tecnológicas facilitam o fluxo de informações e removem barreiras físicas à competição, mais o comportamento humano torna-se a variável que impede a efetiva competição entre empresas"*.[9]

Nesse sentido, também é a proposta de Regulamento Mercados Digitais do Parlamento Europeu, consentânea com a Carta dos Direitos fundamentais da União Europeia (UE), a Convenção Europeia dos Direitos Humanos (CEDH) e o Regulamento Geral sobre a Proteção de Dados. A proposta traz a *"introdução de uma atualização dinâmica da lista de práticas desleais que estaria sujeita ao pleno respeito dos direitos fundamentais a um processo equitativo e à boa administração consagrados na CEDH, que são vinculativos para as instituições da EU"*.[10]

Uma atualização também possível é a prevista no Projeto de Lei 3.514/2015, que alteraria o CDC, para aperfeiçoar as disposições gerais sobre o comércio eletrônico, inspirado nas Diretivas da União Europeia n.º 2019/770, 2019/771 e 2011/83.[11] Assim, por exemplo, embora previsão expressa no artigo 49.º do CDC, que possibilita ao consumidor desistir no prazo de sete dias, sempre que a contratação de fornecimento de produtos e serviços ocorrer fora do estabelecimento comercial, necessária a atualização para o comércio eletrônico desse direito de arrependimento, tendo em vista que a previsão é expressa para o recebimento de produto ou serviço por telefone ou em domicílio.

Sobre os potenciais problemas em mercados digitais específicos, quais sejam, nas plataformas de comparação de preços e na falta de neutralidade dos algoritmos, o Cade, em votos proferidos em processo administrativo e em Nota Técnica no 34/2018/DEE/CADE, decidiu sobre alegações de critérios discriminatórios para apresentação de resultados de produtos dentro de página de resultados de busca geral e de exibição privilegiada de resultados de produtos em detrimento de sítios eletrônicos de comparação de preço. Também apresentou estudo do histórico das apurações de eventuais condutas anticompetitivas relativas ao *Google Shopping* nas jurisdições europeia, estadunidense

[8] Departamento de Estudos Econômicos, "Concorrência em mercados digitais", 7.
[9] Departamento de Estudos Econômicos, "Concorrência em mercados digitais", 12-31.
[10] Comissão Europeia, "Proposta de regulamento do Parlamento Europeu e do Conselho - relativo à disputabilidade e equidade dos mercados no setor digital", in *Regulamento Mercados Digitais* (Bruxelas: Conselho da União Europeia, 2020), 13.
[11] Antonia Espíndola Longoni Klee, *Comércio Eletrônico* (São Paulo: Revista dos Tribunais, 2014).

e francesa, bem como seu cotejo com a investigação brasileira. Trouxe a lume a possibilidade da análise da eficiência, tanto para os consumidores quanto para os anunciantes brasileiros do mercado de mecanismos de buscas, e a possível insuficiência dos remédios antitrustes disponíveis, além dos riscos à política antitruste de falsos positivos. Na fundamentação e discussão teórica, concluiu pelo arquivamento do referido processo e pela inexistência de indícios suficientes de autoria e materialidade da suposta infração, assim como da inexistência de efeitos no Brasil, ainda que potenciais, de eventuais ilícitos anticoncorrenciais.[12]

Em novembro de 2010, a Comissão Europeia decidiu instaurar procedimento investigativo para apurar alegações de que o *Google* teria abusado de sua posição dominante no mercado de buscas *online*, violando o art. 102 do Tratado sobre o Funcionamento da União Europeia – TFUE. Em decisão de junho de 2017, concluiu que, de fato, houve violação do TFUE, e o *Google* foi condenado ao pagamento de multa, bem como a cumprir com o princípio do tratamento igualitário no mercado de comparação de produtos. Restou constatado que, com a implementação do chamado "algoritmo panda", os comparadores de preço em vários países do espaço econômico Europeu perderam visibilidade.[13]

Nos Estados Unidos, de modo muito distinto, foi a apuração sobre eventuais condutas anticompetitivas relacionadas ao *Google Shopping*. Em 2010, as agências americanas investigaram eventuais práticas anticoncorrenciais do *Google Shopping*, apresentadas por algumas de suas concorrentes que alegavam inclinação do mecanismo de pesquisas geral/orgânica. Contudo, nos Estados Unidos, a*Google* foi considerada inocente da prática de abuso de posição dominante pela *Federal Trade Commission*, por não ter sido considerada uma porta de entrada na Internet, pois quando o consumidor acessa o *browser* da Internet, não simultaneamente se conecta à *Google e* nada se restringe para que ele utilize outro mecanismo de pesquisa. Além disso, outra justificativa importante que motivou o arquivamento é que a lei anticoncorrencial estadunidense protege consumidores, mas preservando o processo competitivo entre as empresas, e não existe nenhuma lei que proíba qualquer empresa de promover suas próprias inovações.[14]

Nos termos da decisão n.º 21-D-11 de 7 de junho de 2021, a Autoridade da Concorrência da França sancionou o *Google* por ter abusado de sua posição dominante no mercado de servidores de anúncios do editor de *sites online* e aplicativos móveis, em violação aos artigos L. 420-2 do Código de Comércio e 102.º do Tratado sobre o Funcionamento da União Europeia - TFUE. A referida agência reguladora descobriu que o *GoogleAd Manager*, servidor de anúncios *Doubleclick,* favorecia o *GoogleDoubleclickAdExchange*, plataforma de vendas de espaço publicitário da própria empresa, sendo o *Google* condenado, além de multa, à aplicação de remédio antitruste consistente no dever de mudar suas práticas globais de anúncios.[15]

Para Philip Kotler, o pai do marketing moderno, as novas características de consumo e do consumidor em seu conceito de Marketing 4.0 estão relacionadas às mudanças de poder sobre uma quantidade de dados que nunca fora vista, advinda de

[12] "Nota Técnica no 34/2018/DEE/CADE", *Conselho Administrativo de Defesa Econômica,* acesso em 04.07.2018, https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/notas-tecnicas/2018/nota-tecnica-n34-processo-administrativo-08012010483201194.pdf.

[13] "Nota Técnica no 34/2018/DEE/CADE".

[14] "Nota Técnica no 34/2018/DEE/CADE".

[15] "Décision 21-D-11 du 07 juin 2021 relative à des pratiques mises en œuvre dans le secteur de la publicité sur Internet", *Autorite de la concurrence,* acesso em 10.07.2021, https://www.autoritedelaconcurrence.fr/fr/decision/relative-des-pratiques-mises-en-oeuvre-dans-le-secteur-de-la-publicite-sur-internet-0.

consumidores conectados, ressaltando a Internet móvel, que trouxe a conectividade *peer-to-peer* (ponto a ponto) que empoderou os consumidores, os quais deveriam se tornar muito mais bem informados do que no passado.[16] Desde 1995, adveio o uso comercial da Internet e, em 2008, com o desenvolvimento do *smartphone,* as aplicações de Internet ganharam ainda mais importância e o seu acesso é essencial ao exercício da cidadania, questão ressaltada no Marco civil da Internet, Lei Federal nº 12.965, de abril de 2014.

Segundo dados de pesquisa realizada pela Fundação Getúlio Vargas (FGV), no Brasil, a densidade (*per capita*) de dispositivos digitais era de 50% em 2010, e atingiu 200% em 2020, ou seja, dois dispositivos digitais por habitante.[17] Desde o Marketing 3.0, vem-se definindo o novo marketing centrado no ser humano, retratando grandes mudanças para o marketing (1.0), centrado no produto, e do marketing (2.0), voltado para o consumidor. O Marketing 5.0 já é realidade que une a tecnologia e o ser humano, advindo das inovações tecnológicas e transformações na sociedade mundial com a pandemia da Covid-19, em que massivamente as pessoas estão se informando pelas redes sociais e digitais.[18]

A aplicação da equivalência funcional dos negócios jurídicos eletrônicos com os chamados negócios jurídicos tradicionaissempre funcionou, até mesmo na questão da concorrência, mas diante do Figital, conexão do mundo real e do virtual por meio da imersão total dos usuários, ainda não se sabe quais serão as consequências dessas questões mais recentes da tecnologia. No metaverso dos avatares digitais, por exemplo, a pessoa pode ser outra no mundo digital. A rede, em seus primórdios, era tida como serviço de comunicação, com a *Web,* adveio a Internet comercial e, atualmente, na mudança do mercado de produtos em que esses passaram a não ter mais suporte físico, são tidos como bens digitais ou bem móvel imaterial. Para Claudia Lima Marques e Bruno Miragem, são os serviços simbióticos do consumo digital, gerando dúvidas sobre as aplicações da Internet das coisas no varejo de produtos que, na atualidade, têm grande utilidade para o consumidor, mas que ainda carecem de regulamentação no Direito brasileiro.[19]

Por outro lado, o poder de mercado das plataformas digitais também é gerado pelos próprios consumidores e o comportamento humano é uma variável que impede a efetiva competição entre empresas, permitindo que elas aufiram rendas econômicas sem serem ameaçadas por novos competidores.[20] Para Marcelo Benacchio e Renata Mota Maciel, em grande parte dos países emergentes *"*é a escassez de recursos, ao lado da desigualdade digital e que inclui deficiência em matéria de educação e de pesquisa, conjunto propício à absoluta dependência tecnológica e dominação pelas empresas detentoras do poder econômico*"*.[21] Nesse mesmo sentido, na visão de Bruno Miragem, na atualidade, principalmente em razão do surgimento dessa nova dimensão do mercado de consumo, qual seja, o mercado de consumo virtual e as novas relações estabelecidas por meio dele,

---

[16] Philip Kotler, *Marketing 4.0: do tradicional ao digital* (Rio de Janeiro: Sextante, 2016), Edição Kindle.
[17] Fernando S. Meirelles, "Uso da TI - Tecnologia de Informação nas Empresas", in *Pesquisa Anual do FGV cia*, ed. 32ª (Rio de Janeiro: Fundação Getúlio Vargas, 2021) 91.
[18] Kotler, *Marketing 4.0*.
[19] Claudia Lima Marques e Bruno Miragem, "´Serviços simbióticos` do consumo digital e o PL 3.514/2015 de atualização do CDC", *Revista de Direito do Consumidor*, v. 132 (nov./dez. 2020): 91-118.
[20] Departamento de Estudos Econômicos, "Concorrência em mercados digitais", 31.
[21] Marcelo Benacchio e Renata Mota Maciel, "A LGPD sob a Perspectiva da Regulação do Poder Econômico", in *Comentários à Lei Geral de Proteção de Dados*, ed. Cíntia Rosa Pereira de Lima (São Paulo: Almedina, 2020), 42-43.

como o *e-commerce*. Este integra múltiplos fenômenos, como a oferta pela Internet por meios eletrônicos de pagamento, gerando novas estruturas de negociação de produtos e serviços. E, no caso do fornecimento por plataformas digitais, são necessárias estratégias para uma identificação mais precisa dos interesses dos consumidores e, sobretudo, sobre o tratamento de dados pessoais dele.[22]

A coleta e tratamento de dados pessoais é o grande ativo no mercado da sociedade da informação, as hipóteses que autorizam o tratamento de dados estão previstas no artigo 7.º da LGPD, ou seja, o tratamento regular está previsto emlei e traz a sanções para o tratamento irregular, a partir do artigo 52.º da LGPD. O tratamento irregular de dados determina ainda o dever do ressarcimento de danos, como estabelecem o artigo 42.º e seguintes da LGPD. Portanto, nos contratos à distância no comércio eletrônico ou contratos eletrônicos realizados por consumidores, há o dever de se evitar o abuso na finalidade econômicae social, conforme os princípios previstos no artigo 6.º da LGPD, nos ideais do novo regime das relações contratuais do CDC sobre o limite de contratação e na interpretação dos contratos de adesão, dado que o artigo 9.º da LGPD também proíbe práticas abusivas para proteção também do usuário/consumidor no âmbitodo comércio eletrônico.

Dessa forma, a questão do consentimento do titular para tratamento dos dados é colocado como primeira hipótese no artigo 7.º, inciso I da LGPD, mas tal ponto merece um alerta, devido à falta de reflexão sobre aquilo que se concorda e se discorda nos termos de uso e, muitas vezes, apenas se concorda, pois na prática as pessoas na Internet tendencialmente leem menos ainda e, mesmo se lerem, pode ser que não entendam e, mesmo que leiam e entendam,o consentimento resta prejudicado como nos contratos de adesão.

