Inteligência Artificial Como Oportunidade para a Regulação Jurídica[1]

WOLFGANG HOFFMANN-RIEM[2]

Bucerius Law School, Hamburg, Ex-Juiz do Tribunal Constitucional Federal da Alemanha.

RESUMO: No início do artigo, são apresentados exemplos de possibilidades de utilização de inteligência artificial (IA) e referências a dimensões de efeitos sobre a sociedade. O seu objeto são os desafios postos pela IA para o estabelecimento e a aplicação do Direito, particularmente de regulamentações jurídicas que preservem as oportunidades associadas com a IA, mas evitem ou ao menos minimizem possíveis riscos. O ordenamento jurídico precisa garantir a "boa governança digital", tanto para o desenvolvimento de sistemas algorítmicos de modo geral quanto para a utilização da IA em especial. Especialmente grandes são os desafios que se colocam para a regulação da utilização de algoritmos que operam por meio de aprendizado de máquina, como, por exemplo, no caso do *machine learning*. Particularmente difícil é garantir transparência, responsabilidade, imputabilidade e possibilidade de revisão posterior, bem como mitigar as possibilidades de discriminação (especialmente de discriminação oculta). O artigo sistematiza as abordagens regulatórias disponíveis. Ele enfatiza também que confiar no cumprimento de princípios éticos não é suficiente e que a regulação jurídica complementar é imprescindível também nas áreas caracterizadas, majoritariamente, pela autorregulação das empresas. Acentua-se, ainda, a necessidade de tratados e instituições transnacionais para lidar com o tema.

SUMÁRIO: 1 Exemplos de campos de aplicação de inteligência artificial; 2 Níveis de efeitos; 3 Referência ao Direito; 4 Modalidades de governança; 5 A assunção de responsabilidade pela garantia por meio de medidas visando à boa governança digital; 6 Obstáculos para o emprego eficaz do Direito; 7 Tipos de regulação e regulamentação; 8 Substituição ou complementação de medidas jurídicas por padrões extrajurídicos, particularmente éticos; 9 A necessidade de direito transnacional.

1 EXEMPLOS DE CAMPOS DE APLICAÇÃO DE INTELIGÊNCIA ARTIFICIAL

A contemporaneidade é marcada pela digitalização de muitas áreas da vida. Nela, a utilização de inteligência artificial (IA) contribui em especial para a transformação digital[3]. A IA é uma tecnologia transversal que visa capaci-

1 Traduzido por Luiz Sander e revisado por Laura Schertel Mendes.

2 Orcid: <https://orcid.org/0000-0003-1085-6673>.

3 A literatura sobre a transformação digital está amplamente dispersa. Veja, *pars pro toto*, T. Cole, *Digitale Transformation*, 2017; R. Pfliegl; C. Seibt, Die digitale Transformation findet statt, in: *Elektrotechnik und Informationstechnik*, p. 334, 2017; A. Rolf, *Weltmacht Vereinigte Daten*: Die Digitalisierung und Big Data verstehen, 2018; Kolany-Raiser et al. (Ed.), *Big Data und Gesellschaft*: Eine multidisziplinäre Annäherung,

tar computadores, mediante a utilização de grandes quantidades de dados (*big data*), capacidades computacionais apropriadas e processos específicos de análise e decisão, a alcançar realizações que se aproximam da capacidade humana ou até a superem ao menos em alguns aspectos[4].

A IA é empregada, por exemplo, em máquinas de busca, em plataformas de comunicação e robôs, no reconhecimento facial, em equipamentos inteligentes de gestão de tráfego, em decisões administrativas ou jurídicas tomadas de maneira automatizada, em sistemas automatizados de assistência para veículos, no diagnóstico e na terapia médicos, na *smart home* [casa inteligente], em sistemas de produção ciberfísicos (indústria 4.0), mas também na área militar. A ampliação de sistemas de análise e decisão que se baseiam em algoritmos e operam com IA possibilita formas novas de fiscalização e controle do comportamento[5], mas também novas espécies de ações criminosas[6].

Uma possibilidade de emprego de IA muito utilizada é o aprendizado de máquina. Esse termo se refere a "programas de computador que têm condições de aprender a partir da experiência e, assim, melhorar seu desempenho com o passar do tempo"[7]. O aprendizado de máquina é empregado para reconhecer padrões, avaliar e classificar imagens, traduzir linguagem para textos, produzir de maneira automatizada copiões de áudio e vídeo (por exemplo, "robôs jornalistas") e coisas semelhantes. Possibilidades mais avançadas ainda de utilização da IA são designadas por algumas pessoas com o termo *deep learning* [aprendizado profundo][8]. Nesse caso, os sistemas de TI que operam mediante o emprego de redes neuronais dispõem da capacidade de, aprendendo, continuar a escrever por conta própria os programas digitais inicialmente desenvolvidos por seres humanos e, com isso, desenvolver-se independentemente da programação humana.

Há oportunidades e riscos associados à ampliação da capacidade e possibilidades de utilização da IA. No que se segue, indaga-se a respeito dos desafios daí resultantes para o direito e a regulação[9].

2018; R. D. Precht, *Jäger, Hirten, Kritiker*: Eine Utopie für die digitale Gesellschaft, 2018. Como ilustração da multiplicidade das questões levantadas nesst contexto, v. os artigos no n. 10 de *Elektrotechnik und Informationstechnik*, p. 323-388, 2017.

4 Como introdução à IA: S. Russell; P. Norvig, *Künstliche Intelligenz:* Ein moderner Ansatz, 3. ed., 2012; J. Kaplan, *Artificial Intelligence*, 2016; M. Lenzen, *Künstliche Intelligenz*: Was sie kann & was uns erwartet, 2018; C. Misselhorn, *Grundfragen der Maschinenethik*, 2018.

5 W. Hoffmann-Riem, Verhaltenssteuerung durch Algorithmen – eine Herausforderung für das Recht, AöR, v. 142, p. 1-43, 2017.

6 C. M. Bishop, *Pattern Recognition and Machine Learning*, 2008; A. C. Müller; S. Guido, *Einführung in Machine Learning mit Python*, 2017.

7 H. Surden, Machine Learning and Law, *Washington Law Review*, v. 89, p. 89, 2014.

8 Por exemplo, I. Goodfellow; Y. Bengio; A. Courville, *Deep Learning*, 2016.

9 Para ter uma ideia da multiplicidade dos desafios e das propostas de solução, veja J. Jakobs, *Vernetzte Gesellschaft*: Vernetzte Bedrohungen. Wie uns die künstliche Intelligenz herausfordert, 2016; F.-U. Pieper, Künstliche Intelligenz: Im Spannungsfeld von Recht und Technik, *Zeitschrift zum Innovations- und*

2 NÍVEIS DE EFEITOS

Uma vez que muitas áreas da sociedade são permeadas pela digitalização, seria reducionista restringir as reflexões sobre o papel do direito e as possibilidades de regulação a aspectos avulsos – por exemplo, apenas as formas diretas de lidar com a IA, especialmente. A IA é um elemento parcial na utilização de sistemas de TI e pode ter, dependendo do contexto em que é aproveitada, uma importância diversificada para o tipo de processamento e o efeito sobre a ação. Em consonância com isso, os desafios jurídicos dizem respeito, em cada caso, a áreas distintas do ordenamento jurídico e exigem, além de regulamentações abrangentes, muitas vezes também respostas específicas para áreas diversas.

Ao se lidar com a IA no direito, é preciso superar reduções até agora costumeiras no modo de abordar a questão, como, por exemplo, o foco nos potenciais de vigilância. O mesmo se aplica ao direito de proteção de dados que durante muito tempo se encontrava no primeiro plano da regulação da interação digital. O seu tema era a forma de lidar com informações pessoais e, neste contexto, especialmente a proteção da privacidade[10]. Embora a proteção de dados continue sendo significativa também no emprego da IA, na medida em que nela se processam informações pessoais, também são empregados muitos outros dados, entre os quais se encontram informações das quais se retirou a referência a pessoas, bem como dados sem uma referência passada ou atual a pessoas, como, por exemplo, dados gerados por máquinas na área da Indústria 4.0[11]. Ao se lidar com a IA e as suas múltiplas possibilidades de utilização, muitas outras áreas do Direito, além do direito de proteção de dados, tornam-se relevantes, como, por exemplo, o direito das telemídias, o direito de concorrência, o direito da proteção do patrimônio intelectual e o direito da responsabilidade civil, particularmente o direito da responsabilidade por produtos. Além disso, o direito especial dos respectivos campos de aplicação se torna relevante, como, por exemplo, o direito da medicina, o direito do mercado financeiro ou o direito do tráfego rodoviário.

Technikrecht, p. 9, 2018; Bundesnetzagentur, *Digitale Transformation in den Netzsektoren*: Aktuelle Entwicklungen und regulatorische Herausforderungen, 2017, <https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2017/Digitalisierung.pdf?__blob=publicationFile&v=1>; H. Eidenmüller, The Rise of Robots and the Law of Humans, *Zeitschrift für Europäisches Privatrecht*, p. 765-777, 2017; A. Castilla; J. Elman, *Artificial Intelligence and the Law*, 2017, <http://techcrunch.com/2017/01/28/artificial-intelligence-and-the-law/>; I. Schneider, Bringing the State Back in: Big Data-based Capitalism, Disruption, and Novel Regulatory Approaches in Europe, in: Saetnan et al. (Ed.), *The Politics of Big Data*, 2018; S. C. Djeffal, Normative Leitlinien für künstliche Intelligenz in Regierung und öffentlicher Verwaltung, in: R. M. Kar; B. E. P. Thapa (Ed.), *(Un-)Berechenbar?* Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, p. 493-515, <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-57518-2>.

10 Veja, *pars pro toto*, Roßnagel (Ed.), *Handbuch Datenschutzrecht*, 2003; Roßnagel (Ed.), *Das neue Datenschutzrecht*, 2017; Simitis; Hornung; Spiecker gen. Döhmann (Ed.), *Datenschutzrecht*, 2019.

11 Veja A. Sattler, Schutz von maschinengenerierten Daten, in: T. Sassenberg; T. Faber (Ed.), *Rechtshandbuch Industrie 4.0 und Internet of Things*, 2017, p. 27-52.

