doi: 10.21783/rei.v6i2.484

SUBMETIDO: 24 ABR. 2020
ACEITO: 24 ABR. 2020

BIG DATA E INTELIGÊNCIA ARTIFICIAL: DESAFIOS PARA O DIREITO[1]

BIG DATA UND KÜNSTLICHE INTELLIGENZ – HERAUSFORDERUNGEN AUCH FÜR DAS RECHT

WOLFGANG HOFFMANN-RIEM [2]

ABSTRACT: The article addresses the potential legal responses to the challenges posed by the digital transformation of society, using the example of national German law and EU law. The focus is on the development and use of big data, i.e. large volumes of data that vary in terms of their nature of quality and that can be processed at high speed using big data analytics for a variety of purposes. Law is tasked with facilitating the opportunities associated with big data, but also with warding off or minimising the risks to legally protected individual and collective interests. Of special importance is the protection of rights of freedom, including the right to informational self-determination (data protection). Law also requires innovations. In addition to legal structures, protection through technology is important (such as protection by design/by default). Also necessary are assurances of sufficient transparency and control, as well as judicial protection. In addition, it must be ensured that suitable governance structures are developed. This includes assuring that generally applicable law works in concert with law that specifically targets the handling of digitalisation.

Keywords: Big data; digital transformation, data protection.

[1] Tradução dos Professores Doutores, Gabrielle Bezerra Sales Sarlet e Carlos Alberto Molinaro. Revisão do Prof. Dr. Ingo Wolfgang Sarlet.

[2] Professor afiliado de Inovação e Direito na Bucerius Law School, Hamburgo. Professor emérito de direito público e administração pública da Universidade de Hamburgo. De 1995 a 1997, foi chefe do Departamento de Justiça (Senador) do Estado de Hamburgo, além de Presidente do Comitê de Direito do Bundesrat alemão. De 1999 a 2008, ele foi Juiz do Tribunal Constitucional alemão. Seu campo de responsabilidade como relator incluiu - entre outros - a proteção da privacidade e dos dados, a liberdade de expressão e informação, bem como a inviolabilidade do lar. De 1979 a 1995, 1997 a 1999, foi diretor do Hans-Bredow-Insitute on Radio and TV-Broadcasting. Na Universidade de Hamburgo, fundou e presidiu o Centro de Pesquisa em Direito e Inovação (1995 - 2012). Ele ainda é um dos diretores do Instituto de Pesquisa sobre a Lei de Proteção Ambiental da Universidade de Hamburgo. Desde 2007, ele é membro alemão da "Comissão Europeia para a Democracia através do Direito" (Comissão de Veneza) do Conselho da Europa.

SUMÁRIO: 1. A transformação digital. 2 A transformação digital como um desafio para o Direito. 3. Dados. 4. Comparação entre o petróleo bruto e os dados em bruto. 5. Algoritmos e inteligência artificial. 6. Big Data e Analítica em Big Data. 6.1. Big Data. 6.2 Analítica de Big Data. 7. Sobre a crescente importância social da digitalização. 8. Proteção individual e coletiva de ativos jurídicos significativos. 8.1 Proteção à Liberdade. 8.2 Especialmente: Efeito horizontal da proteção da liberdade e do mandato para o delineamento das possibilidades de exercício da liberdade. 8.3 Especialmente: Inovações em matéria de direitos fundamentais para a proteção dos bens jurídicos. 9. As dificuldades em conceber uma proteção jurídica eficaz. 9.1 Convergências e delimitações. 9.2 Concentração de poder. 9.3 Coleta e utilização de dados. 9.3.1 Requisitos gerais para a licitude da coleta e tratamento de dados. 9.3.2 Revogação da vigência da lei nos Termos e Condições Gerais, em particular: à exigência de consentimento. 9.3.3 Dificuldades na aplicação dos princípios básicos de proteção de dados em aplicativos de Big Data. 9.3.4 A proteção também dos interesses jurídicos coletivos. 9.3.5 Défices de transparência. 9.3.6 Especialmente: Estado de Vigilância. 10. Conclusão provisória: necessidade de revisão da lei existente. 11. Abordagens para possíveis soluções. 11. 1 Redefinição do conceito de dados pessoais. 11.2 Aperfeiçoar a proteção jurídica do consentimento para o processamento de dados. 11.3 Aplicabilidade e reformulação dos Princípios Jurídicos da Proteção de Dados. 11.4 Aumentar a transparência no que respeita ao design técnico e aos algoritmos utilizados. 11.5 Expansão da proteção sistêmica. 11.6 Ampliação da supervisão soberana. 11.7 Ampliação da proteção jurisdicional. 11.8 Limitar as disparidades na distribuição do poder. 11.9 Avaliações de impacto. 11.10 Medidas para aperfeiçoar a cibersegurança. 11.11 Autorregulação e corregulação. 11.12 Melhores Práticas, Benchmarking entre outros. 11.13 Proteção em relação a vigilância do Estado. 12. Associação com outros direitos de regulação e desenvolvimento de estruturas de governação adequadas. 13. Anexo - Dados coletados pelo Facebook para fins de publicidade direcionada.

1. A TRANSFORMAÇÃO DIGITAL

Esta monografia trata da importância do direito nos processos de digitalização, especialmente ao fazer uso de Big Data. O termo "digitalização" refere-se inicialmente apenas às tecnologias da informação específicas que processam dados digitais e às infraestruturas (software e hardware) criadas para as tecnologias digitais. No entanto, o termo também representa a mudança fundamental nas condições de vida desencadeada pela sua utilização em todo o mundo. Permite a utilização de sistemas ciberfísicos para novos processos de produção em rede e automatizados (por exemplo, na indústria 4.0), alterações na forma como as pessoas vivem as suas vidas (por exemplo, na "casa inteligente"[*]), a criação e utilização de redes sociais (como o Google ou o Facebook) e outros novos serviços de comunicação (por exemplo, mensagens instantâneas), bem como novos sistemas de vigilância por empresas privadas e agências governamentais.

Os processos de mudança e adaptação afetam fundamentalmente todas as partes da sociedade[3]. A digitalização permite uma multiplicidade e variedade de novos modelos de negócio, bem como a sua utilização para criar valor. Isso muda as oportunidades de relações de influência e poder. Referimo-nos à transformação digital[4] que está transformando a economia, a sociedade, a cultura e muito mais. Afetam indivíduos que atuam proativamente, mas também estão envolvidos

[*] Smart Home (em inglês, pelo autor). Casas inteligentes, refere-se as habitações que incorporam uma rede de comunicações que conecta os principais aparelhos e serviços e permite que eles sejam controlados, monitorados ou acessados remotamente (Nota dos tradutores).