Logo, esse consentimento fica como uma espécie de autorização formal, muito menos do que um controle da pessoa sobre seus dados.[23] Esse tratamento de dados na etapa pré-contratual deveria ser vinculado aos princípios, como da transparência, conforme artigo 6.º da LGPD. O legítimo interesse no tratamento de dados, como se lê no artigo 10.º da LGPD, é resultado de se buscar apoio e promoção da atividade comercial ou governamental, assim dispõe a Diretiva nº 2016/680 da União Europeia, e, ao mesmo tempo, a proteção em relação ao titular dos dados. Ademais, a proteção de dados privativos é algo com que, mundialmente, as pessoas, governos e empresas têm se preocupado, a exemplo da União Europeia, que conta com o Regulamento Geral sobre a Proteção de Dados -RGPD, UE 2016/679. E nesse sentido, poderia ser fundamento para o tratamento de dados nas redes sociais, em que se presta serviço que beneficiar o usuário, mas ainda não restou claro qual o limite quanto ao uso desses dados. Vale ressaltar que,nos negócios jurídicos digitais, houve a mudança da aplicação do direito à remuneração indireta, quando em serviços gratuitos, com o efeito não-preço ou preço zero, pois esses aumentam o impacto de manipulações comportamentais nacompetição entre diferentes agentes.[24]

Conforme Claudia Lima Marques e Fernando Rodrigues Martins, ainda que crescente o uso da tecnologia tecnicamente disponível para todos, ela não está acessível

---

[22] Bruno Miragem, "Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor", in *Contratos de serviços em tempos digitais*: *contribuição para uma nova teoria geral dos serviços e princípios de proteção dos consumidores*, ed. Claudia Lima Marques *et al.* (São Paulo: Thomson Reuters Brasil, 2021), Kindle edition.

[23] Cláudia Lima Marques, *Contratos no Código de Defesa do Consumidor*: *o novo regime das relações contratuais*, ed. 4ª (São Paulo: RT, 2002), 109.

[24] Departamento de Estudos Econômicos, "Concorrência em mercados digitais", 31.

na prática, uma vez que quase um quarto *"(22,47%) dos brasileiros que não possuem Internet são idosos, aprofundando a 'divisão da sociedade digital' ou o 'Virtual divide"*.[25] Nesse contexto, ainda merecem discussão os temas do assédio de consumo, dadas as novas tecnologias e a conceituação da vulnerabilidade digital no analfabetismo digital. Também para Cláudia Lima Marques e Fernanda Nunes Barbosa, *"O assédio de consumo e o fornecimento de crédito não responsável constituem, atualmente, um grande problema enfrentado pelo Direito do Consumidor, especialmente em relação ao consumidoridoso"*.[26] Por essa razão, representa um dos temas principais do processo de atualização do Código de Defesa do Consumidor no ano de 2021 o advento da Lei Federal n.º 14.181, de julho de 2021, que alterou o CDC e a Lei Federal nº 10.741, de outubro de 2003 (Estatuto do Idoso), para aperfeiçoar a disciplina do crédito ao consumidor e dispor sobre a prevenção e o tratamento do superendividamento.

Ainda sobre a "Divisão Digital" durante o enfrentamento à Covid-19, houve migração de parcelas importantes da população para práticas *online*, o que não foi suficiente para equacionar as desigualdades digitais quanto ao uso da rede, dificultando a implementação dos Objetivos de Desenvolvimento Sustentável da Agenda 2030, sobretudo nas áreas de saúde e educação, conforme o Grupo de Trabalho do Secretário Geral das Nações Unidas sobre o Financiamento Digital dos Objetivos de Desenvolvimento Sustentável.[27]

A Agenda 2030 é guiada pelos propósitos e princípios da Carta das Nações Unidas e o pleno respeito ao Direito Internacional, com fundamento na Declaração Universal dos Direitos Humanos e demais tratados internacionais de direitos humanos. É um plano de ação global que reúne 17 Objetivos de Desenvolvimento Sustentável (ODS), resultado do consenso dos Estados-membros da Organização das Nações Unidas, dentre os quais o Brasil.

Em 2018, foi instituído pelo Decreto nº 9.319, de março de 2018, o Sistema Nacional para a Transformação Digital (SinDigital) que é composto pela Estratégia Brasileira para a Transformação Digital (E-Digital). Dentre seus eixos temáticos, está a reestruturação com o objetivo de aproveitar o potencial das tecnologias digitais existentes para promover o desenvolvimento econômico e social sustentável e inclusivo, com inovação, aumento de competitividade, de produtividade e dos níveis de emprego e renda no país. Assim, merece destaque a educação e a capacitação profissional, que objetiva promover a formação da sociedade para o mundo digital e prepará-la para o trabalho do futuro, assim como a transformação digital do Governo federal, mais acessível à população e mais eficiente em prover serviços ao cidadão, em consonância com a Estratégia de Governo Digital.[28]

---

[25] Claudia Lima Marques e Fernando Rodrigues Martins, "Superendividamento de idosos: a necessidade de aprovação do PL 3515/15", *Revista Consultor Jurídico* (2020), https://www.conjur.com.br/2020-mai-27/garantias-consumo-superendividamento-idosos-preciso-aprolvar-pl-351515.

[26] Claudia Lima Marques e Fernanda Nunes Barbosa. "A proteção Dispensada à Pessoa Idosa Pelo Direito Consumerista é Suficiente Como Uma intervenção Reequilibradora?", *civilistica.Com*, v. 8, no. 2 (2019): 1-26, https://civilistica.emnuvens.com.br/redc/article/view/430.

[27] "Bridging the Digital Divide to Scale Up the COVID-19 Recovery", última modificação em 5.11.2020, https://www.imf.org/pt/News/Articles/2020/11/06/blog-bridging-digital-divide-to-scale-up-covid19-recovery.

[28] "Estratégia Brasileira para a Transformação Digital", *Ministério da Ciência, Tecnologia e Inovações,* última modificação em 21.03.2018, https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacao-digital/estrategia-digital.

3. Considerações finais

Como visto para se garantir a educação para o consumo, conforme previsto na ODS 4 na Agenda 2030 que vem no sentido da educação para o desenvolvimento sustentável. Isso requer mudanças profundas, também, no modo com que a informação e a educação do consumidor vêm ocorrendo na atual economia de mercado do neoliberalismo, que possa garantir os princípios de um referencial teórico fundado no Capitalismo Humanista[29] e, ainda, devido à necessidade depromover as competências como pensamento crítico, reflexões sobre cenários futuros e tomadas de decisão de forma colaborativa, assim como melhorar o acesso à educação e à informação de qualidade.[30]

A evolução nas plataformas digitais refletiu diretamente no mercado eletrônico, na criação de novos modelos de negócios que se apresentam mais acessíveis aos consumidoresem todos os segmentos da sociedade brasileira. Desde a Transformação Digital, as mudanças no mundo digital deixaram de acompanhar o mundo físico, vindo a superá-lo, como na China, em que as vendas de comércio eletrônico já ultrapassam as vendas em lojas físicas. Nesse contexto, o desafio das empresas é manter conexão com o consumidor nas esferas *online* e *offline*, na atual realidade cada vez mais volátil, incerta, complexa e ambígua que reflete na estrutura do mercado e no abuso do poder econômico no mercado de consumo. No direito do consumidor na pandemia, houve o apogeu do consumo digital, apesar de haver o "consumo de vingança" (*revengespending*), associado à recompensa emocional pelos sacrifícios do período e a revalorização do relacionamento entre fornecedor e consumidor, pois restou nítido que consumidores "somos todos nós", mas ainda há muito o que tratar como restou demonstrado ao longo do presente artigo.[31]

Mudanças no estilo de vida e as novas tendências de consumo ampliaram ainda mais o comércio eletrônico e em muito aceleraram o futuro no comércio digital, com o crescimento de novos usuários do *e-commerce* no Brasil, além de impor aos empresários a necessidade de se reinventarem, elaborarem estratégias de marketing digital e adaptarem seus negócios ao novo contexto de consumo e de isolamento social. Há grande tendência de que sejam mantidas essas técnicas no comércio eletrônico no período pós-pandemia, como a combinação de canais de plataformas com início em rede social, passando para aplicativo de mensagem direta, para um atendimento mais específico ao consumidor, o que pode, porém, violar o artigo 30.º, 46.º e 47.º do CDC, nos capítulos das Práticas Comerciais e da Proteção Contratual.

A cidadania está vinculada ao mundo digital e, portanto, é importante preparar o consumidor para o século XXI, em que houve expansão de temas não apenas do mundo digital, mas também de questões como sustentabilidade e das políticas para a relação de consumo e do meio ambiente com os produtos e serviços simbióticos face o atual analfabetismo o digital. Assim, busca-se trazer a inclusão das pessoas, conforme a Política Nacional das Relações de Consumo, alterada recentemente pela Lei Federal nº 14.181, de julho de 2021, incluindo o princípio de evitar a exclusão social do consumidor. Dessa maneira, é estar além do *Homo Consumens*, *"Abdicar da*

[29] Ricardo Sayeg e Wagner Balera, *Capitalismo Humanista a Dimensão Econômica dos Direitos Humanos, Fator Caph* (São Paulo: Max Limonad, 2020), Edição Kindle.

[30] "Education for sustainable development in Brazil", Unesco, acesso em 16.11.2021, https://en.unesco.org/fieldoffice/brasilia/expertise/education-sustainable-development.

[31] Bruno Miragem, "O direito do consumidor pós-pandemia", *Revista Consultor Jurídico* (2021), https://www.conjur.com.br/2021-mar-17/garantias-consumo-direito-consumidor-pos-crise-covid-19.

escassez e restabelecer uma relação baseada na inteligência da abundância – só por aqui poderemos salvar o destino humano e do planeta. Desatá-lo do destino de um sistema destrutivo".[32]

[32] André Barata, "Para uma crítica ao 'Homo consumens'", *O Jornal Económico,* última modificação em 10.06.2021, https://jornaleconomico.pt/noticias/para-uma-critica-ao-homo-consumens-749266.

A aplicabilidade da "teoria das infraestruturas essenciais" aos *datasets* jurídicos

Pedro Petiz Viana[*]

No presente texto, serão primeiramente delineados os impactos da inteligência artificial na área do Direito, com a apresentação de exemplos relativos a várias jurisdições. Seguidamente, será feita uma resenha da relevância dos *datasets* jurídicos ("*legal datasets*") na implementação de soluções de inteligência artificial na área jurídica e por fim, será analisada a aplicabilidade da "teoria das infraestruturas essenciais" à luz da jurisprudência do Tribunal de Justiça da União Europeia.

De acordo com a literatura mais recente, as soluções de Inteligência Artificial (doravante IA) na área do Direito podem ser agrupadas numa de três áreas: análise documental, investigação jurídica e automatização da prática profissional.[1] A automatização da prática profissional através de ferramentas de IA poderá trazer enormes ganhos de produtividade e uma mudança fundamental nas profissões jurídicas, com a possível automatização na redação de peças processuais.[2]

A título de exemplo, a ferramenta *PerfectNDA* da *Neota Logic* utiliza a plataforma de IA da empresa para simplificar o processo de criação de acordos de confidencialidade, a *LegalMation* automatiza a criação de vários documentos processuais relativos a litígios judiciais, nomeadamente requerimentos probatórios; a *WeVorce* e a *Hello Divorce* automatizam os processos relacionados com divórcios. No Reino Unido, a *Keoghs* procede à automatização de pedidos indemnizatórios.[3]

O conceito de *dataset* encontra-se plasmado no artigo 2.º, n.º 10.º da Diretiva 2019/1024, relativa aos dados abertos e à reutilização de informações do setor público, no qual a Diretiva define o conceito de "*high-value dataset*" (ou na tradução para português "Conjuntos de dados de elevado valor"): *"documentos cuja reutilização está associada a importantes benefícios para a sociedade, o ambiente e a economia, nomeadamente devido à sua adequação para a criação de serviços, aplicações e novos empregos dignos e de*

---

[*] Mestre em Direito e Informática pela Universidade do Minho.

[1] Marcos Eduardo Kauffman e Marcelo Negri Soares, "AI in Legal Services: New Trends in AI-Enabled Legal Services," *Service Oriented Computing and Applications* 14, no. 4 (Dezembro, 2020): 223–26, https://doi.org/10.1007/s11761-020-00305-x.