Para a realização do bem-estar individual e comunitário, os efeitos associados às possibilidades de aplicação de sistemas complexos de TI nas diversas esferas da sociedade são de importância especial. Por isso, a forma de lidar com as oportunidades e os riscos ligados à IA e a seus empregos precisa ter um enfoque amplo. Ao se fazer isso, o olhar tampouco deve ser limitado aos resultados produzidos diretamente – como *output* – com tecnologia digital mediante utilização da IA. Os efeitos produzidos por meio da utilização de sistemas complexos de TI sobre os destinatários de decisões ou a terceiros atingidos (*impact* como microefeitos) são igualmente importantes. Além disso, pode ser apropriado compreender de modo geral efeitos adicionais, também em longo prazo, nas esferas da sociedade atingidas e esclarecer até que ponto eles são significativos para o direito e a regulação (*outcome* como macroefeitos).

A título de ilustração, mencione-se que uma série de serviços prestados com base na digitalização produzem efeitos não apenas para seus destinatários, mas, em muitos casos, também para terceiros, assim como para a funcionalidade de sistemas parciais da sociedade. Assim, em decorrência da digitalização e do emprego da IA, existem possibilidades consideráveis de influenciar estilos de vida, experiências, orientações culturais, focos de atenção e noções de valor dos cidadãos e das cidadãs, com possíveis efeitos na vida privada, no sistema educacional, no desenvolvimento da opinião pública e, por meio dela, também nos processos de tomada de decisões políticas[12].

Devem-se levar em conta, ainda, efeitos específicos (mais remotos) em diversas áreas parciais da sociedade. Assim, a robótica empregada em processos de produção para aumentar a eficiência e reduzir custos pode mudar enormemente o mercado de trabalho e, particularmente, as condições de trabalho. O mesmo se pode esperar do maior emprego da *legal technology* [tecnologia jurídica] no âmbito da prestação de serviços jurídicos. Os novos formatos de comercialização para os bens que podem ser adquiridos por uma plataforma como a Amazon também transformam os mercados, como, por exemplo, o do comércio varejista, e, em conexão com isso, eventualmente também a disponibilidade de lojas e prestadores de serviços na área urbana e, por conseguinte, o tipo de convivência social. A intermediação de moradias por meio da AirBnB influencia a disponibilidade de residências de aluguel permanente, mas também produz impactos sobre a indústria hoteleira. O controle algorítmico do que acontece em mercados financeiros pode acarretar desdobramentos imprevisíveis, como, por exemplo, quedas ou saltos nas cotações, etc.

Quando sistemas de TI são empregados mediante a utilização de infraestruturas altamente modernas e mais recentes tecnologias, particularmente da IA

12 Veja, *pars pro toto*, M. Latzer et al., The Economics of Algorithmic Selection of the Internet, in: J. M. Bauer; M. Latzer (Ed.), *Handbook on the Economics of the Internet*, 2016, p. 395.

altamente desenvolvida, para a *social engineering* [engenharia social] de amplo alcance ou para monitorar o ordenamento econômico e social, bem como o comportamento individual e social, isso tem uma importância especialmente ampla para todos os três níveis de efeitos (*output*, *outcome* e *impact*). O desenvolvimento atual que se verifica na China caminha nessa direção. Empresas de orientação comercial – entre elas, principalmente, mas não só, empresas de TI dominantes no mercado como a do Grupo Alibaba (que têm, entre outras, diversas plataformas comerciais e o sistema de pagamentos *on-line* Alipay, amplamente disseminado) ou a da Tencent Holding (redes sociais, agência de notícias, jogos *on-line*, entre outros) operam em estreita cooperação com instituições estatais e o Partido Comunista, e levantam dados de modo abrangente e os interconectam para fazer análises diversas. O seu objetivo é otimizar os processos de mercado, orientar o comportamento social das pessoas por determinados valores normativos (mencionam-se, por exemplo, honestidade, confiabilidade, integridade, asseio, fidelidade jurídica, responsabilidade na família, etc.) e assegurar a estabilidade do Estado e da sociedade. Na China, em seu conjunto está sendo montado um sistema abrangente (atualmente sendo testado em projetos-piloto, mas já aplicado em amplas partes do país) chamado *Social Scoring System/Social Credit System*[13]. Seria um reducionismo analisar a estruturação desse sistema – como acontece muitas vezes na Europa mediante a repressão de opiniões divergentes – primordialmente sob o aspecto da vigilância sobre as pessoas. Os seus objetivos vão muito além disso.

Mas é extremamente improvável que ele encontre imitadores na Alemanha ou na Europa ocidental, em todo caso não na dimensão da *social engineering* que se busca na China. Por isso, nessa contribuição não se visa examinar e avaliar mais de perto esse *Social Credit System*. A sua menção serve apenas para ilustrar potenciais contidos nas novas possibilidades de aplicação da TI.

Por conseguinte, este artigo se limita a expor desafios para o direito e a regulação sob as presentes condições gerais na Alemanha e na União Europeia.

3 REFERÊNCIA AO DIREITO

Os efeitos associados a tecnologias digitais, incluindo a IA, podem – por exemplo, do ponto de vista da ética, da política social ou da política econômica – ser desejáveis ou indesejáveis. Dependendo do resultado dessa avaliação, pode se tornar importante indagar se a criação e/ou utilização de IA necessita

13 Quanto a isso, veja Y. Chen; A. S. Y. Cheung, The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System, *The Journal of Comparative Law*, v. 12, p. 356-378, 2017; R. Creemers, *China's Social Credit System*: An Evolving Practice of Control, 2018, <https://ssrn.com/abstract=3175792>; X. Dai, *Toward a Reputation State*: The Social Credit System Project of China, 2018, <https://ssrn.com/abstract=3193577>.

ser tratada pelo Direito e, especialmente, ser detalhada regulatoriamente para promover interesses individuais e coletivos ou proteger contra efeitos negativos.

É claro que, em princípio, no emprego de tecnologias digitais se aplicam todas as normas vigentes nas áreas atingidas, como as do direito nacional – na Alemanha, portanto, os direitos civil, penal e público e as suas áreas secundárias –, bem como os direitos transnacional e internacional, especialmente o da União Europeia (UE). Esse direito continua sendo aplicável mesmo que para tanto não haja necessidade de uma referência expressa à digitalização. Deve-se indagar, contudo, se e até que ponto esse direito relacionado em grande parte às condições do "mundo analógico" faz jus às exigências da digitalização e, nela, especialmente à forma de lidar com a IA ou precisa ser modificado e complementado.

A isso se acrescenta a questão adicional a respeito de como o direito novo ou por criar, que se relaciona ou pode ser relacionado à digitalização, deve ser situado no conjunto do contexto do ordenamento jurídico. Como se sabe, as diferentes normas jurídicas estão sistematicamente conectadas com outras partes do ordenamento jurídico. Além disso, via de regra elas estão muitas vezes inseridas em estruturas regulatórias complexas. Esse conceito[14] encerra, além das normas disponíveis para a solução do problema, também os procedimentos formais, mas também informais aplicáveis (formas de interação) na concretização e no emprego do direito, assim como os recursos humanos acionáveis para o enfrentamento do problema junto com suas orientações específicas em cada caso. Decisivos podem ser ainda os recursos (por exemplo, tempo, dinheiro, *expertise*) e as formas de atuação disponíveis nas organizações, eventualmente também as possibilidades e medidas de cooperação ou articulação de diversos atores, tanto estatais quanto privados. Tais estruturas regulatórias podem ser particularmente complexas em sistemas de múltiplos níveis, o que é o caso, por exemplo, da UE.

4 MODALIDADES DE GOVERNANÇA

A produção do direito e, especialmente, de medidas de regulação estatal precisa estar ajustada às modalidades de enfrentamento do problema escolhidas em cada caso (as "modalidades de governança": mercado, concorrência, negociação, rede, contrato ou controle digital)[15]. Como essas modalidades e a sua estruturação concreta contribuem para alcançar objetivos desejados pela sociedade e para evitar efeitos indesejáveis? Há necessidade de critérios apropriados para esclarecer o que é desejável. Desses critérios fazem parte, especialmente,

14 Veja W. Hoffmann-Riem, *Innovation und Recht – Recht und Innovation*, 2016, p. 9-12.

15 Quanto à governança de modo geral, veja A. Benz; N. Dose (Ed.), *Governance – Regierung in komplexen Regelsystemen*, 2. ed., 2010; G. F. Schuppert, *Alles Governance oder was?*, 2011.

os valores-alvo constitucionalmente normativos (particularmente a democracia, o Estado de Direito e o Estado Social; v. art. 22 da Lei Fundamental [LF]), a proteção das liberdades de desenvolvimento econômico, cultural, político, etc., o impedimento de manipulação e discriminação e muitas outras coisas mais. Particularmente importantes são também os princípios, as metas e os valores contidos no tratado sobre a União Europeia e na Carta dos Direitos Fundamentais da UE, bem como em outros atos jurídicos da União.

Um desafio consiste na garantia de boa governança no desenvolvimento de sistemas algorítmicos – *governance of algorithms*[16] – e em sua aplicação – *governance by algorithms*[17]. Luciano Floridi[18] descreve a "governança do digital" da seguinte maneira:

> Governança digital é a prática de estabelecer e implementar políticas, procedimentos e padrões para o desenvolvimento, uso e gestão apropriados da infosfera. Trata-se também de uma questão de convenção e boa coordenação, às vezes nem moral nem imoral, nem legal nem ilegal. Por exemplo, através da governança digital um órgão governamental ou uma empresa poderá: 1) determinar e controlar processos e métodos usados por gestores de dados [*data stewards*] e guardiões de dados [*data custodians*] a fim de melhorar a qualidade, confiabilidade, acesso e segurança dos dados e a disponibilidade de seus serviços; e 2) criar procedimentos eficazes para a tomada de decisões e para a identificação de responsabilidades no que diz respeito a processos relacionados com dados.[19]

O cumprimento de exigências éticas e a garantia de *compliance* também se situam no âmbito da boa governança.

Como um exemplo entre outros de critérios importantes para a estruturação da IA citamos aqui uma lista produzida por um grupo instituído pela Comissão Europeia[20]: a) dignidade humana; b) autonomia; c) responsabilidade; d) justiça, equidade e solidariedade; f) Estado de Direito e prestação de contas; h) proteção de dados e privacidade; i) sustentabilidade. Que esse grupo tenha situado esses critérios no campo da ética em nada muda; contudo, o fato de que eles também têm, em grande parte, relevância jurídica. Nesse caso fica claro que o direito e a ética estão inter-relacionados em muitos casos. O direito também tem fundamentos éticos, e princípios éticos também são moldados pelo direito (v. infra, Seção 8).