[3] Os Ministérios Federais da Economia e Energia, do Trabalho e dos Assuntos Sociais, da Justiça e da Defesa do Consumidor da Alemanha publicaram conjuntamente uma descrição e comparação das tendências e desafios, bem como das oportunidades possíveis e dos riscos esperados: BMWi/BMAS/BMJV, Digitalpolitik. Für Wirtschaft, Arbeit und Verbraucher. Trends – Chancen – Herausforderungen, Juni 2017. Aliás, representativo de muitos, veja as contribuições na edição temática de e&i Elektrotechnik und Informationstechnik, Digitale Transformation, Chancen und Risiken, Juli 2017. Como exemplo de uma visão otimista, consulte T. Ramge/V. Mayer-Schönberger, Das Digital: Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus, 2017. Ao final, isso quer dizer: „graças à riqueza de dados nosso futuro não apenas será mais personalizado, eficiente e sustentável, como acima de tudo sociável e profundamente humano", p. 266.

[4] Representativo de muitos, veja T. Cole, Digitale Transformation, 2015; C. Keese, Silicon Germany: Wie wir die digitale Transformation schaffen, 2017; O. Stengel/A. Van Looy/S. Wallaschkowski (Hsrsg.), Digitalzeitalter – Digitalgesellschaft: Das Ende des Industriezeitalters und der Beginn einer neuen Epoche, 2017; R. Pfliegl/C. Seibt, Die digitale Transformation findet statt!, 2017; e&i Elektrotechnik und Informationstechnik (nota de rodapé 3), 333-339; S. Zuboff, Surveillance Capitalism, 2018, A. Rolf, Weltmacht Vereinigte Daten: Die Digitalisierung und Big Data verstehen, 2018; I. Schneider, Bringing the state back in. Big Data-based capitalism, disruption and novel regulatory approaches in Europe, in: R. Saetnan/I. Schneider/N. Green (Ed.), The politics of Big Data – Big Data – Big Brother?, 2018. O significado histórico dessa transformação, na opinião de muitos, não ficará por trás do da invenção da impressão ou industrialização.

passivamente nessas mudanças (indivíduos, cientistas, funcionários), empresas econômicas, associações e outras comunidades, bem como autoridades estatais ou interestaduais.

Um elemento do uso de técnicas digitais é o uso de Big Data[5]. O termo refere-se à dimensão e à diversidade dos dados que podem ser utilizados para a aplicação das tecnologias digitais, bem como às várias possibilidades de as combinar e avaliar e de as tratar pelas autoridades públicas e privadas em diferentes contextos. Os megadados são utilizados para controlar comportamentos individuais e coletivos, para registar tendências de desenvolvimento, para permitir novos tipos de produção e distribuição, bem como tarefas do Estado, mas também para novas formas de ilegalidade, especialmente o cibercrime.

O potencial da digitalização e da utilização de grandes volumes de dados está atualmente a ser consideravelmente ampliado pelos avanços da inteligência artificial[6]. Em termos gerais, isto se refere a métodos que permitem aos computadores lidar com tarefas tão complexas que requerem inteligência quando resolvidas por humanos. O computador torna-se, por assim dizer, um instrumento técnico "pensante" que pode trabalhar em problemas de forma independente e - em sistemas de aprendizagem - desenvolver ainda mais os programas aplicados de forma independente.

Novas qualificações-chave, como engenharia de software, segurança de TI, computação em nuvem ou análise de dados estão se tornando importantes como resultado das mudanças. Em muitos setores, estão surgindo novas possibilidades de resolução de problemas com apoio digital, por exemplo no domínio do diagnóstico e terapia medicamentosas, da genética, da vida profissional (informatização, utilização de robôs), do controle dos sistemas de tráfego ou da monitorização dos espaços públicos, da meteorologia ou mesmo da influência de processos no mercado financeiro controlada por algoritmos. Ao mesmo tempo, os

[5] Veja abaixo nota 6.

[6] Sobre Inteligência Artificial, veja p. ex., E. Alpaydin, Machine Learning, 2016; J. Reichwald, D. Pfisterer, Autonomie und Intelligenz im Internet der Dinge, Computer und Recht, CR 2016, 208-212, 210. Para uma introdução compreensível aos problemas de inteligência artificial S. Russel/P.Norvig, Künstliche Intelligenz: Ein moderner Ansatz, 2012; O. Stiemerling, Künstliche Intelligenz" – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge. Eine technische Perspektive, CR 2015, 762-765; J. Jakobs, Vernetzte Gesellschaft. Vernetzte Bedrohungen. Wie uns die künstliche Intelligenz herausfordert, 2016; Bitkom, Künstliche Intelligenz verstehen als Automation des Entscheidens. Leitfaden, 2017, www.bitkom.org/Bitkom/Publikationen/Kuenstliche-Intelligenz-verstehen-als-Automation-des-Entscheidens.html, Acesso 31.05.2018; M. Lenzen, Künstliche Intelligenz. Was sie kann & was uns erwartet, 2018; K.D. Ashley, Artificial Intelligence and Legal analytics, 2017/2019.

métodos estão mudando nos campos científicos em questão e novos insights estão se formando[7].

A transformação digital traz consigo oportunidades para melhorar as condições de vida, mas também riscos para o bem-estar dos indivíduos e para a preservação de uma ordem social justa. Se/e como as oportunidades oferecidas pela digitalização podem ser exploradas e os riscos minimizados podem ser moldados. Entre os atores de formação incluem-se empresas econômicas, inovadores individuais, grupos de interesse, muitos usuários, mas também hackers. A criação de precauções para salvaguardar o bem-estar individual e público está em mãos de todos os envolvidos. Ao mesmo tempo, esta é uma tarefa importante dos Estados. Para seu cumprimento, o meio de controle do direito pode ser usado, entre outras opções.