[2] "It is predicted that within ten to fifteen years software will routinely generate the first draft of most transactional documents" (…) computer generated-drafts could prove to be valuable and comparable to the efforts of associates who generate drafts that an experienced legal practitioner can then edit and refine for a valid final product" in Sergio David Becerra, "The Rise of Artificial Intelligence in the Legal Field: Where We Are and Where We Are Going", *J. Bus. Entrepreneurship & L.*, v. 11 no. 27 (2018), https://digitalcommons.pepperdine.edu/jbel/vol11/iss1/2

[3] Eduardo Kauffman and Marcelo Negri Soares, "AI in Legal Services: New Trends".

alta qualidade com valor acrescentado e ao número de potenciais beneficiários desses serviços e aplicações neles baseados".[4]

Face à definição supra, poderemos enquadrar o conceito de *dataset* (ou "conjuntos de dados") como integrando o conceito de "base de dados", como definido na Directiva 96/9/CE relativa à protecção jurídica das bases de dados: *"uma colectânea de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros".*[5]

A importância dos *datasets* jurídicos poderá ser demonstrada pela empresa *LegalAI*, uma empresa alemã que automatiza a análise de casos judiciais relativos a direito do consumo, da seguinte forma:

1) o consumidor/demandante visita o *website* da *LegalAI* e preenche um questionário *online* com os detalhes do seu caso,[6]

2) utilizando ferramentas de *Natural Language Processing,* a *LegalAi* procede a uma análise de casos anteriores semelhantes, produzindo uma análise jurídica automatizada,[7]

3) A análise automatizada é utilizada para intimar a empresa incumpridora, sendo alegado o incumprimento das normas de direito do consumo relevantes.[8]

A *LegalAI* treinou o seu algoritmo utilizando uma base de dados de 3 000 casos proveniente de uma sociedade de advogados especializada em direito do consumo, utilizando também dados disponíveis publicamente.[9]

Os *datasets* são essenciais para os sistemas de IA em dois momentos: como material de treino para a criação de algoritmos e como *input* para a sua utilização.[10] No caso da *LegalAi*, o material de "treino" corresponde à base de dados de direito de consumo utilizada para treinar o algoritmo. O material de *input* corresponde aos dados introduzidos pelo consumidor no *website* da empresa através do referido questionário *online.*

Pela sua importância, os *datasets* jurídicos poderão consubstanciar uma barreira à entrada para potenciais concorrentes que queiram criar os seus próprios sistemas de IA na área jurídica. A detenção de dados já foi considerado no passado como um obstáculo à entrada: na decisão Google (Shopping), a Comissão Europeia entendeu que os dados de pesquisa detidos pela Google constituíam uma barreira à entrada para outros potenciais agentes no mercado.[11] No contexto jurídico, a literatura descreve a

---

[4] Artigo 2.º, n.º 10 da Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público, *OJ L 172* (2019), http://data.europa.eu/eli/dir/2019/1024/oj/por.

[5] Artigo 1.º, n.º 2 da Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à protecção jurídica das bases de dados, *OJ L 077* (1996). http://data.europa.eu/eli/dir/1996/9/oj/por.

[6] "They come to LegalAI and fill in an online questionnaire", em artificiallawyer, "'LegalAI' Automates Consumer Case Assessment," Artificial Lawyer (blog), 27.04.2021, https://www.artificiallawyer.com/2021/04/27/legalai-automates-consumer-case-assessment/.

[7] "Using NLP analysis to match previous claims of a similar nature with the new dispute, LegalAI then provides an automated case assessment", em artificiallawyer, "'LegalAI' Automates".

[8] "The assessment can then be used to make a claim against a company, for example, a package holiday provider", em artificiallawyer, "'LegalAI' Automates".

[9] "At present they have trained their NLP models on legal data for 3,000 cases from a law firm that does consumer law, and they have also accessed public data", em artificiallawyer, "'LegalAI' Automates".

[10] Eduardo Kauffman and Marcelo Negri Soares, "AI in Legal Services: New Trends".

[11] Commission Decision in Case AT.39740 — Google Search (Shopping) "6.2.2. Barriers to entry and expansion. (285) The Commission concludes that the national markets for general search services are characterised by the existence of a number of barriers to entry and expansion. (…) (287)

falta de *datasets* jurídicos como um dos obstáculos ao desenvolvimento e utilização de algoritmos de IA na prestação de serviços jurídicos.[12]

Face a esta problemática, elencamos duas possíveis soluções: a implementação de uma política de dados abertos na área da Justiça e aplicabilidade da "teoria das infraestruturas essenciais" aos *datasets* jurídicos.

Relativamente a bases de dados de jurisprudência, enquanto que em Portugal as decisões de Tribunais Superiores e dos Julgados de Paz se encontram publicamente disponíveis, as decisões dos tribunais de primeira instância não o estão.[13] Além disso, Portugal não possui um quadro jurídico que enquadre a publicação online das decisões judiciais.[14] Por conseguinte, teremos de atentar se a jurisprudência disponível em www.dgsi.pt (ou outras bases de dados públicas em linha) constitui uma amostra representativa das decisões judiciais proferidas pelos tribunais em Portugal.

De acordo com as estatísticas disponibilizadas pelo Tribunal Constitucional, o número total de casos decididos pelo Tribunal Constitucional em 2019 foi de 1683. Ao pesquisar o ano de 2019 na sua base de dados online, é possível verificar que apenas 785 casos foram publicados online.[15]

Relativamente ao Supremo Tribunal de Justiça, de acordo com as estatísticas do Ministério da Justiça, o Supremo emitiu 1463 decisões de recurso ("Recursos de Revista") relativas ao ano de 2019, mas apenas 785 foram publicadas online.[16]

Com respeito aos Tribunais de Recurso ("Tribunais da Relação"), 14.948 decisões de recurso ("Recursos de Apelação") foram decididas em 2019, mas apenas 3643 decisões foram publicadas online (um rácio de cerca de 5 para 1 decisões/decisões publicadas).[17]

Para além da quantidade dos dados, o que também é relevante avaliar é a qualidade dos mesmos. Em Portugal, as decisões judiciais só estão disponíveis no formato (X) HTML. Outros formatos, como o XML, seriam preferíveis como um formato de dados abertos para reutilização, uma vez que metadados como data, a decisão final e outras partes relevantes, poderiam ser mais facilmente codificadas como parte de um ficheiro XML.[18]

Second, because a general search service uses search data to refine the relevance of its general search results pages, it needs to receive a certain volume of queries in order to compete viably. The greater the number of queries a general search service receives, the quicker it is able to detect a change in user behaviour patterns and update and improve its relevance", disponível em https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf

[12] "The development and use of AI algorithms in the provision of legal services is limited by a lack of easily accessible and analyzable datasets", em Marcos Eduardo Kauffman e Marcelo Negri Soares, "AI in Legal Services: New Trends".

[13] Disponível em: www.dgsi.pt

[14] Marc van Opijnen *et al.*, "On-Line Publication of Court Decisions in the EU: Report of the Policy Group of the Project 'Building on the European Case Law Identifier`", SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 15.02.2017, https://doi.org/10.2139/ssrn.3088495.

[15] TC > Tribunal Constitucional > Estatísticas", acesso em 1.07.2021, https://www.tribunalconstitucional.pt/tc/tribunal-estatisticas.html.

16 Data from 01/01/2019 to 31/12/2019 in "ECLI - Jurisprudência Portuguesa", acesso em 7.07.2021, https://jurisprudencia.csm.org.pt/.

[17] "Recursos Cíveis Findos Nos Tribunais Judiciais Superiores", acesso em 7.07.2021, https://estatisticas.justica.gov.pt/sites/siej/pt-pt/Paginas/Recursos-civeis-findos-nos-tribunais-judiciais-superiores.aspx.

[18] "File Formats", acesso em 23.06.2021, http://opendatahandbook.org/guide/en/appendices/file-formats/. "Recommendation 20: For reuse purposes court decisions should be made available in the most optimal computer-readable format possible, given the capabilities of the drafting process. JSON or RDF/XML are preferred" in Marc van Opijnen *et al.*, "On-Line Publication of Court Decisions in the EU", 151.

A aplicação da denominada "teoria das infraestruturas essenciais", poderá apresentar-se como uma outra solução para a disponibilização de *datasets* jurídicos. Esta teoria jurídica, emanada do artigo 102 do Tratado sobre o Funcionamento da União Europeia, permite que, em circunstâncias excepcionais, uma empresa dominante não possa recusar o acesso a um bem indispensável para outras empresas que desejem competir.[19] Esta doutrina teve a sua origem nos EUA, no caso *Terminal Railroad Association*,[20] onde o *Supreme Court* ordenou à *Terminal Railroad Association* - uma empresa que controlava todos os cruzamentos ferroviários locais no rio Mississippi (uma infra-estrutura de "estrangulamento"/*bottleneck*) - que concedesse aos seus concorrentes o acesso a esta infra-estrutura crítica.[21] Esta teoria é no entanto, aplicável não apenas a infraestruturas físicas – como caminhos de ferro ou aeroportos – mas também a bens intangíveis protegidos por direitos de propriedade intelectual.[22]

De acordo com a Diretiva 96/9/CE**,** "*as bases de dados que, devido à selecção ou disposição das matérias, constituam uma criação intelectual específica do respectivo autor, serão protegidas nessa qualidade pelo direito de autor*".[23] Uma base de dados poderá implicar um trabalho intelectual original - ao serem selecionados determinados dados em detrimento de outros - e consequente ser protegida por direitos de autor.[24] Por outro lado, a Diretiva referida prevê igualmente um direito *sui generis* relativamente a bases de dados que resultem de um "*investimento substancial do ponto de vista qualitativo ou quantitativo*".[25] Uma base de dados constituída por *datasets* jurídicos poderia teoricamente ser protegida por ambos estes direitos.

Em *Microsoft*, um caso relativo à recusa da *Microsoft* em licenciar a sua informação de interoperabilidade a concorrentes, o Tribunal Geral da União Europeia resumiu as circunstâncias exceptionais em que uma empresa dominante poderá ser obrigada a permitir o acesso a um produto ou serviço:

> *"- em primeiro lugar, o facto de a recusa dizer respeito a um produto ou um serviço indispensável para o exercício de determinada actividade num mercado derivado;*
> *- em segundo lugar, o facto de a recusa ser susceptível de excluir toda e qualquer concorrência efectiva nesse mercado derivado;*

---

[19] Inge Graef, Rethinking the Essential Facilities Doctrine for the EU Digital Economy (Abril, 2019), TILEC Discussion Paper No. DP2019-028, https://ssrn.com/abstract=3371457 or http://dx.doi.org/10.2139/ssrn.3371457

[20] Brett Frischmann e Spencer Weber Waller, "Revitalizing essential facilities", *Antitrust Law Journal*, v. 75, no. 1 (2008); Nikolas Guggenberger, "The Essential Facilities Doctrine in the Digital Economy: Dispelling Persistent Myths", *Yale J.L. & Tech*, v. 23, no. 301 (2021); Marina Lao, "Search, essential facilities, and the antitrust duty to deal", *11 Northwestern Journal of Technology and Intellectual Property*, v. 276, no. 288 (2013); Robert Pitofsky *et al.*, "The Essential Facilities Doctrine under U.S. Antitrust Law", *Antitrust Law Journal*, v. *70*, (2002); James R. Ratner, "Should there be an essential facility doctrine", U.C. Davis L. Rev., v. 21 (1988); David Reiffen e Andrew N. Kleit, "Terminal railroad revisited: foreclosure of an essential facility or simple horizontal monopoly?, J.L. & Econ., v. 33 (1990); Zachary Abrahamson, "Essential Data", Yale L.J., v. 124 (2014).

[21] Guggenberger, Nikolas, "Essential Platforms", *Stanford Technology Law Review*, Yale Law & Economics Research Paper, 30.09.2020, https://ssrn.com/abstract=3703361 or http://dx.doi.org/10.2139/ssrn.3703361

[22] *Ibid.*

[23] Artigo 3.º, Diretiva 96/9/CE.

[24] Pedro Dias Venâncio, "Notas sobre o regime do Direito Especial do Fabricante de Bases de Dados", Actas do IV Congresso Internacional Ciências Jurídico-Empresariais, Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria, 2014, pp. 22-37, 2014.

[25] Artigo 7.º, Diretiva 96/9/CE.

- em terceiro lugar, o facto de a recusa constituir um entrave ao lançamento de um produto novo para o qual exista uma procura potencial por parte dos consumidores."[26]

O primeiro requisito, relativo à indispensabilidade do bem, é geralmente considerado como sendo particularmente difícil de se verificar.[27] Na decisão da Comissão relativa à aquisição da *DoubleClick* pela *Google*, a Comissão afirmou que os dados da *Google* e da *DoubleBlick* não eram essenciais para a prestação de serviços de publicidade num ambiente *online,* visto que dados semelhantes já se encontravam disponíveis para os concorrentes da *Google* (*Yahoo e Microsoft*) e estes dados poderia ser também adquiridos a entidades terceiras.[28]

Quanto a *datasets* jurídicos, interrogamo-nos se estes poderiam ser adquiridos a terceiros, na mesma forma que os dados de pesquisa (*search data*), especialmente se determinadas sociedades de advogados possuírem uma grande coleção de documentos que seja específica a um determinado ramo do direito, como visto no caso da *LegalAI*, não sendo tal base de dados replicável.