---

16 F. Saurwein et al., Governance of Algorithms: Options and Limitations, *info*, v. 17, n. 6, p. 35-49, 2015.

17 N. Just; M. Latzer, Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet, *Media, Culture & Society*, p. 1-21, 2016; Latzer et al. (n. 10).

18 L. Floridi, Soft Ethics, the Governance of the Digital and the General Data Protection Regulation, *Philosophical Transactions of the Royal Society*, 2018, A 376, <http://dx.doi.org/10.1098/rsta.2018.0081>.

19 Floridi (n. 16), p. 4 ss.

20 European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence*, Robotics and "Autonomous" Systems, 2018, <https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf>, p. 16 ss.

Os caminhos possíveis para assegurar a boa governança são múltiplos. Nesse sentido, as medidas não precisam ter a forma de regras fixadas em textos. Também são significativas, por exemplo, as abordagens tecnológicas ou a proteção sistêmica, como o *design* tecnológico escolhido[21].

5 A ASSUNÇÃO DE RESPONSABILIDADE PELA GARANTIA POR MEIO DE MEDIDAS VISANDO À BOA GOVERNANÇA DIGITAL

A boa governança, porém, não ocorre automaticamente. Na medida em que, como nesta contribuição, o olhar está voltado primordialmente para o Direito, são importantes as diretrizes jurídicas normativas e, complementarmente, diretrizes extranormativas (por exemplo, éticas ou morais), bem como a reação dos destinatários das normas a elas, como, por exemplo, a sua disposição para cumpri-las. Uma das tarefas do Estado é produzir o direito ou modificá-lo de tal maneira que ele possibilite e estimule a boa governança digital.

5.1 Deslocamentos na estrutura de responsabilidade

Neste contexto, a transformação digital se depara com um reajuste já por ela introduzido na relação entre direito estabelecido por privados e pelo Estado, especialmente em consequência de medidas anteriores de desregulação e privatização. Pode-se perceber, em especial, um recuo do direito estabelecido pelo Estado como meio de estruturar situações da vida – e isto não obstante o maior número de regras jurídicas estatais. Particularmente duradouro é – não só, mas também – o deslocamento da responsabilidade para portadores privados nas esferas determinadas pela digitalização, especialmente nas áreas de negócios das grandes empresas de TI que operam no mundo inteiro, como, por exemplo, das chamadas *big five* [cinco grandes]: Alphabet/Google, Facebook, Amazon, Microsoft e Apple. Elas atuam, em grande parte, segundo normas elaboradas por conta própria e, na maioria das vezes, estabelecidas e implementadas unilateralmente, também na medida em que elas atingem terceiros – por exemplo, os usuários de seus serviços[22].

O forte peso da autoestruturação e autorregulação[23] privada em nada muda; entretanto, a responsabilidade de órgãos estatais pela proteção de bens individuais e coletivos. Em função dos deslocamentos, porém, mudaram as condições gerais, os instrumentos e as chances de sucesso da influência estatal. Na medida em que a transformação digital é estruturada por atores privados, o

21 Veja supra 5.4.

22 P. Nemitz, Constitutional Democracy and Technology in the Age of Artificial Intelligence, *Philosophical Transactions of the Royal Society*, 2018, A 376, <http://dx.doi.org/10.1098/rsta.2018.0089>, p. 2 ss.

23 Veja, também, infra 7.

Estado, como "Estado garantidor" (*ensuring state*)[24], tem a tarefa de assegurar o bem individual e coletivo também por intermédio do direito. Ele pode ou deve criar estruturas apropriadas, dar orientações normativas para o comportamento e, eventualmente, estatuir limites para o comportamento. Em face da mudança rápida é preciso, além disso, acompanhar o desenvolvimento de maneira contínua e, eventualmente, tomar medidas contrárias caso ocorram distorções.

Embora os atores privados sejam – também protegidos pelos direitos fundamentais – basicamente livres para perseguir seus interesses e especificar seus cálculos de lucro, não estão inteiramente dispensados de levar em consideração os interesses de outros e do bem comum. O direito pode ou precisa, caso necessário, estabelecer um marco para assegurar um exercício da liberdade socialmente compatível. Nesse sentido, se fala com frequência da responsabilidade garantidora do Estado[25]. Diretrizes normativas para o cumprimento dessas tarefas se encontram não só nas definições dos objetivos do Estado, mas também nas normatizações dos direitos de liberdade e nas regulações avulsas em áreas específicas. A concretização dessas diretrizes mediante a interpretação do direito já existente ou mediante a produção de direito e sua modificação compreende, também, a reação à mudança, nesse caso à mudança tecnológica e social associada à digitalização.

5.2 Jurisprudência normativa como exemplo

Encontra-se material ilustrativo para a utilização da tarefa garantidora não só em leis e medidas da administração, mas também na jurisprudência. Remetemos aqui a diversas inovações do Tribunal Constitucional Federal alemão referentes à TI na área dos direitos fundamentais. Já, no ano de 1983, o Tribunal desenvolveu, fazendo referência aos riscos para a proteção da personalidade associados à digitalização incipiente, um "direito fundamental à autodeterminação informacional"[26]. Em 2008, ele estendeu o alcance da proteção dos direitos fundamentais ao "direito fundamental à garantia da integridade e confidencialidade de sistemas de tecnologia da informação"[27]. Enquanto essa decisão, por causa do objeto de litígio na época, ainda dizia respeito a inter-

24 G. F. Schuppert, The Ensuring State, in: Giddens (Ed.), *The Progressive Manifesto*: New Ideas for the Centre-left, 2003, p. 54 ss.; R. Ruge, *Die Gewährleistungsverantwortung des Staates und der Regulatory State*, 2004; C. Franzius, *Gewährleistung im Recht*: Grundlagen eines europäischen Regelungsmodells öffentlicher Dienstleistungen, 2009.

25 H. Schulze-Fielitz, Grundmodi der Aufgabenwahrnehmung, in: Hoffmann-Riem et al. (Ed.), *Grundlagen des Verwaltungsrechts*, 2. ed., 2012, v. 1, p. 823 ss., p. 896 ss.

26 BVerfGE [Decisões do Tribunal Constitucional Federal], 65, 1; quanto a isso, veja, *pars pro toto*, G. Britz, *Freie Entfaltung durch Selbstdarstellung*: Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, 2007.

27 BVerfGE, 120, 274, 313; A. D. Luch, Das neue "IT_Grundrecht" – Grundbedingung einer "Online-Handlungsfreiheit", MMR, p. 75-79, 2011; J.-C. Wehage, *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das bürgerliche Recht*, 2013; M. Hauser, *Das IT-Grundrecht*: Schnittfelder und Auswirkung, 2015.

venções no computador utilizado pela própria pessoa, mais tarde – no ano de 2016 – o Tribunal resolveu que entre os sistemas de TI protegidos não contam apenas computadores utilizados pelas pessoas em questão, mas também sua conexão com outros computadores, como, por exemplo, no caso de colocação de dados na nuvem[28]. Ele acentuou, ao mesmo tempo, que dados armazenados em servidores externos na legítima expectativa de confidencialidade têm parte na proteção. Concede-se proteção, de igual maneira, quando movimentos de usuários são acompanhados na rede. Com isso, a utilização de IA, entre outras, ligada a tais conexões também pode se tornar significativa no âmbito protetivo desse direito fundamental.

O Tribunal entendeu esse direito – muitas vezes designado como direito fundamental da TI na literatura –, assim como o direito fundamental à autodeterminação informacional, como concretização da garantia jusconstitucional da dignidade humana e da proteção do livre desenvolvimento da personalidade (arts. 1º, 1, e 2º, 1, da LF). Normas como os arts. 1º e 2º da Lei Fundamental, mas também outros direitos fundamentais, possibilitam não só a proteção jurídica individual, mas compreendem, igualmente, funções protetivas do ponto de vista do direito objetivo, que produzem, indo além do teor jurídico defensivo, incumbências de estruturação e proteção para o Estado, que estão fundamentadas no direito objetivo[29]. Essas incumbências se referem especialmente à asseguração ou garantia de liberdade também nas relações mútuas de pessoas privadas. Isso é expresso pelo conceito de eficácia horizontal dos direitos fundamentais.

Conteúdos pertinentes de direitos fundamentais da perspectiva do direito objetivo são reconhecidos não só no ordenamento jurídico alemão, mas também, em grau crescente, no âmbito da Carta dos Direitos Fundamentais da UE e na Convenção Europeia dos Direitos Humanos, além de diversos tratados do direito internacional[30]. Entretanto, para poder implementar a incumbência de asseguração, há necessidade de normas jurídicas destinadas a isso. Exemplos de tal direito de asseguração são, por exemplo, o direito de proteção de dados e o direito de segurança da TI. Medidas jurídicas referentes à forma de lidar com a IA e para a garantia de responsabilidade por inovações a ela relacionada

28 BVerfGE, 141, 220, 264 s., 268 ss., 303 ss.

29 M. Dolderer, *Objektive Grundrechtsgehalte*, 2000; C. Callies, Schutzpflichten, in: D. Merten; H.-J. Papier (Ed.), *Handbuch der Grundrechte in Deutschland und Europa*, 2006: § 44, v II, p. 963-991, n. 5 ss.; U. Schliesky et al., *Schutzpflichten und Drittwirkungen im Internet*: Das Grundgesetz im digitalen Zeitalter, 2014.

30 A. Fischer-Lescano, Der Kampf um die Internetverfassung: Rechtsfragen des Schutzes globaler Kommunikationsstrukturen von Überwachungsmaßnahmen, JZ, v. 10, p. 965-974, 2014; Schliesky (n. 27); T. Marauhn, Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure, *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer*, v. 74, p. 373-400, 2015; N. Marsch, *Das europäische Datenschutzgrundrecht*: Grundlagen – Dimensionen – Verflechtungen, 2018, cap. 4.

também deveriam estar comprometidas com a concepção da responsabilidade pela asseguração.