2 A TRANSFORMAÇÃO DIGITAL COMO UM DESAFIO PARA O DIREITO

A discussão pública, mas também a atenção da ciência, especialmente da jurisprudência, tem concentrado o desdobramento das tecnologias e dos usos digitais, especialmente nas últimas décadas, inicialmente sobre o tema da proteção de dados por meio do direito. O foco foi nas preocupações sobre a expansão da vigilância estatal e, mais tarde, também sobre o uso e abuso de dados pessoais por parte do setor privado. Na Alemanha, um debate realizado na década de 1980 sobre os riscos correspondentes representou um ponto de viragem. Pretendia-se realizar um censo em que os dados pessoais eram recolhidos anonimamente para fins estatísticos e processados através de computadores. O conteúdo dizia respeito ao registo do nome, residência, forma de subsistência e ocupação das pessoas envolvidas no recenseamento. Este foi um assunto relativamente inocente comparado com o uso de computadores hoje em dia. O censo seria realizado em 1983, perto do ano emblemático de 1984, que foi o ano que marcou o título do famoso livro de George Orwell sobre "Big Brother" - um sistema de vigilância e repressão estatal. Esta discussão abalou parte do público, incluindo muitos estudantes, e colocou a questão dos possíveis riscos do uso do computador para a sociedade na agenda pública.

Devido a diversas Reclamações Constitucionais[*] foi o Tribunal Constitucional Federal alemão, que em uma "decisão histórica" forneceu a base para o direito à autodeterminação informativa, que influenciou significativamente o desenvolvimento do direito de proteção de dados na Alemanha e em outras partes

[7] Sobre o impacto na ciência, representativo de muitos, veja C. Wadephul, Big Data in der Wissenschaft, in B. Kolany-Raiser/R. Heil/C. Orwat/T. Hoeren (Ed.), Big Data und Gesellschaft. Eine multidisziplinäre Annäherung, 2018, 17-27.

[*] Cf., Verfassungsbeschwerden, Grundgesetz für die Bundesrepublik Deutschland (GG), artigo 93, n. 1 (4a. e 4b.); cf., ainda quanto ao procedimento, Gesetz über das Bundesverfassungsgericht (Bundesverfassungsgerichtsgesetz - BVerfGG) artigos 90 a 96 (Nota dos tradutores).

da Europa[8]. O tema da proteção de dados pessoais desperta atualmente grande interesse em todo o mundo. Em 2018, o Regulamento de Proteção de Dados Pessoais (RGPD pelo acrônimo em português[*]) entrou em vigor na União Europeia, harmonizando os princípios fundamentais da proteção de dados em toda a UE e tornando-os vinculativos[9]. Mas a proteção de dados é também um importante tema para fora da Europa.

Atualmente, a proteção jurídica não pode limitar-se à proteção de dados pessoais individuais. A necessidade de moldar o futuro desenvolvimento através do direito diz essencialmente respeito a todas as facetas da digitalização e da utilização de grandes volumes de dados e de inteligência artificial, mesmo que os dados em causa não sejam pessoais ou já não sejam pessoais em resultado da anonimização, ou mesmo quando se tratar de dados industriais sem vínculo pessoal. No entanto, o novo RGPD, que se limita à proteção de dados pessoais, não é mais suficiente, porque a digitalização também provoca consequências sociais além da preocupação individual. A visão deve ser ampliada em termos de aspectos sociopolíticos e legais, a saber, as oportunidades e os riscos da digitalização no Estado e na sociedade como um todo e sem limitação às áreas nacionais envolvidas.

A transformação digital desenvolveu-se inicialmente com base em estruturas tradicionais, incluindo os anteriores ordenamentos do Estado, da economia e da sociedade. Ela encontrou e ainda encontra um sistema jurídico que tem sido desenvolvido ao longo da história: direito público nacional, direito civil e direito penal, incluindo muitas áreas especiais, como o direito médico ou o direito sobre o mercado financeiro. Com a globalização do desenvolvimento, o direito europeu, o direito transnacional e o direito internacional também são afetados. Na medida em que a ordem jurídica inclui competências e tarefas para moldar a ordem social, isso também afeta o processo e os resultados da transformação digital, que agora são extraordinários.

As inovações provocam respostas à questão de saber se e em que medida as regras jurídicas tradicionais são adequadas para fazer justiça à problemática da situação em transformação e para implementar de forma otimizada os novos valores-alvo ancorados na ordem jurídica e social até à data ou mesmo os valores importantes sob as novas condições. Entre os importantes objetivos contam-se a proteção da liberdade individual, a observância dos princípios do Estado de direito, o funcionamento da ordem democrática, mas também um maior

[8] BVerfGE 65, 1. Veja abaixo item 8.3.

[*] Pelo acrônimo em inglês GDPR - General Data Protection Regulation. DSGVO (Datenschutz-Grundverordnung) pelo acrônimo em alemão (Nota dos tradutores).

[9] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (regulamento de base sobre a proteção de dados), ABl L 119 vom 9. Mai 2016, 1 e ss. Subsequentemente, a Lei Federal Alemã de Proteção de Dados foi revista: BDSG (neu), veja Bundesgesetzblatt (BGBl) I (2017), Nr. 44, 2092.

desenvolvimento econômico e tecnológico e a necessária capacitação para as inovações. A questão central é: como podemos alcançar objetivos de política pública, além das oportunidades sociais e individuais globais do uso de digitalização e, ao mesmo tempo, também tendo em conta os riscos envolvidos?

Menciono seletivamente os objetivos de assegurar a autodeterminação individual e coletiva, a proteção da privacidade, a igualdade de oportunidades, a responsabilidade pelas consequências, a segurança, a proteção contra o controle inconsciente e a discriminação. Até que ponto as oportunidades podem ser garantidas com a ajuda da lei existente, mas os riscos devem ser minimizados tanto quanto possível? Em que medida requer conceitos ou instrumentos alterados ou mesmo fundamentalmente novos de regulação legal, possivelmente até novos modos de governança?[10] Além dos modos de governança tradicionalmente usados de mercado, hierarquia, negociação e rede, o controle de comportamento e estruturas baseado em algoritmos é um novo tipo de modo de governança, também chamado de "regulação algorítmica".[11] Isso pode - como outros modos de governança - ser acoplado a outros estilos de governança (misto de governança).

Há que ter sempre presente que a digitalização está associada a desenvolvimentos inovadores, pelo que a arquitetura jurídica também deve ter o cuidado de não desperdiçar o potencial de inovação. No entanto, há que ter igualmente em conta que os desenvolvimentos inovadores ocorrem frequentemente através da sobreposição ou mesmo da destruição das abordagens

[10] A pesquisa sobre governação aborda diferentes modos de análise. Da rica literatura, faz-se referência a G. Schuppert, Governance-Forschung. Vergewisserung über Stand und Entwicklungslinien, 2005; assim, Governance und Rechtsetzung. Grundfragen einer modernen Regulierungswissenschaft, 2011. W. Hoffmann-Riem, Die Governance-Perspektive in der rechtswissenschaftlichen Innovationsforschung, 2011.