Por outro lado, o requisito de indispensabilidade foi de certa forma reduzido pelo Tribunal Geral em *Microsoft*. Enquanto que o TJUE em *Bronner* afirmou que um bem não seria considerado essencial na existência de outras alternativas economicamente viáveis para a empresa concorrente,[29] no caso *Microsoft* o Tribunal Geral afirmou que os concorrentes deveriam ser colocados em "pé de igualdade".[30]

Quanto ao segundo requisito, relativo à exclusão de concorrência em mercados derivados, em *IMH Health,* relativo a uma licença para uma estrutura de tijolos protegida por propriedade intelectual, o TJUE afirmou que o facto do *input* requerido nunca ter sido vendido separadamente não impede que seja possível identificar um mercado autónomo e de ser aplicada a teoria das infraestruturas essenciais.[31] O TJUE afirmou que "*basta que um mercado potencial, ou mesmo hipotético, possa ser identificado. Assim sucede quando os produtos ou serviços sejam indispensáveis para exercer uma determinada actividade e que exista, para estes, uma procura efectiva pelas empresas que decidem exercer a actividade para a qual aqueles são indispensáveis*.".[32]

---

[26] Caso T-201/04 EU:T:2007:289, par. 332.

[27] "Nevertheless, a significant legal burden has to be met in order to force a dominant platform provider to give competitors access to its data under European competition law. Especially the requirement of indispensability which demands that there are no economically viable alternatives for the required input seems hard to meet." in Inge Graef; Sih Yuliana Wahyuningtyas e Peggy Valcke, "Assessing access problems in online media platforms", 24th European Regional Conference of the International Telecommunications Society (ITS): "Technology, Investment and Uncertainty", Florence, Italy, 20th-23rd October, 2013, International Telecommunications Society (ITS), Calgary, 2014.

[28] Inge Graef; Sih Yuliana Wahyuningtyas e Peggy Valcke, "Assessing access problems in online media platforms", ver também Case No COMP/M.4731 – Google/ DoubleClick (Google/DoubleClick), 11.03.2008, par. 366.

[29] "For such access to be capable of being regarded as indispensable, it would be necessary at the very least to establish, as the Advocate General has pointed out at point 68 of his Opinion, that it is not economically viable to create a second home-delivery scheme for the distribution of daily newspapers with a circulation comparable to that of the daily newspapers distributed by the existing scheme.", in Caso C-7/97 Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs [1998] ECR I-7791, par. 45.

[30] Caso T-201/04 Microsoft v. Commission [2007] ECR II-3601(Microsoft), par. 230. See also Inge Graef, Sih Yuliana Wahyuningtyas e Peggy Valcke, "Assessing access problems in online media platforms".

[31] Caso C-418/01 *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG*, ECLI:EU:C:2004:257, par. 42-43.

[32] Caso C-418/01 *IMS Health GmbH & Co. OHG v. NDC Health GmbH & Co. KG*, ECLI:EU:C:2004:257, par. 44.

No caso dos *datasets* jurídicos, poderá ser afirmado que estes não são (ou melhor, não serão) vendidos separadamente da prestação de serviços jurídicos. No entanto, como podemos verificar através da jurisprudência do TJUE, este facto não impede a aplicação da teoria das infraestruturas essenciais.

Quanto ao terceiro requisito, isto é, que a recusa impeça o surgimento de um novo produto, é suficiente que o "desenvolvimento técnico" seja prejudicado. Como afirmado pelo Tribunal Geral em *Microsoft*, não é necessário que um novo produto seja impedido de emergir.[33]

Em suma, no caso de *datasets* jurídicos, poderá ser entendido que 1) os *datasets* são indispensáveis à criação de algoritmos de IA, visto que estes dados não poderão ser adquiridos a terceiros; 2) a recusa em conceder o acesso a estes *datasets* poderá impedir a concorrência nos mercados derivados, nomeadamente no mercado a jusante de algoritmos; 3) a recusa em conceder o acesso a estes dados irá prejudicar o desenvolvimento técnico, neste caso, o desenvolvimento de algoritmos de AI na área do Direito e a prestação de novos serviços jurídicos.

Poderá ser estabelecido um paralelo com o caso da *Thomson Reuters Enterprise Centre Gmbh e West Publishing Corporation vs. Ross Intelligence Inc.*.[34]

A *ROSS Intelligence*, uma empresa de AI, alega que a *Westlaw* (uma editora jurídica, propriedade da Thomson Reuters) está a abusar da sua posição dominante no mercado da investigação jurídica, proibindo outras empresas de utilizar a sua base de dados em decisões judiciais. A ROSS cita a Secção 2 da Lei *Sherman*, que é o equivalente dos EUA ao artigo 102 do TFUE.

A *ROSS* alega que a "*Westlaw controla a maior, mais abrangente, e mais fiável base de dados jurídica, mas apenas disponibiliza essa base de dados àqueles que também licenciam as suas ferramentas de pesquisa legal através da plataforma Westlaw*". E que a "*Westlaw negou à ROSS o acesso à plataforma Westlaw e, portanto, também à base de dados jurídica*".[35]

Curiosamente, a *Westlaw* não vende a sua base de dados separadamente, mas apenas em conjunto com as suas ferramentas de pesquisa jurídica. No entanto, como vimos supra, este facto não significa que a base de dados não possa ser considerada como parte de um mercado autónomo.

Por outro lado, de assinalar também que a *ROSS* afirma que "*estas condições restritivas de licenciamento asfixiam a inovação (...) as novas empresas encontrariam formas de incorporar a base de dados Westlaw nos seus produtos, ou de construir tecnologia que permita que os seus motores de busca sejam compatíveis com a base de dados Westlaw*".[36] Este argumento é bastante semelhante ao citado pelo Tribunal Geral

---

[33] "Há que referir que a circunstância relativa ao lançamento de um produto novo, tal como é interpretada nos acórdãos Magill e IMS Health, referidos no no. 107, não pode constituir o único parâmetro para determinar se uma recusa de conceder uma licença sobre um direito de propriedade intelectual é susceptível de causar prejuízo aos consumidores na acepção do artigo 82.o, segundo parágrafo, alínea b), CE. Como resulta da redacção dessa disposição, esse prejuízo pode decorrer de uma limitação não só da produção ou da distribuição, como também do desenvolvimento técnico" em Caso T-201/04 *Microsoft v. Commission* [2007] ECR II-3601(*Microsoft*), par. 647

[34] "Amended ANSWER to 1 Complaint, with Jury Demand [Amended Partial Answer and Defenses], Amended COUNTERCLAIM against Thomson Reuters Enterprise Centre GmbH, West Publishing Corporation by ROSS Intelligence Inc for Thomson Reuters Enterprise Centre GmbH et al v. ROSS Intelligence Inc. :," Justia Dockets & Filings, acesso em 28.04.2021, https://docs.justia.com/cases/federal/district-courts/delaware/dedce/1:2020cv00613/72109/24.

[35] *Idem*.

[36] *Idem*.

no caso *Microsoft*, relativamente ao facto de uma recusa de acesso a um bem poder impedir o desenvolvimento técnico.

A análise encetada no presente texto assume-se como um exercício especulativo: não existe ainda jurisprudência europeia sobre a problemática descrita, podendo apenas ser feito um enquadramento teórico dos argumentos jurídicos emanados da teoria das infraestruturas essenciais e uma adaptação dos mesmos à nova realidade tecnológica dos *datasets* jurídicos. No entanto, o caso *Westlaw vs. Ross Intelligence,* a decorrer nos tribunais estado-unidenses, poderá apresentar-se como um caso pioneiro nesta matéria. É possível que, no futuro, os argumentos jurídicos utilizados pela *ROSS* sejam replicados nos tribunais europeus.

A sociedade de controlo na nova era digital

Francisco Salvador Gil García[*]

I. A segurança na nova era digital

Nos últimos anos, a literatura tem demonstrado mais interesse na segurança através das questões conexas ao "policiamento", "vigilância" e "medo do crime".[1] Embora a segurança tenha múltiplos significados e seja utilizada numa grande variedade de contextos na visão de Waldron,[2] as regulamentações nacionais têm-se concentrado cada vez mais em tentar evitar, controlar e prevenir o crime no nosso âmbito social. De fato, os professores Wood e Shearing[3] têm afirmado que a governação da segurança, através da criminalidade, ocupa a maior parte dos nossos esforços. Esta abordagem sobre a criminalidade suscitou preocupações importantes sobre os limites do poder do Estado soberano para manter a ordem pública.[4] A consequência de tudo isto é que a polícia tornou-se só um agente a mais da segurança, o que significou que um número crescente de outros actores tem assumido tarefas e responsabilidades relacionadas com a nossa segurança. Como afirma Schuilenburg,[5] a privatização da nossa sociedade foi acompanhada de novas formas de vigilância, relações de poder e punições. Para fornecer uma visão geral, tentaremos explicar a base da actual transformação de uma sociedade soberana e independente para uma sociedade de controlo cativada pela segurança.[6] Neste contexto, têm surgido recentemente novas correntes filosóficas e culturais que produzem leis desvitalizantes do cativeiro humano. Por esta razão, uma visão

[*] Professor de Direito Processual, Universidade de Sevilha (Espanha).

[1] Sobre estas questões, veja-se Les Johnston e Clifford Shearing, *Governing Security: Explorations in Policing and Justice* (Abingdon: Routledge, 2003); Ian Loader e Neil Walker, *Civilizing Security* (Cambridge: Cambridge University Press, 2007); Lucia Zedner, *On Security* (Abingdon: Routledge, 2009); Marc Schuilenburg, *The Securitization of Society. Crime, Risk, and Social Order* (New York: New York University Press, 2015); Adam Crawford e Steven Hutchinson, "Mapping the contours of 'everyday security': Time, space and emotion", *The British Journal of Criminology*, v. 56, no. 6 (2016): 1184-1202; Francis Dodsworth, *The Security Society: History, Patriarchy, Protection* (United Kingdom: Palgrave Macmillan, 2019).

[2] Jeremy Waldron, "Safety and Security", *Nebraska Law Review*, v. 85, no. 2 (2011): 454–507.

[3] Jennifer Wood e Clifford Shearing, *Imagining Security* (Devon: Willan Publishing, 2007), 5.

[4] Na mesma linha, veja-se Ulrich Beck, *Risk Society: Towards a New Modernity* (London: Sage Publications, 1992); Manuel Castells, *The Information Age: economy, society, and culture, (Volume 1): the rise of the network society* (Oxford: Blackwell, 1996); Zygmunt Bauman, *Liquid Modernity* (Cambridge: Polity Press, 2000).

[5] Para maior interesse, veja-se Marc Schuilenburg, "The Security Society: On Power, Surveillance and Punishments", in *The Pre-Crime Society: crime, culture and control in the ultramodern age*, eds. Bruce Arrigo e Brian Sellers (Bristol: Bristol University Press, 2021), 50-51.

[6] No início dos 90, antes da hegemonia da Internet, Deleuze já nos dizia que "a tecnologia da informação e os computadores" constituem uma função das relações sociais, que conduzem ao surgimento de novas relações de poder, cfr. Gilles Deleuze, "Postscript on Control Societies", in *Negotiations*, ed. Gille Deleuze (New York: Columbia University Press, 1995), 180.

geral da experiência atual com a Covid-19 é essencial para que os fluxos ontológicos e as flutuações epistemológicas permitam uma análise detalhada da evolução do ser humano na era digital. De fato, as práticas, baseadas em directrizes que, mais tarde, se tornarão em leis, têm sua origem no cativeiro das formas de Platão,[7] incluindo as formas de abstracção humana e suas sequelas, segundo Arrigo e Polizzi.[8] Neste contexto social, Arrigo e Milovanovic[9] oferecem uma crítica radical da subjectividade e das forças constitutivas em que esta subjectividade gera uma "sociedade de cautivos"; daí que, quando os excessos deste cativeiro são mantidos em consciência, através de encontros dialógicos ou expressões materiais do mesmo, os excessos alimentam o cativeiro da sociedade. Este cativeiro social tem favorecido a crítica de Bigo[10] à "(in)segurança globalizada". A consolidação destas condições impede o nascimento de novas correntes de pensamento[11] e exclui o que Hardt e Negri[12] descreveram como a "multidão".

II. Rastreio e localização da população na era post-Covid

No contexto das respostas à gestão do Covid-19, surgiu um novo modelo de segurança, baseado no desenvolvimento dos sistemas da vigilância privada de rastreio e localização de contactos. Estes sistemas só serão considerados eficazes se gerarem um sistema de vigilância generalizada que compreenda territórios densamente povoados[13]

---

[7] Platão, *Republic* (trad. Waterfield, Oxford: Oxford University Press, 2008).

[8] Bruce Arrigo e David Polizzi, "Introduction to the special issue: on the laws of captivity", *New Criminal Law Review: An Interdisciplinary and International Journal*, v. 21, no. 4 (2018): 483-491.