5.3 Proteção de sistemas (*Systemschutz*)

O direito fundamental da TI mencionado antes se refere à proteção de sistemas de TI, ou seja, à proteção de sistemas. Em sua dimensão jurídico-objetiva, o direito fundamental contém a incumbência para entes estatais de proteger a funcionalidade de sistemas de TI não só contra intervenções ilegítimas do Estado, mas, também, indo além disso, contra a influência de terceiros. Disposições jusconstitucionais ou ao menos possibilidades de providências para garantir a funcionalidade de sistemas de TI também podem se seguir de outros direitos fundamentais (por exemplo, arts. 3º, 5º, 6º, 10, 13 e 14 da LF, entre outros) e, complementarmente, das definições dos objetivos do Estado: quanto mais importantes para o bem-estar individual e coletivo forem as tecnologias digitais, os modelos de negócios e as formas de ação, bem como as infraestruturas a elas adaptadas, tanto mais intensamente deve ser ativada a tarefa estatal de asseguração referente ao alcance desses objetivos. Ela se refere principalmente à garantia de uma democracia funcional, ao cumprimento de normas do Estado de Direito, à implementação da proteção fundamentada no Estado Social, à prevenção contra riscos previsíveis ou ainda não previsíveis (neste caso, por exemplo, do ulterior desenvolvimento e emprego da IA), mas também à funcionalidade de instituições importantes (por exemplo, do mercado). De particular importância é a garantia da qualidade de sistemas de TI, incluindo medidas visando à segurança das informações[31].

Na área da TI, a proteção de sistemas é, além da proteção jurídica individual, particularmente importante porque os indivíduos enquanto usuários praticamente não podem influenciar a estruturação do sistema e onde nem podem perceber mais a existência de perigos, ou seja, tampouco podem se defender individualmente. De resto, a proteção de esferas importantes da sociedade de modo algum pode ser bem-sucedida se a ativação de medidas protetivas depender exclusivamente da iniciativa e do êxito de ações individuais e, portanto, pontuais. Nesse tocante, existe uma tarefa importante do conjunto da sociedade que também precisa ser cumprida pelo conjunto da sociedade com a ajuda do direito. A proteção de sistemas é um ponto de partida importante para isso.

31 T. Wischmeyer, Informationssicherheitsrecht: IT-Sicherheitsgesetz und NIS-Richtlinie als Elemente eines Ordnungsrechts für die Informationsgesellschaft, *Die Verwaltung*, v. 50. p. 155-188, 2017; H. Leisterer, *Internetsicherheit in Europa*, 2018.

5.4 Proteção sistêmica (*Systemischer Schutz*)

A proteção de sistemas não deve ser confundida com proteção sistêmica. Esta última utiliza a respectiva tecnologia para inserir no próprio sistema tecnológico providências ou dispositivos que preservem por conta própria os interesses protetivos de terceiros[32]. Nesse caso, isso implica especialmente a proteção por meio de *design* tecnológico[33], incluindo também predefinições que facilitem a proteção[34]. Essa proteção sistêmica já vem sendo usada há mais tempo como recurso de proteção de dados. Um exemplo atual disso se encontra no art. 25 do Regulamento Geral de Proteção de Dados da União Europeia (RGPD-UE): "Proteção de dados desde a concepção e por defeito". O art. 32 do mesmo Regulamento contém normas adicionais. Entretanto, o campo de aplicação efetivo e potencial da proteção mediante o *design* da tecnologia é consideravelmente mais amplo e compreende também o emprego de IA. Além disso, discute-se até que ponto a eficácia de princípios básicos não só de caráter jurídico, mas também, complementarmente, de caráter ético mediante a configuração da tecnologia pode ser assegurada ou, ao menos, promovida[35].

5.5 Diretrizes regulatórias

O cumprimento da responsabilidade garantidora por parte de agentes estatais – particularmente legislador, governo e Administração Pública – com o apoio, na medida do possível, dos atores privados envolvidos com o desenvolvimento e a aplicação, pressupõe clarificações não só a respeito dos objetivos, mas também e principalmente de estratégias e concepções para sua implementação. Para tanto, se podem formular diretrizes com essa finalidade. Nesse sentido, retomamos e, ao mesmo tempo, ampliamos a lista de tais diretrizes proposta por Thomas Wischmeyer[36]:

- visibilização do efeito regulatório de sistemas inteligentes;
- nível de qualidade adequado para sistemas inteligentes;
- ausência de discriminação por sistemas inteligentes;

32 I. Spiecker gen. Döhmann, Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen, CR, v. 32, p. 698-704, 698ss., 2016.

33 K. Yeung, Towards an Understanding of Regulating by Design, in: R. Brownsword; K. Yeung (Ed.), *Regulating Technologies*: Legal Futures, Regulation, Frames and Technological Fixes, 2008.

34 M. Hildebrandt, Saved by Design? The Case of Legal Protection by Design, *Nanoethics*, v. 11, p. 307-311, 2017; U. Baumgarten; T. Gausling, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD, p. 308-313, 2017.

35 A. F. T. Winfield; M. Jirotka, Ethical Governance Is Essential to Building Trust in Robotics and Artificial Intelligence Systems, *Philosophical Transactions of the Royal Society*, 2018, A 376, <https://doi.org/10.1098/rsta.2018.0085>; European Group on Ethics in Science and New Technologies (n. 18).

36 T. Wischmeyer, Regulierung intelligenter Systeme, AöR, v. 143, p. 1-66, III 1-6, IV, 2018.

- proteção de dados e segurança informacional na utilização de sistemas inteligentes;
- emprego de sistemas inteligentes adequado aos problemas;
- garantia de transparência no emprego de sistemas inteligentes;
- clareza quanto à responsabilidade civil na utilização de sistemas inteligentes;
- viabilização de controle de sistemas inteligentes de forma democrática e pelo Estado de Direito;
- proteção contra o comprometimento duradouro das condições de vida de gerações futuras por parte de sistemas inteligentes;
- sensibilidade para erros e possibilidade de revisão de sistemas inteligentes.

A lista poderia ser ampliada. Aqui ela visa servir de ilustração da diversidade das dimensões das tarefas regulatórias.

5.6 Possibilidades regulatórias

Tendo em vista a multiplicidade de campos de aplicação da IA, o objetivo dessa contribuição não pode consistir em tematizar todos os instrumentos possíveis para exercer influência jurídica sobre o desenvolvimento e a utilização da IA. Aqui temos de nos contentar com exemplos avulsos, complementados por ponderações gerais.

Anteriormente (2), se formulou a tese de que, em muitos casos, não é suficiente desenvolver regras para a IA sem conexão com as condições contextuais de suas áreas de aplicação e, principalmente, de suas aplicações concretas[37]. Também são concebíveis regras que possam ser empregadas de modo abrangente. Nesse sentido, podem-se igualmente retomar tipos normativos que são empregados no direito de proteção de dados, não só na medida em que ele é aplicável à IA, porque os dados processados se referem a pessoas, mas também na medida em que pode servir de modelo para regulações destinadas à proteção de bens protegidos por lei diferentes do direito à privacidade. Um instrumento aplicável a quase todas as áreas de utilização são avaliações prospectivas de impacto (cf. art. 35 do RGPD-UE). Também se podem prever certificações por parte de órgãos publicamente credenciados ou estatais, por exemplo, para desenvolvimentos ou possibilidades de aplicação particularmente arriscados

37 Veja também U. Pagallo, Even Angels Need the Rules, ECAI, v. 285, p. 209-215, 209 ss., 2016; M. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, *Harvard Journal of Law & Technology*, v. 29, p. 354-400, 2016; A. Tutt, An FDA for Algorithms, *Administration Law Review*, v. 69, p. 83, 2017; M. Martini; D. Nink, Wenn Maschinen entscheiden, *NVwZ Extra*, v. 10, p. 1-14, 2017.

(cf. art. 42 do RGPD-UE). Na medida em que as certificações – como é usual – são voluntárias (segundo o art. 42, 3, do RGPD-UE), faz sentido estabelecer estímulos para sua execução, por exemplo, mediante isenções ou facilidades na responsabilidade civil – por exemplo, para a robótica no direito da responsabilidade pelo produto. Em áreas de risco, contudo, também se podem normatizar obrigações de certificação.

Em face da frequente imprevisibilidade de desenvolvimentos adicionais e da dinâmica das modificações de *softwares* – particularmente no caso de sistemas aprendentes –, também há necessidade de controle contínuo (monitoramento), bem como de avaliações retrospectivas de impacto, executados na forma de autocontrole e/ou controle por terceiros. Para possibilitar esse controle se oferecem, como suporte, obrigações de documentação do *software* e de suas modificações, bem como, no caso de sistemas aprendentes, dos programas de treinamento. Obrigações de marcação dos dados utilizados, bem como de elaboração de registros de aplicações e da utilização de programas de treinamento, assim como obrigações de elaborar relatórios e fornecer informações, também podem fazer sentido[38].

Medidas ou dispositivos para assegurar transparência, imputabilidade, responsabilidade e, eventualmente, revisabilidade adequadas representam uma dificuldade especial, particularmente em sistemas inteligentes de TI[39]. Quanto a esses problemas, remetemos às complexas reflexões feitas por Thomas Wischmeyer em sua contribuição sobre a regulação de sistemas inteligentes[40]. Devem-se aprofundar, particularmente, seus estímulos para a instituição de uma "arquitetura de fundamentação e controle baseada em divisão de trabalho"[41]. Deve-se providenciar também o desenvolvimento ulterior de critérios para avaliar o desenvolvimento, como, por exemplo, a adaptação de normas éticas em face de áreas de aplicação e riscos novos que surjam, especialmente com vistas aos limites da possibilidade de perceber e controlar as consequências ou os impactos.

O direito imperativo também pode ser imprescindível para, por exemplo, vedar discriminações e assegurar a preservação da cibersegurança particularmente importante para o futuro[42]. Devem-se cogitar também proibições ou limitações de aplicações. No Direito alemão, elas também já estão, em parte, normatizadas, como, por exemplo, para o caso de decisões automatizadas por

38 Quanto a essas possibilidades, veja, por exemplo, ainda que com referência especial à proteção da privacidade: Leopoldina Nationale Akademie der Wissenschaften und acatech, Union der deutschen Akademien der Wissenschaften (Ed.), *Stellungnahme: Privatheit in Zeiten der Digitalisierung*, 2018.