[11] K. Yeung, Algorithmic Regulation: A Critical Interrogation, 2017. De acordo com a definição da autora: (6): „Algorithmic regulation refers to decision-making systems that regulate a domain of activity in order to manage risk or alter behaviour through continual computational generation of knowledge by systematically collecting data (...) emitted directly from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine (…) the system's operation to attain a pre-specified goal." (em inglês pelo autor. "Regulação algorítmica refere-se a sistemas de tomada de decisão que regulam um domínio de atividade de modo a gerir o risco ou alterar o comportamento através da contínua geração computacional de conhecimento, recolhendo sistematicamente dados (...) emitidos diretamente de numerosos componentes dinâmicos pertencentes ao ambiente regulado, a fim de identificar e, se necessário, refinar automaticamente (...) o funcionamento do sistema para atingir um objetivo pré-especificado". (Trad. Livre pelo tradutor). Veja mais em N. Braun Binder, Algorithmic Regulation – der Einsatz algorithmischer Verfahren im staatlichen Steuerungskontext, in: H. Hill/J. Wieland (Ed.), Zukunft der Parlamente – Speyer-Konvent, 2018. F. Musiani, Governance by algorithms. Internet Policy Review vol. 2, 2013, http://policyreview.info.

tradicionais (inovação disruptiva)[12]. Além disso, convém observar que a inovação tecnológica não é, de modo algum, apenas a única questão, mas também, em grande medida as inovações sociais.[13] Isto ilustra, por exemplo, a importância das redes sociais para a concepção não só dos processos de comunicação, mas também das oportunidades de desenvolvimento individual e social em quase todas as áreas.

3. DADOS

A digitalização pressupõe o processamento de dados analógicos em dados digitais utilizando uma linguagem binária. Isso permite, entre outras coisas, o processamento de informações pela máquina, a transmissão automatizada de dados e a transmissão de informações para seres humanos e máquinas.

Os dados na literatura teórica da informação[14] são entendidos como sinais ou símbolos para mensagens que podem ser formalizadas e (aleatoriamente) reproduzidas e facilmente transportadas por meio de meios técnicos adequados. Os dados, enquanto tais, não têm significado. No entanto, podem ser portadores de informação, nomeadamente "informação codificada". O significado é-lhes atribuído quando estão envolvidos num processo de comunicação de informação por um remetente e de geração de informação pelo destinatário, ou seja, quando se tornam objeto de comunicação. Esta comunicação pode ocorrer entre humanos, mas também entre humanos e máquinas ou entre máquinas.

Note-se, contudo, que o conceito de dados na chamada legislação em matéria de proteção de dados é definido de forma mais estrita como um direito à proteção da personalidade, ou seja, conteúdos relacionados com informações de um determinado tipo. Por exemplo, o Artigo 4º Nº 1 do RGPD define "dados pessoais" na acepção do presente regulamento como "toda a informação relativa a uma pessoa singular identificada ou identificável". Uma pessoa singular identificável é aquela que pode ser identificada direta ou indiretamente, nomeadamente por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou a uma ou mais características específicas que constituem expressões da identidade física, fisiológica, genética, psicológica, econômica, cultural ou social dessa pessoa singular. O RGPD refere-se exclusivamente à "proteção das pessoas no que diz respeito ao tratamento de dados pessoais e à livre circulação de tais dados" (Art. 1, parágrafo 1). Não é

[12] Cf., para a cunhagem do conceito T. Christensen, The Innovator's Dilemma. Warum etablierte Unternehmen den Wettbewerb um bahnbrechende Innovationen verlieren, 2011.

[13] Para o conceito veja W. Zapf, Über soziale Innovationen, in: Soziale Welt 1989, Bd 40, 170 e ss.

[14] Para mais informações, consultar, por exemplo T. Vesting, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, 2012, in: W. Hoffmann- Riem/E. Schmidt-Aßmann/A. Voßkuhle (Ed.), Grundlagen des Verwaltungsrechts. Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen 2012.

especificamente voltado para Big Data, mas enlaça Big Data no que se refere ao processamento de dados pessoais. No entanto, os usos de Big Data não estão limitados a informações pessoais.

4. COMPARAÇÃO ENTRE O PETRÓLEO BRUTO E OS DADOS EM BRUTO

Os dados digitais são frequentemente mencionados em discussões públicas como uma espécie de "petróleo bruto da sociedade moderna"[15]. Por um lado, isto alude à sua grande importância econômica e à diversidade de utilizações possíveis do petróleo e dos dados. Por outro lado, devem ser tidas em conta as enormes dimensões tecnológicas, econômicas, políticas, societais etc., que emanam da disponibilidade destas "matérias-primas". De outro lado, as enormes possibilidades tecnológicas, econômicas, políticas, societais etc., que resultam da disponibilidade destas "matérias-primas", que estão geralmente associadas às mudanças em vários domínios da sociedade[16]. A comparação com o petróleo bruto deve esclarecer, em particular, os potenciais dos dados digitais. No entanto, as questões relacionadas ao uso desses fatores de produção, em particular a relevância dos dados para as economias regional e global, não podem, aqui, de maneira geral ser abordadas.

A seguinte - um tanto metafórica - comparação entre o petróleo bruto e os dados digitais têm outro objetivo: serve para ilustrar as características especiais dos dados que são usados como produtos ou fatores de produção, de tal forma que eles criam oportunidades para a economia e a sociedade que não existiam anteriormente.

As seguintes seis teses enfatizam as diferenças entre o petróleo bruto e os dados digitais:

- Ao contrário do que acontece com o petróleo - e também com o gás natural - os dados podem ser produzidos em segundos e o fornecimento de dados digitais é basicamente ilimitado na sociedade da informação. Em particular, o processamento de dados não recorre a um "tesouro" que foi formado no passado imensurável. Pelo contrário, o estoque de dados é diariamente alargado em nível mundial - por um lado, por aqueles que utilizam as vantagens da digitalização para produzir novos dados e, por outro lado, pela recolha de dados sem ou contra a vontade das pessoas afetadas.
- Os dados não se escondem em camadas profundas de rocha e não requerem buracos complicados ou mesmo perigosos. Eles estão praticamente em todos os lugares e são tecnicamente fáceis de capturar e armazenar. Há uma

[15] Exemplos do uso dessa metáfora podem ser encontrados em M. Spitz, Daten. Das Öl des 21. Jahrhunderts? Nachhaltigkeit im digitalen Zeitalter, 2017, 9-13.