[9] Esta crítica radical da forma prisional desconstrói a dualidade "acção humana/estrutura social" que sustenta a panótica criminal, cfr. Bruce Arrigo e Dragan Milovanovic, *Revolution in Penology: rethinking the society of captives* (New York: Rowman and Littlefield, 2009), 170-175.

[10] Nas últimas décadas, os discursos institucionais após os atentados do 11-S reforçaram a necessidade de globalizar a segurança que assumiu uma intensidade sem precedentes na história recente da humanidade. Estes discursos justificaram-se através da "insegurança mundial" ao qual se atribui o desenvolvimento de ameaças de destruição maciça, atribuídas às organizações terroristas ou outras organizações criminosas, quando existem governos que, no entanto, as apoiam. Como Bigo critica, esta *des-globalização* pretende tornar as fronteiras nacionais e obrigar a outros atores da esfera internacional a colaborar com o único objetivo de adquirir um maior controlo sobre a população, cfr. Didier Bigo, "Globalized (in)security: the field and the ban-opticon", in *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, eds. Didier Bigo e Anastassia Tsoukala (Abingdon: Routledge, 2008), 10.

[11] A ignomínia das condições de vida que nos são oferecidas surge do interior da nossa sociedade atual. Não nos sentimos fora do nosso tempo. De facto, não nos falta comunicação, antes temos demasiada comunicação. Por esta razão, o que nos falta é criação. Deste modo, pode-se argumentar que falta-nos resistência ao presente. Como Deleuze e Guattari salientaram, a "criação de conceitos" exige "uma forma futura", para "uma nova terra" e "pessoas que ainda não existem". A europeização não constitui um devir sem novas dificuldades e constantes desafios, mas apenas a história do capitalismo, que impede o desenvolvimento livre dos seres humanos numa sociedade dominada pelo digital, cfr. Gille Deleuze e Guattari, *What is Philosophy?* (New York: Columbia University Press, 1994), 108.

[12] Sobre as singularidades relativas ao conceito de "multidão", veja-se Michael Hardt e Antonio Negri, *Multitude: war and democracy in the age of empire* (New York: Penguin, 2004), 97-157.

[13] Vários estudos têm sugerido que o incremento dos níveis de controlo policial [veja-se, entre outros, John Bright, "The beat patrol experiment" (London: Home Office Police Research and Development Branch, Unpublished, 1969); e Geoge Kelling, Tony Pate, Duane Dieckman e Charles Brown, *The Kansas City Preventive Patrol Experiment* (Washington: Police Foundation, 1974)] ou mudanças nos métodos de vigilância preventiva, têm escasso efeito nas taxas de criminalidade. Embora nem sempre esteja claro que os níveis de policiamento tenham sido alterados nas experiências [veja-se as críticas de Richard Larson, "What happened to patrol operations in Kansas City? A review of the Kansas City preventive patrol experiment", *Journal of Criminal Justice*, v. 3 (1975): 267-297], as razões apresentadas para os efeitos limitados da vigilância são convincentes. Estes efeitos estão relacionados com a rara ocorrência de crime em comparação com as oportunidades para a sua comissão, representadas pelas

e cumpra com os objectivos de detecção e prevenção previstos para evitar a propagação da Covid-19. Em contraste com os sistemas tradicionais de segurança preventiva, a utilização de um sistema generalizado de vigilância privada que permite o rastreio e localização de contactos estreitos parece ser justificada por razões de saúde pública. De facto, numerosos países optaram no último ano pelo desenvolvimento desses sistemas de segurança conforme um modelo de vigilância baseado em aplicações de rastreio desenvolvidas por grandes empresas tecnológicas como a Google e a Apple. Diferentes governos propuseram assim um modelo de vigilância privada, no qual as empresas mais importantes do sector privado desenvolvem continuamente novas medidas de vigilância, negoceiam a implementação destas medidas com governos individuais, e actuam como guardiões da segurança e privacidade em matéria de protecção de dados.

A evolução deste modelo de segurança levanta inumeráveis questões sobre a relação de poder entre autoridades públicas e privadas[14] numa paisagem extraordinariamente volátil no qual o sector privado parece controlar o monopólio do desenvolvimento tecnológico e a vantagem competitiva quanto à eficácia[15] e compatibilidade destes sistemas com os padrões de protecção definidos pelas normas de privacidade e protecção de dados.[16] Contudo, isso não impede que o nascimento de um novo modelo de segurança baseado na vigilância preventiva, generalizada, privada e descentralizada continue colocando importantes reptos no campo da protecção dos direitos fundamentais.

1. Privacidade limitada

A recolha de dados sensíveis ou de carácter personal de um grande número de pessoas no âmbito dos sistemas de localização e rastreio coloca desafios significativos à privacidade e proteção de dados no era digital.[17] Em particular, existem actualmente numerosas preocupações em torno da recolha de grandes quantidades de dados pessoais

---

atividades dos cidadãos numa área geográfica densamente povoada. Mesmo que a polícia se concentre nos lugares mais perigosos, as probabilidades de apanhar um crime no momento da sua comissão são escassas. Em tudo caso, grande parte do crime tem lugar em locais privados ou ruas não vigiadas onde a polícia não se encontra presente [cfr. Ronald Clarke, "Situational crime prevention: its theoretical basis and practical scope", *Crime and Justice*, v. 4 (1983): 233].

[14] Alguns exemplos das reacções a nível estatal podem encontrar-se nas notícias publicadas em alguns jornais ou meios digitais. Entre outras, destacam as seguintes notícias: Vince Cable, "The tech titans must have their monopoly broken – and this is how we do it", *The Guardian*, de 20 de abril de 2018; "US tech giants accused of 'monopoly power", *BBC News*, 7 de outubro de 2020; Ievas Ilves, "Why are Google and Apple dictating now European democracies fight coronavirus?", *The Guardian*, 16 de junho de 2020; e James Clayton, "Google and Apple attacked on app store 'monopoly'", *BBC News*, 22 de abril de 2021.

[15] Em junho de 2020, o governo britânico foi forçado a abandonar o investimento no desenvolvimento de uma aplicação centralizada de rastreio de contactos de coronavírus, após ter gastado três meses e milhões de libras em tecnologia que os peritos tinham repetidamente avisado que não iria funcionar. Numa reviravolta embaraçosa, Hancock disse que a aplicação mudaria para uma alternativa mais eficaz oferecida pelas grandes empresas norte americanas de tecnologia móvel (vid. Dan Sabbagh e Alex Hern, "UK abandons contact-tracing app for Apple and Google model", *The Guardian*, 18 June 2020).

[16] eHealth Network, "Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States", Bruxelas, 15 de abril de 2020.

[17] Em relação aos desafios levantados pelo estabelecimento de um sistema de vigilância em massa pós-Covid sobre os princípios da confiança e da cidadania no uso dos metadatos, veja-se Rita Raley, "Dataveillance and Countervailance", in *'Raw Data' is an Oxymoron*, ed. Lisa Gitelman (Cambridge: MIT Press, 2013), 121-146; e Valsamis Mitsilegas, "Responding to Covid-19: surveillance, trust and the rule of law", Queen Mary Criminal Justice Centre blog series on *Responding to Covid-19: Surveillance, Trust and the Rule of Law*, 26 de maio de 2020.

que não se encontravam necessariamente relacionados com os fins para os quais foram coletados, os extensos períodos de retenção e a erosão do princípio da limitação da finalidade, que permite o acesso a estes dados por uma vasta gama de autoridades nacionais. Neste contexto, o respeito e a protecção do princípio da proporcionalidade são essenciais, porque os sistemas generalizados de vigilância em massa, seguimento e localização só deven ser utilizado se são proporcionais ao objectivo prosseguido e os meios empregados cumprem o padrão de protecção dos direitos fundamentais. Deste modo, a adopção de medidas invasivas da privacidade que constituem uma séria ingerência nos direitos fundamentais só pode ser considerado proporcional se se deseja evitar uma ameaça iminente para a saúde pública da população. Pelo contrário, seria discutível considerar a medida de segurança proporcional se só for justificada por motivos de segurança pessoal ou para geração de conhecimento científico cujo uso reputa-se a um futuro próximo.[18] Em todo o caso, deve ser essencial uma justificação detalhada para a introdução da vigilância em massa como um elemento de segurança nacional.

2. Confiança obrigada: persuasão, discriminação e estigmatização

A aceitação dos sistemas de vigilância de massa baseados em aplicações de rastreio e localização depende em grande medida da confiança e participação públicas. Durante meses num cenário de excepcionalidade, têm existido um debate sobre a natureza facultativa ou coerciva da participação cidadã. Em qualquer caso, o consentimento dos cidadãos para uma participação activa nos sistemas de localização e seguimento deve ser uma expressão de vontade livre, específica, informada e inequívoca que permita a qualquer usuário aceitar, através de uma declaração afirmativa clara e expressa, o tratamento dos seus dados pessoais. A este respeito, o TJUE indicou que tal consentimento ficaria certamente comprometido se os cidadãos não tivessem uma verdadeira escolha para se oporem ao tratamento dos seus dados pessoais ou as cláusulas contratuais tivessem induzido a erro.[19]

Neste contexto, é essencial que a pressão governamental através da persuasão não gere discriminação ou estigmatização social. Ao centrar-se nas classificações dos indivíduos, os autores explicam como o poder entendido como dano por Henry e Milovanovic[20] é institucionalmente legitimado a nível judicial. Como Arrigo, Bersot

[18] As medidas invasivas da privacidade que constituem uma intromissão nos direitos fundamentais só podem ser consideradas proporcionais se o objetivo for prevenir ou evitar uma ameaça iminente à saúde pública, a menos que sejam justificadas por outros motivos como a geração de conhecimento para seu uso futuro [cfr. Valsamis Mitsilegas, "5. The Privatisation of Surveillance in the Digital Age", in *Surveillance and Privacy in the Digital Age*, eds. Valsamis Mitsilegas e Niovi Vavoula (Oxford: European, Transatlantic and Global Perspectives, Hart, Bloomsbury, 2021), 152].

[19] TJUE de 17 de outubro de 2013 (apdo. 32), Quarta Secção, caso *Michael Schwarz contra Stadt Bochum*, processo C-291/12, ref. ECLI:EU:C:2013:670 e relator: J. Malenovský; de 13 de maio de 2014 (apdo. 67), Grande Secção, caso *Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEDP) e Mario Costeja González*, processo C-131/12, ref. ECLI:EU:C:2014:317 e relator: M. Ilešič; de 20 de dezembro de 2017 (apdos. 48-50), Segunda Secção, caso *Peter Nowak contra Data Protection Commissioner*, processo C-434/16, ref. ECLI:EU:C:2017:994 e relator: M. Ilešič; de 11 de noviembre de 2020 (apdos. 41, 45, 50 y 51), Segunda Secção, caso *Orange România SA contra Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, processo C-61/19, ref. ECLI:EU:C:2020:901 e relator: T. Von Danwitz.

[20] Como resposta às definições apresentadas nas últimas décadas, Henry e Milovanovic desenvolveram uma definição constitutiva de crime. As versões críticas das anteriores definições consensuais de crime concebidas de dano como lesão social impulsionaram a ideia de que as vítimas de danos são encontradas para além das definidas por lei [cfr. Paul Tappan, "Who is the Criminal?", *American Sociological Review*, v. 12, no. 1 (Fev., 1947): 96-102; e Herman Schwendinger e Julia Schwendinger,

e Sellers[21] resumiram, "*quando a lógica da gestão do risco governa a escolha, a acção, e o progresso, os esforços políticos que apoiam a experimentação e a inovação [...] são interpretados [...] como [elementos] perigosos. Este é o prisma perturbador [desde] o qual as práticas de confinamento total têm sido [...] decretadas, nutridas e sustentadas*" durante meses no ocidente. De facto, tais práticas têm sido consideradas recentemente inconstitucionais em alguns países europeus pelo seu impacto nos direitos fundamentais dos cidadãos.[22] Consequentemente, o legislador deve prestar muita atenção para não utilizar termos que impliquem o desrespeito ético ou moral dos cidadãos para um comportamento social mais ou menos aceitável. As possibilidades da vigilância como meio para classificar os cidadãos na era digital constitui um elemento crucial entre os estudiosos da vigilância maciça acrítica. Na década de 1990, o sociólogo Gandy[23] resumiu esta ideia como "*panoptic sort*", utilizando a conhecida expressão de Jeremy Bentham.[24] Esta tendência tem servido para empoderar uma "alta nobreza estatal"[25] com a intenção de impor disciplina de mercado e promover certas políticas como a privatização, a externalização[26] e a desregulamentação. De facto, o TJUE tem sido testemunha deste período que tem impulsado a posição das empresas de segurança que proporcionam serviços de biometria e utilizam bases de dados de usuários para traçar o perfil destes, classificando-os em categorias e depois discrimina entre as categorias, atribuindo oportunidades com base na classificação.