39 Veja, também, 6.3.

40 Wischmeyer (n. 34).

41 Wischmeyer (n. 34), p. 32 ss.

42 Quanto a ela, veja: Wischmeyer (n. 29); K. Beucher; J. Utzerath, Cybersicherheit – Nationale und internationale Regulierungsinitiativen: Folgen für die IT-Compliance und die Haftungsmaßstäbe, MMR, p. 362-367, 2013.

parte de órgãos estatais (v. §§ 3 a; 24, item I; 35a, 37, item 2, III, IV; § 41, item II, frase 2 do Código do Procedimento Administrativo [VwVfG, na sigla em alemão]; § 155, item IV do Código Geral dos Impostos; § 31a do Código de Segurança Social X). Deve-se esperar, porém, que os campos de aplicação sejam consideravelmente aumentados especialmente com a ampliação do governo eletrônico e, sobretudo, que novas experiências venham a criar ensejos para limitações da aplicação.

Em face das oportunidades e dos riscos da IA que vão muito além dos relacionados ao processamento de dados pessoais, é preciso esclarecer se faz sentido recorrer, para a tarefa de monitoramento, às autoridades até agora encarregadas da proteção de dados. Para tanto, seria preciso, em todo caso, ampliar suas competências e dotá-las, tanto qualitativa quanto quantitativamente, de recursos humanos adequados. Entretanto, seria preferível criar uma instituição especializada responsável, eventualmente em nível federal ou até para toda a UE, não só pelo monitoramento, mas também e principalmente de IA, como, por exemplo, uma agência digital. Para o âmbito jurídico americano, Andrew Tutt[43] sugeriu a criação de um órgão que deveria ter um poder semelhante à Federal Drug Administration [Administração Federal de Produtos Alimentícios e Farmacêuticos]. Essa instituição deveria ser encarregada, além do monitoramento[44], também do desenvolvimento de padrões (de desempenho, de *design*, de confiabilidade), ou ao menos participar dele.

Com as possibilidades aqui abordadas para o cumprimento da tarefa de garantia estão descritas primordialmente apenas formas de procedimentos, mas não os critérios com base nos quais se possa verificar a conformidade do emprego de IA nos respectivos campos de aplicação. Esses critérios devem estar orientados pelas normas jurídicas jusconstitucionais, mas também transnacionais, além de observar princípios éticos[45].

Temos de deixar de lado aqui as dificuldades técnicas da implementação de instrumentos jurídicos. Para enfrentá-las é imprescindível, além da *expertise* jurídica e técnica, também o conhecimento da matéria por parte da sociedade civil. Na medida em que se tornem necessários instrumentos jurídicos cuja implementação necessita de outras inovações, também se deve pensar em trabalhar, na área do direito, com o instrumento da *innovation forcing* [inovação

43 Tutt (n. 35).

44 Um primeiro passo para isso é a certificação de sistemas de IA. Para isso as respectivas informações são importantes. Assim, Scherer (n. 35), p. 397, exige o seguinte: "As empresas que busquem a certificação de um sistema de IA deveriam divulgar todas as informações técnicas referentes ao produto, incluindo (1) o código-fonte completo; (2) uma descrição de todos os ambientes de hardware/software em que a IA foi testada; (3) qual foi p desempenho da IA nos ambientes de teste; e (4) quaisquer outras informações pertinentes para a segurança da IA".

45 Quanto a isso, veja, também, supra 4; 6.7.

forçada][46]. Isso se refere à fixação normativa de metas ou padrões que ainda não podem ser atingidos segundo o estado da arte atual, mas cujo atingimento é plausível. Esse direito concede, então, um prazo de implementação. Caso ele se esgote sem que a meta seja alcançada e não seja prolongado, é preciso abrir mão do desenvolvimento e da utilização do respectivo tipo de IA.

6 OBSTÁCULOS PARA O EMPREGO EFICAZ DO DIREITO

Entretanto, para que tais medidas jurídicas sejam criadas e se assegure sua aplicação eficaz, deve-se contar com o surgimento de dificuldades que existem em função de algumas particularidades do campo de regulação. Destacamos apenas algumas delas aqui.

6.1 Abertura para novos desenvolvimentos e potenciais de risco

Em face da constante rapidez da mudança tecnológica, do desenvolvimento de novas áreas de atuação e modelos de negócios e das mudanças da sociedade a eles associadas, muitas vezes a aplicação do direito tem de ocorrer sob grande insegurança[47]. O risco de ineficácia ou de consequências disfuncionais de medidas jurídicas pode estar ligado com o desconhecimento e, frequentemente, com a imprevisibilidade. Uma regulação jurídica deve, por um lado, estar aberta para inovações adicionais para não inviabilizar as oportunidades associadas com a digitalização, mas, por outro, não deve ser tão aberta a ponto de não servir para evitar ou minimizar riscos. Além disso, o ordenamento jurídico precisa conter possibilidades de reversão para o caso de o objetivo jurídico não ser alcançado e/ou surgirem consequências imprevistas avaliadas como negativas (medidas para a reversibilidade). Nesse sentido, sistemas autoaprendentes de TI acarretam riscos especiais na medida em que, sem que se perceba, seus processos de aprendizado se encaminhem para direções que causem consequências indesejáveis ou até irreversíveis.

Provavelmente não é acaso que no presente se esteja apontando cada vez mais para os riscos do emprego da IA. A proteção regulatória está sendo exigida também por atores que, ao longo de sua história de vida, impulsionaram o desenvolvimento da IA e a utilizaram intensivamente em seus negócios, como, por exemplo, o cofundador da Paypal e proprietário da Tesla, Elon Musk, o cofundador da Microsoft, Bill Gates, e o cofundador da Apple, Steve Wozniak[48].

46 Quanto a isso, veja Hoffmann-Riem (n. 12), p. 430 ss., com mais referências.

47 Quanto à forma de lidar com o desconhecimento e a insegurança, veja, em termos fundamentais, W. Hoffmann-Riem, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data., in: Hoffmann-Riem (Ed.), *Big Data – Regulative Herausforderungen*, 2018, p. 11 ss., com mais referências na 5ª Parte.

48 Quanto a isso, veja Scherer (n. 35), p. 355. Quanto aos riscos, veja os trabalhos – provavelmente escritos de forma alarmista demais – de N. Bostrom, *Superintelligence*: Paths, Dangers, Strategies, 2014; M. Tegmark,

O genial pesquisador Stephen Hawking (que se autodesigna como cosmologista) assumiu essas preocupações e exigiu esforços para ampliar os magníficos potenciais da IA, mas dar mais atenção ao tema da segurança da IA[49]. Embora as advertências se concentrem em aspectos específicos, elas também dizem respeito ao risco. A IA poderia se subtrair ao controle humano e desenvolver potenciais destrutivos para a humanidade em geral.

Como exemplo já de riscos em áreas restritas seja mencionado aqui o emprego de "transplantes cerebrais e outros dispositivos neurais"[50]. Nesse caso, a tematização de riscos para o futuro não se dá apenas com vistas, sobretudo do ponto de vista ético, a consequências para o desenvolvimento humano e à concepção e ao funcionamento da inteligência humana. Temem-se também novas formas de cibercriminalidade, como, por exemplo, pelo hackeamento de marca-passos ou outros implantes comandados por IA. Nas palavras de Gasson e Koops, por exemplo:

> As consequências de ataques contra implantes humanos podem ser bem maiores para a vida e saúde humana do que no caso do cibercrime clássico. Além disso, à medida que a tecnologia dos implantes continua se desenvolvendo, torna-se difícil traçar um limite exato entre o corpo e a tecnologia, e os ataques afetam não apenas a confidencialidade, integridade e disponibilidade dos computadores e dados de computação, mas também a integridade do próprio corpo humano. A combinação de tecnologias de rede com corpos humanos pode muito bem constituir um novo salto qualitativo na evolução do cibercrime, transformando o ataque contra humanos através de implantes em uma nova geração do cibercrime.[51]

6.2 Diluição de limites

Dificuldades para a abordagem jurídica de sistemas complexos de TI também decorrem do fato de que as tecnologias acarretam, em muitos sentidos, uma diluição de limites ou exigem uma atuação em áreas sem limites[52]. Assim, as tecnologias digitais utilizadas, suas infraestruturas e os modelos de negócios empregados não têm limites regionais – por exemplo, nacionais – ou só os têm

Lie 3.0: Being a Human in the Age of Artificial Intelligence, 2017. Veja também R. D. Precht, (n. 1). É elucidativo que Brad Smith, presidente e *Chief Legal Officer* da Microsoft, tenha proposto a criação de uma "Digital Geneva Convention", que se refere primordialmente a ciberataques e, com isso, a cibersegurança, mas também tem de se ocupar necessariamente com o tema da IA; veja <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>.

49 S. Hawking, *Kurze Antworten auf große Fragen*, 2018, p. 209 ss., 213 ss.

50 Veja, por exemplo, S. S.Wu; M. Goodman, Neural Implants and their Legal Implications, *GPSolo Magazine*, v. 30, p. 68-69, 2013.

51 M. N. Gasson; B.-J. Koops, Attacking Human Implants: A New Generation of Cybercrime, *LIT*, v. 5, p. 248, 276, 2013.

52 M. Cornils, Entterritorialisierung im Kommunikationsrecht, *Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer*, v. 76, p. 391-437, p. 391 ss., 2017; T. Vesting, Digitale Entgrenzung, in: Lomfeld (Ed.), *Die Fälle der Gesellschaft:* Eine neue Praxis soziologischer Jurisprudenz, 2017, p. 81 ss.; Hoffmann-Riem (n. 45), p. 36 s.

em casos excepcionais. Com frequência, eles estão disponíveis em nível transnacional e especialmente global. O mesmo se aplica aos serviços prestados com a tecnologia digital e a seus efeitos. Em consonância com isso, o emprego de IA também não se dá em espaços limitados. Principalmente as grandes empresas de TI que operam em nível global estão interessadas em trabalhar em estruturas tão uniformes quanto possível, moldadas global ou transnacionalmente. Para elas, regulamentações consagradas em diversos ordenamentos jurídicos nacionais e, por conseguinte, diferenciadas representam um obstáculo para a utilização de seus modelos de negócios. Em consequência disso, essas empresas buscam e aproveitam possibilidades de evitar ou se esquivar de tais regulamentações[53].