[16] Mais próximo da comparação da importância do petróleo bruto e dos dados em diferentes áreas sociais, veja M. Spitz (nota 13 supra). Spitz pergunta em particular (mas não somente) se/e em que medida os processos desencadeados pelo petróleo bruto – incluído a concentração de poder – oferecem razões para aprender lições para lidar com dados.

infinidade de "tanques" pequenos e grandes de dados em todo o mundo - desde o computador individual, passando pelos bancos de dados de várias empresas e autoridades estaduais, até os mainframes dos provedores de nuvem. A maioria dos tanques deste tipo está ficando mais cheia a cada dia e o valor de muitos dos recursos de dados já existentes aumenta principalmente pelo reabastecimento e por novos métodos de avaliação. O mesmo se aplica ao valor dos dados reabastecidos no contexto dos dados já existentes.

- Os dados brutos devem ser processados de forma semelhante ao petróleo bruto para serem utilizáveis. Em todos os lugares existem pequenas "refinarias" de dados, incluindo aquelas nas mãos de players (atores) particularmente poderosos, como Google, Facebook, Microsoft ou Amazon, bem como empresas especiais de nuvem de dados, mas também agências governamentais como os EUA. Agência Nacional de Segurança dos EUA (NSA) ou outros serviços de inteligência. O processamento dos dados cria mais conhecimento que transmite poder, não apenas nos mercados econômicos, mas pelo menos potencialmente em quase todas as áreas da ação social.
- Assim como produtos de alta qualidade podem ser produzidos refinando óleos crus, técnicas inovadoras, como o uso de sofisticadas formas de inteligência artificial, permitem novos produtos "refinados" com novo valor agregado. Os mesmos dados - ao contrário do petróleo - podem ser alimentados em diferentes "acabamentos". Até mesmo o produto "refinado" pode ser usado como matéria-prima para "acabamento" relacionado a dados.
- Ao contrário do petróleo ou do gás, a utilização de dados - incluindo a sua coleta e tratamento legais e ilegais pelos serviços secretos do Estado ou por terceiros privados - não significa o seu consumo (a chamada não rivalidade no consumo). Através do processamento, o valor de tesouraria dos dados pode até aumentar e podem ser utilizados para muitos outros fins. Ao longo do tempo, porém, certos dados podem perder a sua atualidade ou usabilidade, mas podem voltar a ser importantes no futuro no contexto de outras aplicações.
- Os dados digitais, ao contrário do óleo, não são visíveis aos olhos humanos devido à sua desmaterialização. O fluxo e o uso dos dados não são, portanto, reconhecíveis por terceiros, ou apenas com esforço técnico especial. O valor acrescentado a obter através do processamento e da utilização pode ser igualmente invisível. Isto torna mais fácil para as empresas ocultarem este valor acrescentado e quaisquer lucros que possam ser gerados, por exemplo, pelas autoridades fiscais. Isso também aumenta as oportunidades de lucro.

As particularidades dos dados digitais assim apresentados e a forma como são tratados são pontos de partida para a sua especial importância econômica, mas

também política, cultural, ecológica e social em muitas áreas da vida social. Também possibilitam inovações de várias formas e são uma das causas das mudanças estruturais, incluindo a concentração de poder de muitas áreas marcadas pela digitalização. Ao mesmo tempo, podem ser observadas assimetrias consideráveis nas possibilidades de utilização dos recursos de dados, por exemplo, na clarificação da questão de saber se é dada a devida atenção à usabilidade dos dados, se todas ou quais as partes interessadas têm acesso aos dados, se são tratadas de forma responsável e se os diferentes interesses dos membros da sociedade são tidos em conta de forma equitativa através da utilização dos dados.

5. ALGORITMOS E INTELIGÊNCIA ARTIFICIAL

Os algoritmos são indispensáveis para a utilização de dados digitais [17]. Algoritmos são - em geral - regras que resolvem certas tarefas em etapas individuais definidas - de forma determinística. Tais algoritmos também existem fora da digitalização, por exemplo, para o controle técnico de máquinas. Para que possam ser utilizados em computadores, os algoritmos devem ser escritos numa linguagem digital - processável por computador - e a tarefa em questão é então processada de acordo com um padrão específico, com a ajuda de passos individuais predefinidos. Na maioria dos casos, os algoritmos individuais são partes de sistemas de decisão digitais complexos, consistindo em software e hardware e incorporados em sistemas de informação socio-técnicos.

Atualmente, a capacidade de computação e as possibilidades de análise oferecidas pelos computadores estão sendo muito ampliadas, bem como as possibilidades de aplicação e desempenho dos algoritmos estão crescendo e mudando em rápida sucessão. A inteligência artificial é particularmente importante para isto[18]. Este termo refere-se, em particular, ao esforço de reproduzir digitalmente estruturas de decisão semelhantes às humanas, ou seja, de conceber um computador e, em particular, de o programar utilizando as chamadas redes neurais[19], de modo a poder trabalhar os problemas da forma mais independente possível e, se necessário, continuar a desenvolver os programas utilizados.

Atualmente, o desenvolvimento de sistemas de aprendizagem está sendo promovido ou fomentado. Isso inclui a denominada aprendizagem de máquina. É usada para reconhecer padrões, avaliar imagens, traduzir o idioma em textos e apoiar decisões (como Scoring, Ranking, Predicting[*]). O objetivo também é lidar com tarefas particularmente complexas, como a produção industrial com a ajuda

[17] Como uma introdução geralmente compreensível para as propriedades e possibilidades de algoritmos, cf., C. Drösser, Total berechenbar? Wenn Algorithmen für uns entscheiden, 2016.

[18] Ver as verificações supra (nota de rodapé 6).

[19] Isto se refere a redes de neurônios artificiais que são replicadas de redes neuronais naturais.

[*] Em inglês pelo autor: pontuação, classificação, previsão (Nota dos tradutores).

de robôs ou a avaliação de imagens de raios-X na medicina e muito mais. Mas, algoritmos podem fazer mais[20].

Cada vez mais, os sistemas baseados em algoritmos de aprendizagem são capazes de se adaptar de forma independente a novas situações problemáticas e continuar seus próprios programas. Algoritmos de aprendizado não são apenas programados para resolver problemas específicos, mas também para aprender a resolver problemas [21]. Eles devem então ser capazes de se desenvolver independentemente da programação humana. Alguns falam em "aprendizagem profunda" [22]. Aqui o sistema aprende sem intervenção humana adicional; em particular, pode capturar relacionamentos, estruturas e arquiteturas e melhorar seu desempenho de forma independente. A capacidade de aprendizagem do sistema condiciona os procedimentos de forma independente. Os passos individuais, como tais, permanecem controlados de forma determinista; no entanto, eles existem em grande número e muitas vezes estão dinamicamente conectados de modo que é difícil ou quase impossível reconstruir o determinístico. Tais programas orientados para o aprendizado são usados, por exemplo, no processamento de imagens e linguagem, robótica e prognóstico.