A emergência de novas tecnologias de vigilância e análise preditiva das que emana a classificação reforça o poder da discriminação destes desenvolvimentos através da introdução de bases de dados que servem "*para domar a indisciplina da discrição local e as práticas idiossincráticas através de normas, formulários, regras, caixas de verificação, procedimentos, requisitos de relatórios, etc*".[27] Esta vigilância preditiva baseada na

"Defenders of order or guardians of human rights?", *Issues in Criminology*, v. 5, no. 2 (1970): 123-157]. Assim, alertaram-nos sobre a excessiva confiança depositada durante tanto tempo no conceito de "indivíduo" como único destinatário do dano, uma vez que o dano também pode ser dirigido e experimentado por grupos e categorias sociais determinadas. Estes críticos também têm demonstrado que o dano pode ser criado por aqueles que detinham posições dominantes de poder ou autoridade na era digital. No entanto, estas críticas encontram os seus limites ao identificar entidades individuais ou coletivas específicas como abusadores em linha com o pensamento de Henry e Milovanovic, uma vez que as mesmas não são suficientes para definir com uniformidade o único elemento comum todas as formas de dano: o exercício do poder [cfr. Stuart Henry e Dragan Milovanovic, "Constitutive definition of crime: power as harm", in *What is crime?: Controversies over the nature of crime and what to do about it*, eds. Stuart Henry e Marc Lanier (Lanham: Rowman & Littlefield Publishers, 2001), 165-178].

[21] Bruce Arrigo, Heather Bersot e Brian Sellers, *The ethics of total confinement: a critique of madness, citizenship, and social justice* (New York: Oxford University Press, 2011), 4.

[22] Um exemplo é a STC de 31 de julho de 2021, Grande Secção, Recurso de inconstitucionalidade, no. 2054-2020, ref. BOE-A-2021-13032 e relator: Pedro José González-Trevijano Sánchez.

[23] Oscar Gandy, "Coming to terms with the Panoptic sort", in *Computers, surveillance and privacy*, eds. David Lyon e Elia Zureik (United States: University of Minnesota Press, 1996), 133.

[24] Jeremy Bentham, *Panopticon: postscript* (London: Panopticon Penitentiary-House, 1791), 222.

[25] Pierre Bourdieu, *La Noblesse d'État: grandes écoles et esprit de corps* (Paris, 1989).

[26] No seu conjunto, a análise de Bourdieu sobre a reificação do Estado e a sua concepção totalizante, não faz parte de um Estado que tem – pelo menos retoricamente – renunciado aos seus poderes e externalizado o maior número possível deles para o mercado, cfr. Alan Scott, "We are the State: Pierre Bourdieu on the State and the political field", *Rivista di Storia delle Idee*, v. 2, no. 1 (2013): 65-70.

[27] Nos últimos tempos, tem sido formulado numerosas críticas sobre o uso das bases de dados no âmbito da segurança. Seu funcionamento variável e contingente conduziu na prática ao desenvolvimento de múltiplos sistemas operacionais. Mas muitas destas críticas foram apresentadas contra os programas dos governos europeus independentemente das bases de dados serem ou não utilizadas como um

discriminação por classe corrói inevitavelmente a confiança recíproca da cidadania nas autoridades nacionais, europeias ou internacionais.[28] Assim, podemos dizer junto a Bonelli e Bigo[29] que, embora a lógica da justiça penal se baseie na análise do próprio indivíduo alegado infractor, a lógica da inteligência de antecipação do risco centra-se nos grupos. No entanto, o poder de tratar as pessoas de forma diferente dependendo de uma classificação produzida por um sistema informatizado é muito perigoso. Esta desconfiança mútua provocou a discriminação de numerosos cidadãos dos sistemas inovadores de seguimento e localização, seja por opção ou por falta de acesso à tecnologia,[30] e conduziu desgraçadamente à exclusão automática das áreas mais essenciais da vida diária. Essa desconfiança também gerou uma rejeição social significativa contra esses meios de controle; especialmente, pela gestão conjunta de autoridades públicas e privadas na coleta, tratamento e uso de seus dados pessoais.

Como se viu nas declarações dos tribunais constitucionais nacionais do nosso entorno geográfico, a sensação de estar constantemente vigiado ou sob suspeita gera grande incerteza na população. Esta preocupação é certamente condicionada pela dependência da utilização das novas tecnologias e das implicações destes para os direitos fundamentais sem uma consciência crítica que o permita em condições de equidade. Assim, embora alguns autores como Beer[31] tenham tentado promover as tecnologias que sustentam a pré-criminalidade como "visões de objectividade calculada", outros autores como Kitchin[32] têm assinalado que as novas formas de análise preditiva estão

---

solução ou como um suporte. Através de numerosos dispositivos governamentais, governos de todo o mundo procuram a conformidade, coerência e consistência nos seus programas locais para controlar a discrição da polícia local. Neste âmbito, as bases de dados constituem um desses dispositivos introduzidos como uma solução para lidar com esta diversidade funcional, cfr. Evelyn Ruppert, "The governmental topologies of database devices", *Theory, Culture and Society*, v. 29, nos. 4-5 (2012): 118.

[28] Para assegurar uma supervisão e regulação eficazes e manter, ao mesmo tempo, a confiança pública no aparelho de segurança estatal, é essencial – segundo Murray – que seja dada prioridade a transparência. As utilidades professadas das medidas em massa devem ser demonstradas mais claramente, e a sua avaliação de necessidade mais claramente abordada. A divulgação pública de certas atividades pode legitimamente ser restringida com base nas considerações de segurança nacional. Em todo o caso, "a transparência deve ser a regra e o sigilo a exceção" nesta matéria, cfr. Daragh Murray e Pete Fussey, "Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data", *Israel Law Review*, v. 52, no. 1 (2019): 53.

[29] Sobre a lógica da inteligência de antecipação do risco e a sua influência no processo penal, veja-se o estudo conjunto de Laurent Bonelli e Didier Bigo, *Mapping the European field of the professionals of security: a methodological note on the problematique*, Relatório de síntese dos seminários organizados em Sciences Po Paris, 10 de outubro e 9 de novembro de 2005, 37-38.

[30] Na sua análise do impacto discriminatório da aplicação Covid-19, o Instituto dos Direitos Humanos concluiu que uma conta suficiente deve ser tomada de pessoas para as quais o acesso a aplicações não é evidente por falta da alfabetização digital ou recursos financeiros, ou por razões de saúde ou incapacidade. Estes grupos não devem ser excluídos da aplicação Covid-19, cfr. Collegevoor de Rechten van de Mens, *Corona-apps moeten toegankelijk zijn voor iedereen,* Toegelicht, 10 abril 2020.

[31] A exploração da noção do algoritmo pode permitir-nos ver como os algoritmos também desempenham um papel essencial nos processos de ordem social, tanto em termos de como o algoritmo é usado para promover certas visões de objetividade calculada, como também em relação às mais vastas civilizações que este conceito pode ser usado para abrir, cfr. David Beer, "The social power of algorithms", *Information, Communication and Society*, v. 20, no. 1 (2017): 7.

[32] Como observam Montfort, Baudoin, Bell, Bogost, Douglass, Marino, Mateas, Reas, Sample e Vawter, o "[c]ódigo não é puramente abstrato e matemático; tem dimensões sociais, políticas e estéticas significativas", inerentemente enquadrado e moldado por todo o tipo de decisões, política, ideologia e materialidade do *hardware* e infraestruturas que decretam as suas instruções, cfr. Nick Montfort *et. al.*, *10 PRINT CHR$(205.5+RND(1)); : GOTO 10* (Cambridge: MIT Press, 2012), 3. Embora os programadores possam procurar manter um elevado grau de objetividade – sendo

frequentemente longe de ser neutras ou objetivas. Contudo, conhecer o funcionamento exacto destes sistemas não é uma questão simples, porque os algoritmos são formulados por empresas do sector privado que utilizam acordos de confidencialidade para impedir que a polícia revele a terceiros qualquer informação relacionada com o equipamento de vigilância como tem reconhecido Joh.[33] No entanto, argumenta Seaver, que o interesse não deve estar centrado "*na configuração específica de um algoritmo, em particular, num determinado momento, mas nos algoritmos de mundos mais persistentes, [assim] a evidência útil não esta[ria] vinculada ao segredo empresarial*".[34] Em cualquer caso, os sistemas de vigilância em massa operam conforme a decisões ou avaliações algorítmicas de natureza automática, que reduzem em grande medida e, às vezes, eliminam a possibilidade de impugnar os seus resultados ou proporcionar uma solução eficaz aos indivíduos afectados.[35] Na mesma linha, também se podemos questionar, como fizeram Dencik,

distantes, desligados e imparciais da forma em que trabalham e atuando independentemente dos costumes, cultura, conhecimento e contexto locais [Theodore Porter, *Trust in numbers: the pursuit of objectivity in science and public life* (Princeton: Princeton University Press, 1995)] –, no processo de tradução num algoritmo, eles nunca poderão escapar totalmente a determinados aspectos. Nem podem escapar a fatores sociais e culturais nas escolhas e condicionalidades relacionadas com *hardware*, plataformas, banda larga e línguas [Rob Kitchin e Martin Dodge, *Code/space: Software and everyday life* (Cambridge: MIT Press, 2011); Nicholas Diakopoulos, *Algorithmic accountability reporting: on the investigation of black boxes* (Columbia: Columbia Journalism School, 2014); Daniel Neyland, "On organizing algorithms", *Theory, Culture & Society*, v. 32, no. 1 (2015): 119-132]. Na realidade, os algoritmos estão sujeitos a limitações que se refletem na quantidade de eleições que estes realizam diariamente, cfr. Tarleton Gillespie, "The relevance of algorithms", in *Media technologies: essays on communication, materiality, and society*, eds. Tarleton Gillespie, Pablo Boczkowski e Kirsten Foot (Cambridge: MIT Press, 2014) 167-193. Além disso, os algoritmos são criados para "procurar, combinar, ordenar, categorizar, agrupar, combinar, analisar, traçar o perfil, modelar, simular, visualizar e regular pessoas, processos e lugares", cfr. Rob Kitchin, "Thinking critically about and researching algorithms", *Information, Communication and Society*, v. 20, no. 1 (2017): 18.

[33] Os acordos de confidencialidade proíbem aos departamentos de polícia que utilizam tecnologia avançada de grandes companhias revelar "qualquer informação" dos sistemas operativos relativa aos equipamentos de vigilância a quaisquer terceiros, privados ou públicos, cfr. Elizabeth Joh, "The new surveillance discretion: automated suspicion, Big Data, and policing", *Harvard Law & Policy Review*, v. 10 (2016): 39; e Adam Lynn, "Defendant challenges use of secret "Stingray" cell device", *News Tribune*, 26 de abril de 2015, onde relata que a polícia Tacoma "recusou-se a discutir publicamente os detalhes da *Stingray*, citando um acordo de não divulgação com as autoridades federais que lhes forneceram a ferramenta"; tanto é assim, que a União das Liberdades Civis de Nova Iorque publicou, em abril de 2015, um acordo de confidencialidade que o FBI impôs à Oficina do Xerife no condado de Erie. Este acordo estabelecia que a Oficina do Sheriff "não distribuirá, divulgará, ou de outra forma divulgará qualquer informação ao público, incluindo a quaisquer indivíduos ou agências não policiais" (Carta de Christopher M. Piehota, Agente Especial responsável da Divisão de Buffalo adscrito ao FBI, a Scott R. Patronik, Chefe, Erie Cty. Oficina do Xerife, 29 de junho de 2012). Neste contexto, alguns procuradores optaram mesmo por retirar provas em alguns casos para não serem obrigados a revelar detalhes sobre a possível utilização desta tecnologia de vigilância, cfr. Elizabeth Joh, "The undue influence of surveillance technology companies on policing", *New York University Law Review Online,* v. 92, no. 19 (2017), apesar do facto de a divulgação pelo governo de provas materiais desculpatórias ou incriminatórias seja parte da garantia constitucional de um julgamento justo [*Brady v. Maryland*, 373 U.S. 83, 87 (1963); e *Giglio v. United States*, 405 U.S. 150, 154 (1972)].

[34] Uma grande quantidade de informação sobre os sistemas algorítmicos só estará disponível para quem não define o seu objeto de interesse como "*aquele que está fora dos limites [legais] ou intencionalmente escondido*" nos atos destinados a determinar a configuração específica do algoritmo que protege o segredo empresarial, cfr. Nick Seaver, "Algorithms as culture: some tactics for the ethnography of algorithmic systems", *Big Data and Society*, v. 4, no. 2 (2017): 7.