Contudo, em princípio não se exclui a possibilidade de vincular normativamente empresas que atuam em nível transnacional a regulamentações jurídicas com âmbito de vigência limitado na medida em que elas operem nesse âmbito. Um exemplo mais recente disso é o art. 3º do RGPD-EU. Segundo ele, o Regulamento é aplicável ao processamento de dados pessoais "efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União"[54]. Regras complementares se encontram no § 1º da Lei Federal de Proteção de Dados (nova).

A diluição de limites também diz respeito à dimensão dos objetos. Assim, no âmbito da TI os limites entre *hardware* e *software* se diluem, ou determinados problemas podem ser resolvidos tanto na área do *hardware* quanto do *software*. De maneira semelhante, a comunicação privada e a pública se confundem cada vez mais (remetemos, *pars pro toto*, a Jünger, 2018). A comunicação *off-line* e *on-line* está cada vez mais entremeada – por exempli, na Internet das coisas –, de modo que uma nova espécie de mundo, que algumas pessoas chamam de mundo "*onlife*", torna-se determinante[55].

Como uma dissolução de limites significativa para a regulação jurídica também pode ser contabilizado o fato de que a digitalização compreender quase todas as esferas da vida e, por isso, normas para o emprego de IA podem ou até devem se dar tanto em termos abrangentes quanto específicos para cada esfera.

Na medida em que são utilizados sistemas algorítmicos autoaprendentes que continuam desenvolvendo seu *software* por conta própria, dedicam-se a

53 Nemitz (n. 20).

54 Versão em português extraída de <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT>.

55 L. Floridi (Ed.), *The Onlife Manifesto*: Being Human in a Hyperconnected World, 2014, <https://link.springer.com/book/10.1007%2F978-3-319-04093-6>; M. Hildebrandt, *Smart Technologies and The End(s) of Law*: Novel Entanglements of Law and Technology, 2015, p. 41 ss., 77 ss.

novos problemas e desenvolvem soluções para esses problemas, eles ultrapassam os limites do campo de aplicação ou as possibilidades de resolução de problemas fixados pela programação inicial. Ao mesmo tempo, os limites da perceptibilidade, verificabilidade e revisabilidade de sua capacidade de desempenho podem ser ampliados ou até ultrapassados[56].

6.3 Formas de intransparência (*Intransparenzen*)

Por um lado, a transformação digital criou novos espaços para a geração, a captação e o aproveitamento de informações que até agora eram praticamente inacessíveis. Ao mesmo tempo, porém, vedam-se acessos aos procedimentos utilizados e aos resultados mediante a estruturação tecnológica ou outras formas de manutenção de segredo[57]. Formas de intransparência também podem resultar do processo de desenvolvimento de diversas partes de programas e da criação de *hardware*, cuja organização esteja baseada em divisão de trabalho. Isso se aplica especialmente na medida em que não existam conhecimentos suficientes sobre os "componentes" provenientes de outros atores participantes do processo e sobre a funcionalidade deles. Na medida em que sejam empregados algoritmos aprendentes, nem mesmo os atores participantes da programação conhecem os programas modificados por aprendizado automático. Também na medida em que é possível superar o caráter de "caixa preta" de sistemas de TI[58], por exemplo, por meio de engenharia reversa, isto pressupõe, via de regra, um grande conhecimento de causa e o emprego de processos dispendiosos. Os obstáculos são grandes.

Exemplos de obstáculos para a transparência jurídica são os casos em que algoritmos são reconhecidos como segredos comerciais[59] ou segredos oficiais (um exemplo: § 32a, item 2, frase 2, do Código Geral dos Impostos).

É importante, não só para os usuários, mas também para os órgãos de fiscalização, bem como para o público em geral como corresponsável pela democracia, que a forma de lidar com tecnologias digitais, incluindo a utilização de IA, seja fundamentalmente compreensível, em todo caso passível de fundamentação e tão controlável quanto possível. Nesse sentido, uma transparência suficiente é um pressuposto não só para a criação de confiança, mas também de prestação de contas e, eventualmente, para a responsabilidade civil[60].

56 Veja, sobre isso, 6.3, na sequência.

57 Veja, *pars pro toto*, J. Kroll, The Fallacy of Inscrutability, *Philosophical Transactions of the Royal Society*, 2018, A 376, <http://dx.doi.org/10.1098/rsta.2018.0084>; Wischmeyer (n. 34).

58 Quanto a isso, veja Leopoldina et al. (n. 36), p. 50.

59 Segundo Bundesgerichtshof in Zivilsachen (BGHZ) [Supremo Tribunal Federal em Matéria Civil], 200, 38 para a classificação por parte da Schufa [Companhia de Análise de Crédito].

60 Mais detalhes em Wischmeyer (n. 34).

6.4 Concentração de poder

A utilização do direito e seu êxito são, além disso, consideravelmente dificultados pela forte concentração de poder[61] que se verifica na área de TI. Mencionamos isso aqui apenas como palavra-chave, sem explanações mais detalhadas. O desenvolvimento da IA também é dominado em grau crescente pelas grandes empresas de TI e empresas especializadas a elas associadas. Empresas de TI poderosas em termos de mercado obtiveram êxito no esforço de manter o desenvolvimento de *software* – também o que emprega IA – e a disponibilização e comercialização de serviços de TI tão livres de regulação estatal quanto possível. Nesse caso, o direito de proteção de dados (cf. *supra*, Seção 2) só consegue dar uma proteção limitada. A legislação antitruste costumeiramente empregada para limitar o poder econômico também é aplicável a empresas com negócios na área de TI e também já foi aplicada[62], mas a legislação antitruste nacional e a da UE são limitadas tanto em termos de sua vigência espacial quanto do alcance de seu conteúdo. Não existe uma legislação antitruste global referente à área de TI.

De resto, a legislação antitruste é um direito que visa assegurar a funcionalidade dos mercados, sobretudo em termos econômicos e, por isso, restritos. Interesses mais abrangentes relativos ao bem individual e comum, como, por exemplo, proteção da personalidade, liberdade frente à manipulação, justiça informacional e justiça no tocante às oportunidades de acesso ou ao impedimento de discriminação, podem ser ameaçados por assimetrias e abuso de poder. A sua proteção abrangente, porém, não faz parte do espectro de tarefas da legislação antitruste usual e não é automaticamente assegurada ou suficientemente assegurável por meio de medidas previstas nessa legislação. Nesse sentido, há eventualmente necessidade de uma legislação regulatória adicional e de sua harmonização com o direito regulatório tradicional[63].

6.5 Fuga da vinculação jurídica

Mesmo na medida em que o direito nacional ou transnacional seja aplicável na área de TI, as empresas atuantes em nível transnacional ou até global se esforçam muitas vezes – como já se mencionou antes (6.2) – para subtrair-se

61 J. J. Welfens et al., *Internetwirtschaft 2010*: Perspektiven und Auswirkungen, 2010; Rolf (n. 1); Nemitz (n. 20), p. 2 ss. Especificamente sobre o chamado capitalismo de plataformas, veja N. Srnicek, *Platform Capitalism*, 2016; A. McAfee; E. Brynsjolfsson, 2017.

62 Assim, a Comissão Europeia moveu processos com base na legislação antitruste contra empresas fortes no mercado, como a Google, e impôs sanções por sua violação. Como exemplo, vejas as referências a processos, particularmente contra a Google, em Schneider (n. 7), p. 156-159; T. Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, *Zeitschrift für Urheber- und Medienrecht*, p. 93-101, 2017.

63 Quanto a isso, veja Hoffmann-Riem (n. 45), p. 72 ss.

a essas vinculações[64]. Na medida em que o direito é eludido, não é cumprido ou sua implementação – bem como sua execução por parte das instâncias estatais responsáveis por ela – não ocorre, ele perde sua eficácia.

É possível eludir a forte vinculação jurídica por meio de uma escolha deliberada da sede ou da transferência de atividades para outras partes da corporação se, subsequentemente, as vinculações jurídicas a serem observadas perdem força ou se as normas jurídicas no respectivo Estado não são implementadas e violações não sofrem sanções. As empresas também podem utilizar seus termos e suas condições gerais para aproveitar margens de manobra jurídicas ainda restantes para isenções de um direito rigoroso[65].

7 TIPOS DE REGULAÇÃO E REGULAMENTAÇÃO

Essas (e outras) dificuldades não significam que a área de TI seja um espaço livre de regras. Além das regulamentações estatais específicas para essa área – ainda que só limitadas –, aplica-se, também nesse caso, como mencionamos, o ordenamento jurídico em seu conjunto. Há, ainda, formas de regulação e regulamentação privada, entre as quais formas que os órgãos estatais podem influenciar regulatoriamente no cumprimento de sua responsabilidade de garantia. Para ilustrar a multiplicidade de estruturações possíveis, no que se segue serão descritos tipos de regulação e regulamentação que também são empregados na área de TI. Esses tipos não foram desenvolvidos com vistas às oportunidades e aos riscos particulares da IA, mas é possível verificar até que ponto podem ser relacionados com problemas específicos da IA ou podem ser modificados de modo a dar conta das necessidades de regulação ligadas à criação e utilização da IA (asseguração de oportunidades, prevenção de riscos e medidas para minimizar desvantagens).

7.1 Autoconformação

O comportamento próprio e autônomo, não vinculado por regras, visando ao alcance de objetivos estabelecidos por ponta própria, não se situa, entretanto, na esfera da regulação e regulamentação. Por meio da autoconformação podem ocorrer, por exemplo, o desenvolvimento e a utilização de algoritmos digitais e, neste contexto, também a utilização de IA por parte de diversas empresas. O mesmo se aplica a decisões referentes à aquisição de *software* produzido por terceiros. De igual maneira, os modelos de negócios desenvolvidos e, muitas vezes, implementados mediante utilização de IA por empresas de TI

64 Nemitz (n. 20), p. 4 ss.

65 Um exemplo disso são as condições de uso da Google vigentes desde o início de 2019, que declaram como aplicável exclusivamente o Direito irlandês – que, como se sabe, é débil –, na medida em que o RGPD-UE e as diretrizes referentes à proteção de dados deixam margens de manobra para a escolha do direito.

e, neste contexto, também em grande parte a estruturação do relacionamento com os usuários de serviços estão sujeitos à autoconformação. Na esteira da autoconformação também se podem criar, para a área da própria empresa, medidas para auditoria, monitoramento e outros recursos de controle prévio e concomitante, bem como de *compliance*. A criação de diretrizes para o próprio comportamento por parte de empresas também representa uma medida de autoconformação. Nesse sentido, remete-se aqui, a título de exemplo, a diretrizes da empresa Deutsche Telekom[66] sobre o emprego de IA e a *AI at Google: Our Principles*, da Google[67].