O procedimento humano anteriormente requerido para a programação de algoritmos e sistemas algorítmicos complexos está se tornando cada vez menos importante em sistemas de aprendizado com a consequência de que os passos individuais e sua interação e a lógica usada pelos programadores não são mais compreensíveis. Andrew Tutt formulou para tais sistemas de aprendizagem:

> […] Even if we can fully describe what makes them work, the actual mechanisms by which they implement their solutions are likely to remain opaque: difficult to predict and sometimes difficult to explain. And as they become more complex and more autonomous, that difficulty will increase*.

[20] De rica literatura, veja, H. Surden, Machine Learning and Law, Washington Law Review 89, 2014, 87 e ss.; A. Tutt, An FDA for Algorithms, in: Administrative Law Review 2017, 83-123, em particular, 83-105; T. Wischmeyer, Regulierung intelligenter Systeme, in: Archiv des öffentlichen Rechts 2018, 143, 1-66.

[21] Para esse efeito, ver, A. Tutt (nota de rodapé 20 supra), 85.

[22] I. Goodfellow/Y. Bengio/A. Courville, Deep learning, 2016; C. Müller-Hengstenberg/S. Kirn, Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems?, in: Multimedia und Recht 2014, 307-313; F. Stalder, Kultur der Digitalität, 2016, 177 e ss.; T. Wischmeyer (nota de rodapé 20), 11-14 e *passim*.

* Em inglês no original ("Mesmo que possamos descrever plenamente o que os faz funcionar, os mecanismos através dos quais eles implementam as suas soluções tendem a permanecer opacos: difíceis de prever e, por vezes, difíceis de explicar. E à medida que se tornam mais complexos e mais autônomos, essa dificuldade aumentará." Trad. Livre). Tutt, A. 2016. 'An FDA for algorithms?' Administrative Law Review 69, 83-123, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994.

Isso também aborda o problema da falta de controlabilidade humana do desenvolvimento autodirigido dos programas. Mesmo os desenvolvedores e programadores podem perder a transparência dos processos. As possibilidades de supervisão humana ou mesmo de contrariar acontecimentos ou catástrofes indesejáveis são dificultadas ou mesmo eliminadas[23]. Não surpreende, portanto, que nos últimos tempos cada vez mais pessoas tenham sido alertadas para a utilização indiscriminada da inteligência artificial, mesmo por atores que, ao longo das suas vidas, promoveram o desenvolvimento da inteligência artificial e a utilizaram intensivamente para fins comerciais[24].

6. BIG DATA E ANALÍTICA EM BIG DATA

A seguir, o foco está em lidar com Big Data. Para entender o que deve ser dito, é importante caracterizar os fenômenos de Big Data e o uso da função analítica em Big Data. A combinação e o trabalho em rede de dados como Big Data e seu processamento por meio da análise de Big Data são particularmente atraentes para a possibilidade de lidar com grandes dados e para o valor agregado digitalmente associado.

6.1. BIG DATA

O termo big data[25] refere-se às possibilidades de acesso a grandes quantidades de dados digitais ("alto *volume*"), de diferentes tipos e qualidade, bem como várias possibilidades de coleta, armazenamento e acesso ("alta *variedade*"), e alta velocidade de seu processamento ("alta *velocidade*"). A utilização da inteligência

[23] Por exemplo, A. Tutt (nota de rodapé 20), 85, aponta para riscos significativos para os indivíduos e a sociedade no caso de os algoritmos de aprendizagem produzirem erros ou serem indevidamente utilizados.

[24] Menção deve ser feita do cofundador da PayPal e proprietário da Tesla Elon Musk, o fundador da Microsoft, Bill Gates, ou o cofundador da Apple, Steve Woznak. Comprovado por M. Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, Harvard Journal of Law & Technology 2016, 29, 353, 355. Há também críticas fundamentais ao desenvolvimento. A título de exemplo, é feita referência às obras especificamente alarmante escritas por N. Bostrom, Superintelligence, paths, dangers, strategies, 2013 e M. Tegmark, Life 3.0. Being Human in the Age of Artificial Intelligence, 2017; N. Colwin, The Internet Apologizes … Even those who designed our digital world are aghast at what they created. A breakdown of what went wrong – from the architects who built it, 2018, http://nymag.com/selectall/2018/04/an-apology-for-the-internet-from-the-people-who-built-it.html.

[25] Para Big data, ver entre muitos, Taeger, Big Data & Co: Neue Herausforderungen für das Informationsrecht. Tagungsband Herbstakademie 2014; Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 2014; V. Mayer-Schöneberger/K. Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think, 2013; T. Hoeren (Ed.), Phänomene des Big-Data-Zeitalters, 2019.

artificial, em especial, torna possível novas formas altamente eficientes de tratamento de dados, a verificação da sua coerência e também a garantia de qualidade ("*veracidade*"). Além disso, Big Data é o objeto e a base de novos modelos de negócio e as possibilidades de criação de valor ("*valor*"). Estes são os cinco "*V*" para identificar Big Data.

Exemplos de suas aplicações são: comunicação eletrônica (por exemplo, com o smartphone); interação e comunicação nas redes sociais; tecnologias em rede (smart home, smart meter); sistemas de assistência de voz como o Alexa da Amazon; vigilância eletrônica; uso de cartões de crédito ou de fidelização; mobilidade inteligente e outros.

6.2 Analítica de Big Data

Para a interpretação dos dados e a expansão das possibilidades de utilização de dados, especialmente com a ajuda da inteligência artificial, destaca-se o "Big Data Analytics"* (frequentemente utilizado apenas como um termo em inglês: Big Data Analytics). A este respeito, são utilizados procedimentos analíticos diferentes para fins diferentes:

- A análise descritiva serve para filtrar e processar o material para fins de avaliação. Um exemplo de campo é o uso de big data para mineração de dados [26] e para o registro e sistematização dos dados (em particular priorização, classificação e filtragem).