35 Até mesmo na situação atual, os indivíduos conservam o direito de não serem sujeitos a uma decisão que afeta-lhes significativamente e que se baseia exclusivamente no tratamento automatizado de dados pessoais sem que a sua própria opinião seja tida em conta. É evidente que implicações como

Hintz, Carey e Bucher,[36] até que ponto os princípios de responsabilização e transparência são minados, quando "*os algoritmos utilizados pela vigilância preditiva permanecem obscuros tanto para a polícia como para o público em geral*". De facto, deve-se, em grande medida, a esta obscuridade que se encontra subjacente nos sistemas algorítmicos, segundo Cukier e Mayor-Schonberger,[37] a sua objetividade, imparcialidade, fiabilidade e legitimidade na tomada de decisões.

2. Interoperabilidade privada

O uso de novas tecnologias no desenvolvimento de aplicações de localização de contactos coloca uma série de desafios de transparência e responsabilidade conjunta que são difíceis de resolver.[38] Estes desafios são agravados pela dependência demasiado acrítica da tecnologia do sector privado como mecanismos apropriados na procura de soluções simples para problemas extraordinariamente complexos. A confiança excessiva na tecnologia na busca incessante de soluções para os problemas actuais tem frequentemente efeitos adversos nos direitos fundamentais dos cidadãos. Ao mesmo tempo, estas preocupações têm ajudado a interligar os sistemas nacionais de vigilância

---

o autoisolamento e os testes podem ter efeitos significativos nesta matéria. Portanto, os usuários do sistema de localização e seguimento digital não devem ter consequências que lhes sejam impostas sem uma clara possibilidade de impugnar ou, pelo menos, questionar, sobretudo, se se tiver em conta as possíveis imprecisões levantadas ou deturpações causadas pelo uso de tais sistemas (Council Europe, "Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe", 28 April 2020).

[36] A maioria dos instrumentos utilizados pela polícia são sistemas comerciais obtidos fora dos produtos habituais que oferecem as empresas, cfr. Taina Bucher, "Want to be on the top? Algorithmic power and the threat of invisibility on Facebook", *New Media & Society*, v. 14, no. 7 (2012): 1164-1180. Este novo modelo de aquisição levanta inumeráveis questões em torno da responsabilização, uma vez que a configuração interna dos algoritmos utilizados para o policiamento preditivo que serve a prática profissional da polícia permanecem na sombra ao abrigo do segredo empresarial, cfr. Lina Dencick, Arne Hintz e Zoe Carey, "Prediction, pre-emption and limits to dissent: Social media and Big Data uses for policing protests in the United Kingdom", *New Media and Society*, v. 20, no. 4 (2017): 1445.

[37] Kenneth Cukier e Viktor Mayor-Schonberger, *Big Data: A revolution that will transform how we live, work and think* (New York: John Murray, 2013); Lina Dencick, Arne Hintz e Zoe Carey, "Prediction, pre-emption and limits to dissent: Social media and Big Data uses for policing protests in the United Kingdom", *New Media and Society*, v. 20, no. 4 (2017): 1436.

[38] Centro Europeu de Prevenção e Controlo das Doenças, *Rastreio de contactos: gestão da saúde pública de pessoas, incluindo profissionais de saúde, que tenham tido contacto com casos de COVID-19 na União Europeia – quarta actualização*, Estocolmo, 28 de outubro de 2021. O presente documento descreve as principais etapas para o rastreio de contactos, incluindo a identificação, a listagem e o seguimento dos contactos, no âmbito da resposta à Covid-19. Isto permitem ajudar as autoridades de saúde pública da UE/do EEE no rastreio e na gestão de pessoas, incluindo profissionais de saúde, que tenham tido contacto com casos de Covid-19. O objetivo da identificação e gestão dos contactos de casos prováveis ou confirmados de Covid-19 é identificar rapidamente casos secundários que possam surgir após a transmissão a partir de casos primários conhecidos, a fim de poder intervir e interromper a transmissão subsequente. Este objetivo é alcançado através: (i) da identificação imediata dos contactos de um caso de Covid-19 provável ou confirmado; (ii) da disponibilização de informações aos contactos identificados sobre autoquarentena, higiene adequada das mãos e medidas de etiqueta respiratória e de aconselhamento sobre como devem proceder se desenvolverem sintomas; (iii) da realização de testes laboratoriais em tempo útil a todos os que apresentam sintomas. E é que o rastreio de contactos constitui uma medida essencial para combater a epidemia de Covid-19 em curso, juntamente com a identificação ativa de casos e em sinergia com outras medidas, como o distanciamento físico. De facto, uma aplicação rigorosa e atempada de medidas de rastreio de contactos em áreas onde existem um número limitado de casos pode desempenhar um papel fundamental na limitação de uma maior propagação do surto. Se os recursos permitem, o rastreio de contactos também deve ser efectuado em localizações geográficas com mais transmissão generalizada.

relativos a Covid-19, sob o manto da interoperabilidade. A este respeito, os Estados-Membros, com o apoio da Comissão Europeia, adotaram uma recomendação relativa a um conjunto de instrumentos comuns ao nível da União com vista à utilização de tecnologias e dados para combater a crise da Covid-19, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados,[39] um conjunto de orientações de interoperabilidade para aplicações móveis de localização por contacto autorizadas no território da União Europeia,[40] assim como um conjunto de especificações técnicas relativas ao quadro de interoperabilidade transnacional relativa à aplicações de localização de contactos móveis.

A fim de apoiar a interoperabilidade e reforçar a confiança da cidadania nas autoridades nacionais, a Rede Europeia de Saúde em Linha da União Europeia em colaboração com as agências europeias, o Comité de Segurança da Saúde, a Organização Mundial da Saúde e outras instituições implementou uma série de "especificações técnicas detalhadas", com o objectivo de instaurar uma arquitectura informática de *backends* que permitem o "Rastreamento Europeu de Proximidade" através de um "Serviço de *Gateway* da Federação",[41] que aceita chaves de diagnóstico de todos os países, protege-as temporariamente, e fornece-as para que todos os países possam descarregar

[39] Recomendação (UE) 2020/518 da Comissão de 8 de abril de 2020 relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a crise da Covid-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados (*JOUE L 114*, 14.4.2020, 7-15). A presente recomendação estabelece um processo regulamentado para o desenvolvimento de uma abordagem comum, designada por «conjunto de instrumentos», para a utilização de meios digitais no combate à crise. Em particular, o conjunto de instrumentos consistirá em medidas práticas para uma utilização eficaz das tecnologias e dos dados, com especial incidência em dois domínios: (i) uma abordagem pan-europeia da utilização de aplicações móveis, coordenada a nível da União, para permitir que os cidadãos adotem medidas eficazes e específicas de distanciamento social, que facilitam o alerta, a prevenção, a deteção, o seguimento e o rastreio de contactos com o objetivo principal de limitar a propagação da doença Covid-19. Essa aproximação incluirá um método de seguimento e avaliação da eficácia das aplicações, da sua interoperabilidade e das implicações nos direitos fundamentais à privacidade e à proteção dos dados; e (ii) um sistema único de utilização de dados anonimizados e agregados relativos à mobilidade das populações, destinado a prever a evolução da doença, monitorizar a eficácia das decisões adotadas pelas autoridades nacionais europeias – como o distanciamento social ou o confinamento temporário –, e aprovar uma estratégia conjunta.

[40] eHealth Network, *Interoperability guidelines for approved contact tracing mobile applications in the EU*, Brussels, Belgium, 13 de maio de 2020, disponível no seguinte website: https://ec.europa.eu/health/sites/default/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf. Este documento aborda a primeira acção de seguimento prevista pela "Aplicações móveis para apoiar a localização de contactos na luta da UE contra a Covid-19, Caixa de Ferramentas Comum da UE para os Estados Membros Versão 1.0" ("Caixa de Ferramentas") da eHealth Network. Neste contexto, a maioria dos Estados Membros lançou uma aplicação de rastreio de contactos móveis, concebida para cumprir objetivos operacionais específicos da sua estratégia nacional de gestão de crises à Covid-19. Para efeitos deste documento, a interoperabilidade refere-se à possibilidade destas aplicações poderem compartilhar um mínimo de informação necessária para que os usuários da aplicação sejam alertados se tiverem estado na proximidade, dentro de um período relevante, com outro usuário que tenha notificado na aplicação de que deu positivo para a Covid-19. Este alerta e seguimento deve estar em conformidade com os procedimentos definidos pelas autoridades de saúde pública com possíveis implicações à privacidade e a segurança dos cidadãos.

[41] Vários padrões de interoperabilidade foram discutidos no documento intitulado "*European Interoperability-Conceptual View*". Contudo, o padrão preferido pela Rede Europeia de Saúde em Linha foi o Serviço do Portal da Federação Europeia, no qual cada *backend* nacional carrega as chaves dos cidadãos recentemente infetados ("chaves de diagnóstico") de duas em duas horas e descarrega as chaves de diagnóstico dos outros países que participam neste esquema de interoperabilidade pública.

os dados em tempo real. Neste contexto, a maioria dos países europeus desenvolveu aplicações de localização de proximidade para reduzir a propagação da Covid-19, geralmente utilizando a aplicação de notificações de exposição da Google e da Apple.[42] Sob estas aplicações, a União Europeia implementou um sistema de interoperabilidade privada com profundas implicações nos direitos fundamentais da cidadania europeia, como possa ser o direito à livre circulação. A adopção destes mecanismos de transmissão e troca de informação em tempo real facilitou a livre circulação e promoveu a segurança, alertando para uma possível exposição ao risco de contágio através de *backends* nacionais autónomos; daí que seja essencial, como manifestou o grupo de trabalho Covid+, alcançar um elevado nível de interoperabilidade entre os sistemas de informação nacionais.[43]

3. Interoperabilidade Pública

A implicação da interoperabilidade entre os diferentes sistemas de informação da União levanta numerosos desafios no ámbito dos direitos fundamentais.[44] Entre eles, destacam a interoperabilidade como uma questão puramente técnica, automática e passiva. Assim foi definido desde a primeira vez que a interoperabilidade foi apresentada pela Comissão em 2005[45] até ao projecto de gestão para a interoperabilidade dos

[42] Um aplicativo deste tipo foi lançado na Alemanha sob o nome "*Corona Tracing App*". Esta aplicação –elaborada a partir de Apple e Google, podendo os cidadãos descarregar voluntariamente de forma gratuita – documenta o encontro digital entre dois telefones inteligentes. A aplicação guarda então as suas *IDs Bluetooth* aleatórias (códigos aleatórios) por um tempo limitado. Estas identificações encriptadas (códigos aleatórios) não permitem tirar quaisquer conclusões sobre si ou sobre a sua localização. Desta forma, a aplicação móvel pode informá-lo particular e rapidamente se tiver tido contacto com uma pessoa que tenha dado positivo no teste Covid-19. Quanto mais depressa obtiver esta informação, menor será o risco de muitas pessoas ficarem infestadas. A aplicação também permite mostrar digitalmente o estado da vacinação, guardar um resultado de teste rápido e registar-se para eventos usando um código QR. Portanto, para além de medidas de higiene como a lavagem das mãos, manter a distância e as máscaras diárias, a aplicação é um meio eficaz de conter o coronavírus. O governo federal expressou publicamente o seu apoio a este pedido, alegando que ele serve a proteção e saúde da comunidade, cfr. Die Bundesregierung, *Die wichtigsten Fragen und Antworten*, Corona-Warn-App, 29 de outubro de 2021, disponível no seguinte website: https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392.

[43] Na plena evolução do Covid-19, os Estados Membros, com o apoio da Comissão, acordaram um conjunto de especificações técnicas para assegurar o intercâmbio seguro de informações entre as aplicações nacionais de localização de contactos, com base numa arquitetura técnica descentralizada. Uma vez implementada a solução técnica, tais aplicações nacionais funcionarão sem problemas quando os utilizadores viajarem para outro país da UE que também siga a abordagem descentralizada (cfr. eHealth Network Guidelines, "Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps", European Commission, Bruxelas, 16 de junho de 2020).

[44] Valsamis Mitsilegas, "Interoperability as a Rule of Law challenge", *Blog Forum on Interoperable Information Systems in Europe's Area of Freedom, Security and Justice*, European University Institute.