7.2 Autorregulamentação social (*Gesellschaftliche Selbstregelung*)

O cumprimento voluntário de normas não vinculantes, mas formuladas ou ao menos reconhecidas coletivamente sobre o comportamento de empresas na área de TI com a inclusão do emprego de IA, também se situa no âmbito da ação autônoma. Essas formas – e nesse sentido falo de autorregulamentação social – já existem há tempo também na esfera da digitalização. Delas fazem parte regras informais da decência (como a netiqueta na época inicial da Internet), bem como regras para o desenvolvimento colaborativo de *software* (por exemplo, de Open Source ou Open Content). Devem-se mencionar ainda códigos de conduta não vinculantes ou outras regras de comportamento em forma de normas de conduta fundamentadas em termos morais ou éticos. Além disso, são relevantes padrões técnicos desenvolvidos por empresas individualmente quando também são acessíveis a outras e usadas por elas, sem que, com isso, os padrões já se tornem juridicamente vinculantes para terceiros.

Apesar de seu caráter juridicamente não vinculante, as regras estabelecidas pela própria sociedade podem ser socialmente sancionáveis (perda da reputação, exclusão da comunidade de usuários e semelhantes).

7.3 Autorregulação social (*Gesellschaftliche Selbstregulierung*)

Utilizo o conceito de regulação na medida em que regras visem a um objetivo de ordenamento que vá além de casos avulsos e sejam juridicamente vinculantes. Na medida em que sejam criadas no espaço da sociedade sem participação estatal, falo de autorregulação social. Trata-se, nesse caso, de regras de comportamento consentidas por grupos de profissionais ou empresas, particularmente daquelas desenvolvidas por associações cujos membros estão comprometidos com sua observância por força do estatuto da entidade. Nessa categoria também podem ser classificados padrões técnicos, inclusive os que

66 Deutsche Telekom, *Die neun Leitlinien der Telekom zum Einsatz von künstlicher Intelligenz*, 2018, <https://www.telekom.com/de/konzern/digitale-verantwortung/details/ki-leitlinien-der-telekom-523904>.

67 Google, *AI at Google*: Our Principles, 2018, <https://blog.google/technology/ai/ai-principles/>.

tenham sido desenvolvidos por uma só empresa, mas tenham se imposto no mercado de tal maneira que praticamente se tornaram vinculantes, como, por exemplo, por adquirirem caráter determinante no caso de decisões sobre questões de responsabilidade civil (por exemplo, padrões como expressão do estado da arte na ciência e tecnologia).

7.4 Autorregulação social regulada pelo Estado (*Hoheitlich regulierte gesellschaftliche Selbstregulierung*)

O conceito de autorregulação regulada[68] visa descrever situações em que órgãos ou autoridades estatais confiam, para a solução de problemas, nas medidas de ordenamento produzidas com (relativa) autonomia pelos membros da sociedade, mas exercem influência ou através de estímulos juridicamente regulados ou de forma regulatória (por meio de normas vinculantes do direito material ou processual) para que sejam levados em conta determinados objetivos, especialmente o cumprimento de finalidades referentes ao bem comum. A influência estatal pode ser exercida de maneiras extremamente diversificadas, não só em forma de estímulos comportamentais (por exemplo, em forma de diretrizes de contratação), mas também do estabelecimento de estruturas ou instituições para a cooperação entre atores privados e estatais. Deve-se mencionar também a abertura de um corredor de ação para escolher entre diversas opções, mas cujos limites estão fixados juridicamente.

Candidatos para a autorregulação regulada pelo Estado são normas jurídicas para a certificação e auditoria por parte de agências privadas credenciadas[69]. Esses instrumentos, há muito tempo testados não só no direito da proteção de dados, também podem ser relacionados com sistemas inteligentes de TI. Neste contexto, essas formas de atuação não precisam ser, forçosamente, estruturadas de modo vinculante do ponto de vista jurídico, ou seja, como direito imperativo. Existe, pelo contrário, também a possibilidade da criação, por parte do Estado, de estímulos para sua utilização, como, por exemplo, por meio da perspectiva de concessão de facilidades quanto à responsabilidade civil em caso de cumprimento das normas[70].

O Regulamento Geral da Proteção de Dados da UE, por exemplo, confia nas possibilidades de regulação estatal da autorregulação. Assim, ele incentiva que associações e outros grêmios elaborem regras de comportamento que facili-

68 M. Eifert, Regulierte Selbstregulierung und die lernende Verwaltung, *Die Verwaltung*, suplemento 4, p. 137 ss., 2001.

69 Quanto a essas formas de atuação e monitoramento de modo geral, veja P. M. Huber, Überwachung, in: W. Hoffmann-Riem; E. Schmidt-Assmann; A. Vosskuhle (Ed.), *Grundlagen des Verwaltungsrechts*, 2. ed., 2013, v. III, n. 167 ss., n. 172 s., 181 ss., 191 ss.

70 Veja supra 5.6.

tem uma aplicação correta e eficaz do regulamento[71]. O emprego de IA também pode se enquadrar nisso, na medida em que o RGPD-UE se aplique a ela. O art. 40, item 2, do Regulamento menciona muitas áreas temáticas para as quais podem ocorrer especificações mais precisas. Os estímulos para a especificação são concebidos como orientações regulatórias para as regras de comportamento, que, entretanto, as associações ou os grêmios não têm a obrigação de emitir. Elas tampouco são obrigadas a fazer uso da oferta prevista no art. 40, item 5, de apresentar a minuta ao órgão de controle com a possibilidade de obter uma aprovação. Para as regras de comportamento vigentes em vários Estados-membros, a Comissão Europeia pode, inclusive, resolver, mediante um ato de execução, que elas tenham validade geral na UE (art. 40, item 9). O art. 41 do RGPD-UE prevê possibilidades de credenciamento de órgãos apropriados para o monitoramento do cumprimento das regras de conduta. Buscam-se também processos de certificação específicos para a proteção de dados, bem como selos e marcas de conformidade que atestem a proteção de dados (art. 42 do RGPD-UE). Medidas pertinentes também podem ser juridicamente desenvolvidas para o emprego da IA fora do âmbito de vigência do RGPD-UE.

Também se pode enquadrar na categoria de autorregulação regulada pelo Estado a possibilidade de, no âmbito das empresas privadas, serem impostos determinados padrões (técnicos, por exemplo) que sejam tratados, em normas jurídicas estatais, como determinantes para a avaliação de um procedimento jurídico – por exemplo, em questões de responsabilidade civil na esfera da robótica ou dos veículos automotores fabricados para serem dirigidos de modo autônomo ou automatizado. Por meio dessa transferência eles são, ao mesmo tempo, transformados em área da normatividade jurídica. Outro exemplo são os padrões de segurança da TI formulados por um grupo de trabalho da Bitkom[72]. Eles só contêm recomendações, mas também podem ter consequências jurídicas, por exemplo, para a avaliação de negligência na produção de bens.

Também a jurisprudência pode contribuir para a regulação da autorregulação social. Um exemplo disso – mas não referente à IA – é a decisão do Tribunal de Justiça da União Europeia sobre a Google Spain[73]. Esse Tribunal determinou à Google Inc. que tomasse providências para proteger o chamado direito ao esquecimento na operação de sua máquina de busca. Mediante aplicação da Diretiva de Proteção de Dados 95/46 (agora não mais em vigor) da UE, a empresa Google foi obrigada a, sob determinados pressupostos (agora ampliados no art. 17 do RGPD-UE), remover o *link* para uma informação – a que

71 Considerandos do RGPD-UE, nº 77, 98.

72 Quanto a isso, veja BITKOM/DIN (Ed.), *Kompass der IT-Sicherheitsstandards – Auszüge zum Thema Elektronische Identitäten*, 2014, <https://www.bitkom.org/sites/default/files/file/import/140311-Kompass-der-IT-Sicherheitsstandards.pdf>.

73 Acórdão de13.05.2014 – C-131/12, *Zeitschrift für Datenschutz*, p. 350 ss., 2014.

terceiros afetados objetaram – nas opções que sua máquina de busca oferece na Europa (a informação, entretanto, não é apagada como tal). O poder de decisão sobre a remoção é exclusivamente da Google[74]. A empresa criou um conselho consultivo formado por especialistas de países europeus, que desenvolveu recomendações para a prática de remoção autorregulatória[75].

7.5 Regulação híbrida (*Hybride Regulierung*)

Falo de regulação híbrida nos casos em que uma regulação surge pela autorregulação da sociedade, mas órgãos estatais participam do desenvolvimento das regras e/ou da definição de sua relevância. Isto também se aplica a vários dos exemplos tratados no item 7.4.

Outro exemplo se encontra no direito da segurança da TI. Os catálogos de proteção básica de TI[76] elaborados e atualizados mais ou menos semestralmente pelo Departamento Federal de Segurança na Tecnologia da Informação não são juridicamente vinculantes, mas podem ser utilizados como base para uma certificação. Por meio desta se indica que a empresa tomou medidas apropriadas – por exemplo, garantias na utilização de IA – para proteger seus sistemas de TI contra ameaças à sua segurança.

A legislação sobre segurança da TI visa particularmente à prevenção e defesa contra perigos do cibercrime e da cibersabotagem. Esses crimes são praticados, em muitos casos, mediante utilização de IA. Mas a IA também pode ser empregada para se defender deles. Em especial no tocante às chamadas infraestruturas críticas, as empresas envolvidas são obrigadas a tomar medidas tecnológicas e organizacionais apropriadas, a fim de evitar transtornos na disponibilidade, integridade, autenticidade e confidencialidade de seus sistemas de TI (§ 8a, item 1, da Lei sobre o Departamento Federal de Segurança na Tecnologia da Informação). As empresas e suas entidades de classe podem elaborar sugestões para padrões de segurança (§ 8a, item 2). O Departamento examina a pertinência desses padrões para cumprir as exigências de segurança e constata sua pertinência caso o exame seja bem-sucedido. Também há a possibilidade de auditorias de segurança e certificações (§ 8a, item 3).