* Hoje, muitas organizações estão coletando, armazenando e analisando grandes quantidades de dados. Esses dados geralmente são chamados de "big data" devido ao seu volume, à velocidade com que chegam e à variedade de formas que toma. Big data está criando uma nova geração de gerenciamento de dados de suporte à decisão. As empresas estão reconhecendo o valor potencial desses dados e estão colocando as tecnologias, pessoas e processos em prática para aproveitar as oportunidades. Uma chave para derivar valor de big data é o uso de *análises*. Coletar e armazenar big data cria pouco valor; é apenas infraestrutura de dados neste momento. Ele deve ser *analisado* e os resultados utilizados pelos tomadores de decisão e processos organizacionais para gerar valor. *Big data e análise* estão interligados, mas a análise não é nova. Muitas *técnicas analíticas*, como análise de regressão, simulação e aprendizado de máquina, estão disponíveis há muitos anos. O que há de novo é a união de avanços em tecnologia e software de computador, novas fontes de dados (por exemplo, mídias sociais) e oportunidades de negócios. Essa confluência criou o interesse e as oportunidades atuais na *análise de big data*. Está até gerando uma nova área de prática e estudo chamada "ciência de dados", que abrange técnicas, ferramentas, tecnologias e processos para dar sentido a ideia de Big Data (Nota dos tradutores).

[26] Para este fim, entre outros, ver H. Petersohn, Data Mining: Verfahren, Prozesse, Anwendungsarchitektur, 2005; Y. Hofstetter, Sie wissen alles: Wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen, 2016, 88-89; P. Radlanski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, 25-28.

- A análise preditiva[27] tem por objetivo - ainda muito distanciada de um processo de compreensão - identificar indicadores para uma possível conexão de causalidade, mas (ao menos por enquanto) na forma de correlações estatisticamente significativas[28]; nessa forma, os eventos devem ser previstos com uma certa probabilidade. O objetivo é obter informações sobre o comportamento das pessoas e, por exemplo, identificar tendências e padrões de comportamento em desenvolvimento, prever comportamentos futuros e, a partir daí, poder tomar *Automated Decision Making* (ADM)*. A análise preditiva pode ser usada, por exemplo, para registrar preferências e desejos do consumidor (*Predictive Consumer Interests**), ou para o caso de "*Predictive Policing*"*[29]
- A análise prescritiva visa recomendações para a ação, a fim de utilizar o conhecimento descritivo e preditivo para alcançar determinados objetivos, por exemplo, para a seleção personalizada em preços ou para estratégias e táticas para influenciar atitudes e comportamentos, incluindo o impacto na formação da opinião pública e na percepção e apoio/prevenção da evolução social.

A analítica de grande volume de dados é voltada para a expansão e uso de conhecimento que pode ser gerado por dados de todos os tipos, especialmente no campo da inteligência artificial, em vários campos de aplicação. Permite muito mais do que a coleta, o armazenamento e a utilização de dados pessoais, que está no centro da legislação de proteção de dados tradicional.

7. Sobre a crescente importância social da digitalização

A importância dos dados e da utilização de algoritmos, incluindo a sua utilização no contexto dos grandes volumes de dados, está em pleno crescimento.

[27] Para o problema da análise preditiva, consulte os seguintes artigos em: W. Hoffmann-Riem (Ed.), Big Data – Regulative Herausforderungen, 2018; Y. Hermstrüwer, Die Regulierung der prädiktiven Analytik: Eine juristisch-verhaltenswissenschaftliche Skizze, 99-116; S. Dreyer, Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie, 135-143; T. Singelnstein, Big Data und Strafverfolgung, 179-185; T. Rademacher, Predictive Policing im deutschen Polizeirecht. Archiv des öffentlichen Rechts 2017, 142, 366-416.

[28] Par mais informações, veja V. Mayer-Schönberger/K. Cukier (cit., nota de rodapé 25).

* Em inglês no original (Tomada de decisão automatizada – ADM pelo acrônimo em inglês – nota dos tradutores).

* Em inglês no original (Interesses Preditivos do Consumidor) (nota dos tradutores).

* Em inglês no original, "Policiamento Preditivo" (nota dos tradutores).

[29] Cf., S. Gless, Predictive Policing und operative Verbrechensbekämpfung, in: F. Herzog/R. Schlothauer/W. Wohlers (Ed.), Rechtsstaatlicher Strafprozess und Bürgerrechte, 2016, S. 165 e ss.; T. Singelnstein, (nota 25); T. Rademacher, (nota 25).

Um grupo de pesquisa liderado pelo cientista de Zurique Michael Latzer[30] ilustrou aspectos individuais como segue:

> [...] Os algoritmos mudam a percepção do mundo, afetam nosso comportamento influenciando decisões, e são uma fonte importante de ordem social. Uma grande parte de nossas atividades diárias em geral e nosso consumo de mídia em particular são cada vez mais moldados por algoritmos que trabalham nos bastidores. Algoritmos são usados para monitorar nosso comportamento e interesses, bem como para prever nossas necessidades e ações futuras. Eles dirigem nossas ações e, assim, determinam, entre outras coisas, o sucesso econômico de produtos e serviços, mas também o nosso comportamento cultural e político.

Exemplos da utilização de algoritmos são a Internet das Coisas e a Internet dos Serviços, a utilização de aplicações como dispositivos auxiliares ou para a monitorização da saúde com a ajuda de objetos "inteligentes" (utilitários), ou as múltiplas redes na produção, distribuição e utilização de produtos (rubrica: indústria 4.0).

A vida cotidiana nem sempre é *on* nem *off-line*, mas ambas, para que um novo tipo de mundo – o mundo *onlife* – começa a se formar[31]. Os sistemas informáticos podem, em grande medida, dispensar as pessoas da necessidade de tomar decisões, ou seja, substituir as decisões humanas. Isto pode significar um ganho na qualidade de vida através do auxílio à decisão e da poupança de custos, mas também uma perda na medida em que a pessoa afetada não tem qualquer oportunidade realmente viável para uma intervenção voluntária e pode, portanto, tornar-se objeto de controle inconsciente e, de muitas maneiras, já se tornou objeto de controle inconsciente. O termo "inteligência ambiental", isto é, "ambiente inteligente" (*Ambient Intelligence*[*])[32] é usado para descrever a onipresença de um mundo digitalizado que pensa adiante das pessoas.

[30] M. Latzer/K. Hollnbuchner/N. Just/F. Saurwein, The economics of algorithmic selection of the Internet. In J. M. Bauer & M. Latzer (Ed.), Handbook on the Economics of the Internet, 2016, 395 (im Text oben eigene deutsche Übersetzung).

[31] Cf., M. Hildebrandt, Smart technologies and the end(s) of law: Novel entanglements of law and technology, 2015, 41 e ss., 77 e ss., 263.

[*] Em inglês no original, na computação, a inteligência ambiente (AmI, pelo acrônimo em inglês) refere-se a ambientes eletrônicos sensíveis e responsivos à presença de pessoas (nota dos tradutores).