[45] Comunicação da Comissão ao Conselho e ao Parlamento Europeu relativa ao reforço da eficácia, da interoperabilidade e das sinergias entre as bases de dados europeias no domínio da justiça e dos assuntos internos, COM(2005) 597 final, de 24.11.2005. A Comunicação fornece uma definição de "interoperabilidade" como "a capacidade dos sistemas das tecnologias da informação e dos processos operacionais de que constituem o suporte para trocar dados e assegurar a partilha de informações e conhecimentos" (cfr. European Interoperability Framework for Pan-European eGovernment Services, "Quadro europeu de interoperabilidade para os serviços pan-europeus da administração em linha", Serviço das Publicações Oficiais das Comunidades Europeias, 2004, ponto 1.1.2). Segundo a Comissão, este é um conceito técnico e não jurídico/político. Esta ênfase na técnica tem sido criticada pela Autoridade Europeia para a Proteção de Dados na sua Opinião sobre a Comunicação da Comissão ao Conselho e ao Parlamento Europeu relativa ao reforço da eficácia, da interoperabilidade e das

sistemas de informaçao adoptado pela União, sob a supervisão de certas agências de natureza técnica.[46] A transição para um novo paradigma digital no tratamento e intercâmbio de dados pessoais no quadro da interoperabilidade levanta novas questões relativas à segurança nacional, que são reforçados pela opacidade ou maximização dos dados que a interoperabilidade visa fornecer. Como declarou o SEPD nas conclusões apresentadas na Opinião 4/2018, "os sistemas informáticos interoperáveis em grande escala causaram um impacto profundo e permanente na sua estrutura e modo de funcionamento, senão que também alteraram a forma como os princípios legais nesta área têm sido interpretados até agora, marcando assim um «ponto de não retorno»".[47]

Esta transição para um novo paradigma da interoperabilidade com base no fluxo incessante de dados coloca grandes desafios à cidadania, que terão de enfrentar uma considerável incerteza jurídica no que respeita à identificação das agências encarregadas do tratamento dos seus dados pessoais, assim como à escolha de vias de recurso mais eficazes contra o tratamento de dados pessoais pela administração responsável.

---

sinergias entre as bases de dados europeias no domínio da justiça e dos assuntos internos, cfr. European Data Protection Supervisor, *Comments on the Communication of the Commission on interoperability of European databases,* Bruxelas, 10 de março de 2006; na mesma linha, manifestou-se Valsamis Mitsilegas, "Border Security in the European Union – towards centralised controls and maximum surveillance", in *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy*, eds. Anneliese Baldaccini, Elspeth Guild e Helen Toner (United States: Bloomsbury, Hart Publishing, 2007), 393-394.

[46] As redes de inteligência no espaço de liberdade, segurança e justiça que resultam da política de interoperabilidade europeia são compostas por tipos bastante diferentes de entidades jurídicas da União Europeia. De facto, existem nós multiníveis e multi-atores que abrangem tanto o sector público como privado. A singularidade da interoperabilidade como sistema de relações entre diferentes autoridades reforça e incrementa os problemas de responsabilidade e transparência associados a diferentes tipos de administração. Deste modo, a interoperabilidade fortalece a obscuridade e a difícil responsabilização que resulta do carácter fragmentado da administração. Por este motivo, torna-se difícil identificar exatamente a que nível de erros de administração são cometidos. É também realmente difícil para o público ou as instituições não envolvidas nas redes interoperáveis exigir o acesso às mesmas e o processamento dos seus dados de acordo com as normas europeias. A afluência maciça de enormes quantidades de dados pessoais e não-pessoais determina sua confluência, favorece sua transmissão através de bases de dados interoperáveis e facilita a sua livre circulação. No entanto, este afluxo maciço mina o controlo dos dados até tal ponto que os utilizadores perdem o controlo absoluto sobre os seus dados nas redes de inteligência do espaço de liberdade, segurança e justiça da União, cfr. Deirdre Curtin, "Second order secrecy and Europe's legality mosaics, *West European Politics*, v. 41, no. 4 (2018): 856.

[47] A AEPD reconhece que, hoje mais do que nunca, existe a necessidade de partilhar melhor a informação e utilizar mais eficazmente os sistemas de informação em larga escala dentro da União Europeia para superar os desafios migratórios e fornecer uma resposta às questões que o terrorismo e a grave criminalidade nos colocam. No entanto, a necessidade de uma melhor exploração dos dados nunca deve conduzir à violação do direito fundamental à proteção de dados. A interoperabilidade não é nem deveria ser entendida como uma escolha técnica, mas sim como uma escolha política. Tendo como pano de fundo a clara tendência para misturar legislação e objetivos políticos distintos da União Europeia (como possam ser os controlos fronteiriços, asilo e imigração, cooperação policial e agora também cooperação judicial em matéria penal), bem como o acesso rotineiro às bases de dados não policiais, a decisão do legislador da União de tornar interoperáveis sistemas informáticos de grande escala não só afetaria permanente e profundamente a sua estrutura e a sua forma de funcionamento, como também alteraria e transformaria a forma como os princípios legais têm sido interpretados nesta área até agora e marcaria como tal um "ponto de não retorno". Por estas razões, a AEPD apela a um debate mais amplo sobre o futuro do intercâmbio de informações dentro da própria União Europeia, a sua governação e as formas de salvaguardar os direitos fundamentais neste contexto de volatilidade sistêmica, EDPS, *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, 16 de abril de 2018, 10.

III. Vigilância privada em grande escala na sociedade do risco súbito

Outras preocupações relacionadas com os direitos fundamentais decorrem dos esforços incessantes para amparar o novo paradigma da segurança através de vigilância privada baseada em aplicações com fins de gestão. A partir destos esforços, surge um novo movimento de protecção dos direitos fundamentais que permitiu aos provedores de telecomunicações facilitar uma série de dados dos clientes às autoridades nacionais com o objectivo não só de localizar e rastrear contactos, senão também de alcançar outros objectivos da política relativa à Covid-19.[48] À vista da jurisprudência do TJUE relativa à retenção de dados, pode-se afirmar que a compatibilidade das iniciativas de vigilância em grande escala com a legislação da União Europeia e a sua constitucionalidade são questionáveis na Europa atual.[49] Um exemplo de excesso no uso dos mecanismos de segurança existentes baseados na vigilância privada e o controlo da Covid-19 pode constatar-se nas recentes petições da Presidência alemã do Conselho da União aos Estados Membros para que comuniquem dados PNR com fins de seguimento e localização. A medida foi justificada pela necessidade de as autoridades nacionais terem acesso rápido à informação sobre a doença para controlar a sua propagação inicial.[50] Além das questões relativas à legalidade das transferências

[48] É precisamente este comportamento que Foucault quis definir quando argumentou que "o poder produz; produz a realidade; produz domínios de objectos e rituais de verdade". Neste aspecto, reside a difusão do poder como entidade garante de um tipo de microfísica e uma forma de biopolítica, cfr. Michel Foucault, *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (New York: Vintage, 1980). A primeira reduz o potencial do ser humano e eleva as suas ações a um estado panótico pré-criminal; enquanto a segunda reprime as relações de humanidade através da hermenêutica da governação da sociedade do risco que supõe a evolução do homem na era digital. Ambas as técnicas fomentam as tecnologias do mercado (como uma verdade compartilhada) e dominam as tecnologias da subjectividade (como uma liberdade negativa), cfr. Bruce Arrigo e Brian Sellers, "The 'risk' society thesis and the culture(s) of crime control", in *The pre-crime society: crime, culture and control in the ultramodern age*, eds. Bruce Arrigo e Brian Sellers (Bristol: Bristol University Press, 2021): 38-39. De facto, como Foucault observou, "ao pensar nos mecanismos do poder", que o poder é concebido como uma formulação sistémica que abarca diferentes processos que atingem a alma humana e determinam as suas acções e atitudes, assim como o itinerário de seus processos de aprendizagem e, por conseguinte, o devir de sua vida quotidiana, cfr. Foucault, op. cit., 39. É assim que o poder molda corpos de "utilidade abjecta", nos quais o sujeito se torna um "mero funcionário do Estado", cfr. Michel Foucault, *Discipline and punish: the birth of a prison* (New York: Pantheon, 1977), 210. A subjetividade torna-se moeda de câmbio no desenvolvimento cultural de uma população, emerge na consciência do risco abstrato de ser domesticada, encontra coerência narrativa no pensamento reflexivo individual e encarna-se no agente privado através da ação intencional do Estado.

[49] Resolução do Tribunal Constitucional da República Eslovaca de 13 de maio de 2020, Grande Secção, ref. PL. ÚS 13/2020-103 e relator: Ivan Fiačan. Neste caso, o Tribunal Constitucional Eslovaco pôs fim ao desenvolvimento de um contacto numa aplicação de rastreio que tinha desencadeado a preocupação sobre a necessidade de recolha de dados em massa, declarando inconstitucionais algumas secciones da lei de telecomunicações – recentemente modificada – que permitiram às autoridades estatais aceder aos dados de telecomunicações para efeitos de localização de contactos, cfr. Responses to the Covid-19 pandemic in the fields of non-discrimination, diversity and inclusion. Promising and good practice examples, ref. CDADI/2021 3rev, de 9 de março de 2021, 38).

[50] Uma das lições aprendidas com a experiência da pandemia da Covid-19 é que as autoridades competentes dos Estados Membros necessitam de informações suficientes disponíveis para lidar com a rápida propagação de uma doença. Esta necessidade levantam a questão mais vasta de como é o tratamento de dados PNR para fins de saúde pública, cfr. European Union Agency for Fundamental Rights, *Coronavirus Pandemic in the EU-Fundamental Rights Implications: with a foces on contact-tracing Apps*, Bulletin 2, março/abril de 2020, 47, uma vez que é sabido que as informações sobre os movimentos de viagem e dos contatos entre pessoas suspeitas de infecção torna-se vital para o

de dados PNR, estas propostas levantam a posibilidade de ampliar o sistema de vigilância em grande escala existente, cujos principais elementos de transferência no âmbito das relações externas da União Europeia foram considerados contrários à legislação europeia pelo TJUE.[51] As implicações no âmbito dos direitos fundamentais para apoiar a segurança preventiva em massa baseada nas aplicações de vigilância privada existentes são verdadeiramente significativas tendo em conta às crescentes reivindicações de uma vigilância privada cada vez maior na era digital.[52]

controlo em grande escala da doença. Os dados PNR que proporcionam os passageiros e a recolha e conservação das grandes companhias aéreas facilitariam o rastreio e o contacto das pessoas afetadas e favoreceria a tomada de decisões e medidas mais eficazes. No entanto, a utilização de dados PNR na luta contra pandemias levanta uma questão jurídica incontornável. O art. 1.2 da Directiva PNR só prevê que os dados recolhidos em conformidade com esta Directiva podem ser tratados para efeitos de prevenção, deteção, investigação e repressão de infrações terroristas e crimes graves. Desta forma, exclui seu uso para a proteção da saúde pública ou controle de doenças. Consequentemente, a sua utilização para tais fins exigiria a modificação da diretiva (Documento do Conselho no. 9031/20, de 2 de julho de 2020, 1).

[51] Na sua Opinião no. 1/15, o TJUE confirmou a possibilidade de ampliar o sistema de vigilância em grande escala existente, incluindo a transmissão de dados sensíveis como "a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical" ou sobre "a saúde e a vida sexual", desde que as Partes do acordo admitam esta possibilidade e independentemente de os princípios subjacentes ao envio da informação serem contrários aos valores da União Europeia, cfr. Opinião 1/15 do TJUE de 26 de julho de 2017 (apdos. 164-165), Grande Secção, parecer 1/15, ref. ECLI:EU:C:2017:592 e relator: T. von Danwitz.

[52] Na reunião do dia 7 de maio de 2021, os Conselheiros JAI concordaram o projeto de Conclusões do Conselho, sujeito ao aditamento estabelecido na primeira versão revista. Nenhuma observação foi submetida ao Secretariado-Geral dentro do prazo estabelecido (segunda-feira, 10 de maio de 2021, 13:00 hrs.). Além disso, não foram apresentadas observações dentro do prazo estabelecido (quarta-feira, 12 de maio de 2021, 10:00 hrs.) sobre a segunda versão revista, incluindo um segundo aditamento. Uma vez que nenhuma delegação notificou uma reserva sobre o projeto revisto de Conclusões do Conselho, a "Proposta de Conclusões do Conselho sobre a transferência de dados dos Registos de Identificação dos Passageiros (PNR) para países terceiros, em particular a Austrália e os Estados Unidos, para efeitos de combate ao terrorismo e à criminalidade grave" foi acordado em 11 de maio de 2021, cfr. Documento do Conselho no. 7376/2/21 REV 2, de 11 de maio de 2021 e aprovado, um dia mais tarde, em 12 de maio de 2021, cfr. Documento do Conselho no. 8635/21, de 12 de maio de 2021. Na reunião dos dias 7-8 de junho de 2021, o Conselho JAI publicou as Conclusões do Conselho em linha com as reivindicações dos direitos fundamentais num âmbito de forte vigilância policial. Um exemplo a mais da força destas exigências.

UNIO
EU LAW JOURNAL

Universidade do Minho

With the support of the Erasmus+ Programme of the European Union