74 Este é um claro ponto fraco da decisão do Tribunal de Justiça europeu: a decisão – de fato até certo ponto ampla – sobre o impedimento do acesso a uma informação proveniente de um terceiro é colocada na mão de uma empresa oligopolista que opera comercialmente.

75 Google, *The Advisory Council to Google on the Right to be Forgotten*, 2015, <https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1>.

76 Quanto a eles, veja, por exemplo, F. Stetter; S. Heukrodt-Bauer, IT-Grundschutzkataloge des BSI – Last oder Mehrwert?, *Wirtschaftsinformatik & Management*, 9, n. 4, p. 62-66, 2017.

7.6 Regulação estatal

Nesse conceito se enquadram normas estatais que sejam diretamente vinculantes para os destinatários, ou seja, não necessitem de intermediação ulterior por meio de atos autorregulatórios. Exemplos disso são as normas contidas no RGPD-UE sobre as exigências concernentes à legalidade do processamento de dados, sobre obrigações de prestar informações, sobre obrigações de correção e remoção ou, também, sobre proibições de discriminação ou proibições de utilização de dados. A regulação estatal também produz normas vinculantes, como a obrigação de avaliações de impacto nos casos de processamento arriscado de dados (art. 35s. do RGPD-UE).

Em especial, o direito imperativo, que estabelece limites, situa-se na categoria de regulação estatal, como, por exemplo, na esfera das regulações da segurança da TI ou do combate a discriminações – que também podem acarretar a utilização de IA[77]. O direito imperativo é imprescindível no âmbito da prevenção e defesa contra perigos, por exemplo, como norma para a construção e o *software* de veículos automotores automatizados.

As possibilidades de uso do direito imperativo para restringir os riscos associados ao emprego de IA de modo algum estão esgotadas até agora. Também não se deve deixar de mencionar, porém, que o direito imperativo pode ter um efeito contraproducente em áreas inovadoras, especialmente que demandam a disposição dos atores para a criatividade e cooperação, se, com isso, margens de manobra são obstruídas desnecessariamente, como, por exemplo, para o desenvolvimento de IA inovadora desejável para a sociedade. Por outro lado, a asseguração de abertura para a inovação não pode ser o único objetivo da prevenção jurídica. Também há necessidade de garantir a responsabilidade pela inovação[78].

7.7 Tecnorregulação (*Technoregulierung*)

Para a implementação de diretrizes normativas se dispõe das formas de ação contidas nas áreas do direito que sejam afetadas em cada caso, mas também de formas de ação de caráter informal. Isso será apenas mencionado aqui. Acrescente-se que em tempos de digitalização também se podem empregar algoritmos digitais como tomadores de decisões. Já se fez referência a isso ao falar de "governança por algoritmos"[79]. O termo *legal technology* diz respeito ao emprego da digitalização no estabelecimento e aplicação do direito e à substi-

77 Veja, *pars pro toto*, A. Bozdag, Bias in Algorithmic Filtering and Personalization, *Ethics and Information Technology*, v. 15, p. 209-227, 2013.

78 Quanto a esses dois polos, veja Hoffmann-Riem (n. 12), p. 28-35.

79 Veja supra 4.

tuição de decisões humanas por algoritmos, incluindo a utilização de IA[80]. As possibilidades – tanto oportunidades quanto riscos – a isso associadas só podem ser mencionadas aqui, sem que seja possível aprofundar o assunto.

8 SUBSTITUIÇÃO OU COMPLEMENTAÇÃO DE MEDIDAS JURÍDICAS POR PADRÕES EXTRAJURÍDICOS, PARTICULARMENTE ÉTICOS

Já se fez referência ao entrelaçamento de normas éticas e jurídicas em termos genéricos, mas também em conexão com a digitalização e o emprego da IA[81]. Entre os desafios para a estruturação do desenvolvimento e emprego de IA está o esclarecimento da questão de até que ponto medidas protetivas devem ser moldadas por critérios éticos e acompanhadas do direito e, em especial, de regulação, mas também até que ponto é suficiente confiar unicamente na ética.

Em tempos recentes, muitas instituições têm se ocupado com questões da ética da digitalização, também com vistas à IA[82], e várias ainda estão trabalhando nisso. O governo federal alemão definiu pontos de referência para uma estratégia de inteligência artificial[83]. Também instituiu uma Comissão de Ética de Dados e especificou algumas questões pelas quais ela deveria se guiar[84]. A Câmara de Deputados alemã instituiu uma comissão de inquérito sobre inteligência artificial que também deverá tratar de questões éticas[85]. Deve-se mencionar, além disso, que algumas empresas elaboraram diretrizes ou princípios de ética para problemas parciais, como, por exemplo, conforme já se mencionou antes, a Google e a Deutsche Telekom. Também em meio à opinião pública, assim como na comunidade científica[86], estão em andamento discussões intensivas sobre o papel da ética e sua relação com regras jurídicas[87].

---

80 Quanto a ela, veja, *pars pro toto*, G. Buchholtz, Legal Tech: Chancen und Risiken der digitalen Rechtsanwendung, *JuS*, p. 955-960, 2017; V. Boehme-Neßler, Die Macht der Algorithmen und die Ohnmacht des Rechts: Wie die Digitalisierung das Recht relativiert, *NJW*, p. 3031-3017, 2017; Hartung et al. (Ed.), *Legal Tech*: Die Digitalisierung des Rechtsmarkts, 2018; Breidenbach; Glatz (Ed.), *Rechtshandbuch Legal Tech*, 2018.

81 Veja supra 4.

82 Nemitz (n. 20), p. 7, com mais referências nas n. 18 e 19.

83 Bundesregierung, *Eckpunkte der Bundesregierung für eine Strategie künstlicher Intelligenz*, 2018, <https://www.bmbf.de/files/180718%20Eckpunkte_KI-Strategie%20final%20Layout.pdf>.

84 Bundesministerium des Innern, für Bau und Heimat; Bundesministerium der Justiz und für Verbraucherschutz, *Leitfragen der Bundesregierung an die Datenethikkommission vom* 5. Juni 2018, <https://www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Leitfragen.pdf;jsessionid=6CA29F251088B5AA5ABF4C31528A0239.1_cid324?__blob=publicationFile&v=1>.

85 Enquête-Kommission, *Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale*, 2018, <https://www.bundestag.de/blob/574748/7c0ecbc8a847bb8019f2045401c1d919/kuenstliche_intelligenz_1-data.pdf>.

86 K. W. Himma; H. T. Tavani (Ed.), *The Handbook of Information and Computer Ethics*, 2008; Van den Hoven et al. (Ed.), *Handbook of Ethics, Values, and Technological Design*, 2015; M. Rath et al., *Maschinenethik*: Normative Grenzen autonomer Systeme, 2018.

87 Veja, *pars pro toto*, Winfiel; Jirotka (n. 33); C. Cath, Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges, *Philosophical Transactions of the Royal Society*, 2018, A 376, <http://dx.doi.org/10.1098/rsta.2018.0080>; P. Ott; E. Gräf (Ed.), *3TH1CS:* Die Ethik der digitalen Zeit, 2018; S. Leonelli, Locating Ethics in Data Science: Responsibility and Accountability in Global and Distributed

Em tais discussões existe, em face das dificuldades fundamentais de regulação jurídica e da implementação na área da IA – além das dificuldades particulares de chegar a um entendimento quanto a um marco jurídico transnacional –, o risco de que, em última análise se permaneça – quando muito –, em grande parte, em princípios éticos não vinculantes e, muitas vezes, formulados de modo apenas vago. Em todo caso, deve-se esperar que a maioria das empresas de TI, particularmente as que dominam o mercado, prefiram princípios éticos a uma vinculação jurídica e tentem evitar, na medida do possível, uma juridicização e sanções e, com isso, conservar margens de manobra para assegurar seus próprios interesses[88].

Confiar unicamente em princípios éticos não deve corresponder à responsabilidade estatal de proporcionar garantias. Em face dos riscos associados à digitalização de modo geral e à utilização da IA em particular, o direito estabelecido pelo Estado ou, em todo caso, pelo qual ele é corresponsável e que esteja dotado de possibilidades de sanção deve ser imprescindível. O direito concernente a isso deveria, porém, ser estruturado de tal maneira que reforce, tanto quanto possível, a efetividade de critérios éticos. O reconhecimento verbal de princípios éticos não deveria ser usado para se abrir mão da vinculatividade.

9 A NECESSIDADE DE DIREITO TRANSNACIONAL

Em decorrência da diluição de fronteiras territoriais[89] típica do emprego de IA, esforços nacionais, incluindo regras jurídicas nacionais, muitas vezes são insuficientes para enfrentar os problemas. Por isso, deve-se buscar também instrumentos transnacionais e globalmente atuantes que, na medida do possível – em todo caso, na medida em que adquirem forma jurídica –, sejam apoiados em acordos transnacionais e internacionais pertinentes. Nesse sentido, são necessárias novas propostas, convenções e instituições de uma governança transnacional[90] voltadas para a cooperação de atores estatais com as respectivas partes interessadas, como, por exemplo, com as entidades representativas e empresas da economia digital, mas também com organizações não governamentais (ONGs) e outros representantes de interesses da sociedade civil[91]. Efeitos duradouros de acordos transnacionais dependem do direito estabelecido pelo Estado ou, em todo caso, pelo qual ele seja corresponsável e que esteja acoplado a instrumentos de execução.

Knowledge Production Systems, *Philosophical Transactions of the Royal Society*, 2016, A 374, <http://dx.doi.org/10.1098/rsta.2016.0122>.

88 Nemitz (n. 20), p. 3 ss.

89 Veja supra 6.2.

90 Um exemplo disso é a NETmundial-Multistakeholder-Statement de 24 de abril de 2014, que descreve um conjunto de regras para "Internet Governance Principles" e contém um "Roadmap for the Future Evolution of the Internet Governance Ecosystem"; disponível em <https://www.alainet.org/images/NETmundial-Multistakeholder-Document.pdf>.

91 Cf. Hoffmann-Riem (n. 12), p. 691-693, com mais referências.