[32] Cf., Y. Hofstetter, Das Ende der Demokratie: Wie die künstliche Intelligenz die Politik übernimmt und uns entmündigt, 2016, S. 28 e *passim*.

O uso de algoritmos também afeta naturalmente o cumprimento das tarefas de estado. São exemplos as utilizações no e-Governo[33] e na Administração da Justiça (esta última também sob a rubrica "Legal Technology*"[34]) - como por exemplo

[33] Cf., Bundesregierung, Digitale Verwaltung, BT-Drucks. 18/3074 (2014); Senat der Freien und Hansestadt Hamburg, Digital First – Chancen der Digitalisierung für eine bürgerfreundliche und moderne Verwaltung nutzen – Erweiterung der Strategie Digitale Verwaltung, Senatsdrucksache 2016/03060 (2016); v. a lei sobre o governo eletrônico (E-Government-Gesetz – EgovG) que entrará em vigor no ano de 2020; também, A. Roßnagel, Auf dem Wege zur elektronischen Verwaltung. Das E-Government-Gesetz, in: Neue Juristische Wochenschrift 2013, 2710-2716. Para informações gerais sobre o Governo Electrónico, ver M. Eifert, Electronigovernment: Das Recht der elektronischen Verwaltung, 2006; E. Engel, (Ed.), IT-Governance in Staat und Kommunen. Vernetzung, Zusammenarbeit und die Steuerung von Veränderungsprozessen in der öffentlichen Informationstechnik, 2015; S. Köhl,/K.Lenk/S. Löbel/T. Schuppan/K. Viehstädt, Stein-Hardenberg 2.0: Architektur einer vernetzten Verwaltung mit E-Government, 2014; U. Berlit, Elektronische Verwaltungsakte und verwaltungsgerichtliche Kontrolle, in: Neue Zeitschrift für Verwaltungsrecht 2015, 4, 197-200; N. Braun Binder, Vollständig automatisierter Erlass eines Verwaltungsaktes und Bekanntgabe über Behördenportale, Die Öffentliche Verwaltung 2016, 891 e ss.; T. Siegel, Automatisierung des Verwaltungsverfahrens – zugleich eine Anmerkung zu §§ 35a, 24 I 3; 41, IIa VwVfG, in: DVBL 2017, 24-28; H.P. Bull, Der „vollständig automatisiert erlassene" Verwaltungsakt – zur Begriffsbildung und rechtlichen Einhegung von e-Government, DVBL 2017, 409-417. Em julho de 2017, o artigo 91c da Lei Fundamental foi ampliado pelo n. 5, que prevê uma regulamentação do acesso aos sistemas de tecnologia da informação que abrange a Federação e os Estados federados.

* Em inglês no original (Tecnologia Jurídica). Sobre o tema cf., K. Williams/J. M. Facciola/P. McCann/V. M. Catanzaro, The Legal Technology Guidebook, 2017 (Nota dos tradutores).

[34] Para a tecnologia jurídica, consulte O. Raabe/R. Wacker, Recht ex machina: Formalisierung des Rechts im Internet der Dienste, 2012; Y. Frese, Recht im zweiten Maschinenzeitalter, in: Neue Juristische Wochenschrift 2015, 2090-2092; por exemplo, as contribuições de M. Kaulartz/N. Kuhlmann/J. M. Schmittmann, in: J. Taeger (Ed.), Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, 2016, 1023 e ss.; G. Buchholtz, Legal Tech. Chancen und Risiken der digitalen Rechtsanwendung, in: Juristische Schulung 2017, 955-960; V. Boehme-Neßler, Die Macht der Algorithmen und die Ohnmacht des Rechts. Wie die Digitalisierung das Recht relativiert, in: Neue Juristische Wochenschrift 2017, 42, 3031-3037; J. Wagner, Legal Tech und Legal Robots in Unternehmen und den diese beratenden Kanzleien, in: Betriebsberater 2017, 88-905; A. Klafki/F. Würkert/T. Winter (Ed.), Digitalisierung und Recht: Tagung des Vereins Junge Wissenschaft im öffentlichen Recht an der Bucerius Law School am 26. November 2016; M. Hildebrandt, Law as computation in the era of artificial legal intelligence. Speaking law to the power of statistics, in: Toronto Law Journal 2018; M. Hartung/M.-M Bues/M. Halbleib, Legal Tech. Die Digitalisierung des Rechtsmarkts, 2018; S. Breidenbach/F. Glatz, Rechtshandbuch Legal Tech, 2018; J. Wagner, Legal Tech und Legal Robots, 2018; W. Hoffmann-Riem, Legal Technology – Preconditions, Opportunities, and Risks, in: Bucerius Law Journal, 57 e ss. Crítico em relação à regulação por algoritmos, v., dentre muitos, J. Danaher, The Threat of Algocracy: Reality, Resistance and Accommodation, in: Philos. Technol. 2016, 29, 245-268. Ver, além disso, as evidências acima, nota de rodapé 11.

serviços jurídicos automatizados (nomeadamente, aconselhamento jurídico, investigação), gestão de contratos digitais, procedimentos digitais de resolução de litígios, decisões administrativas automatizadas. As medidas de vigilância do Estado[35], por exemplo, pela polícia ou pelos serviços de informações, são também controladas por algoritmos. Também se aplica à vigilância através da coleta de dados e da avaliação por agentes privados.

De particular importância são as atividades dos provedores de informação/plataformas[36] como o Google ou o Facebook. Os seus serviços não só permitem a coleta de muitos dados e sua utilização para a implementação de seus modelos de negócios. As infraestruturas digitais utilizadas pelos provedores de informação permitem uma variedade de formas de interação entre fornecedores de /serviços, utilizadores e anunciantes. As atividades dos intermediadores de informação* incluem igualmente o controle do comportamento dos utilizadores dos seus serviços.[37] Por exemplo, os intermediadores de informação podem influenciar o comportamento dos consumidores através de publicidade personalizada em linha. No entanto, também podem ajudar a moldar valores reconhecidos na sociedade ou influenciar o comportamento de votação política[38].

Os dados coletados podem ser repassados a outros atores públicos ou privados, que os processam em seus próprios campos de atividade e geralmente os relacionam com outros dados. Deve ser feita uma menção especial às possibilidades

[35] Cf., entre outros, M. Bäcker, Kriminalpräventionsrecht: eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, 2015; W. Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JuristenZeitung 2014, 53 e ss.

[36] Sobre as características das plataformas digitais, cf., N. Sreicek, Platform capitalism, 2017.

* Aqui em sentido amplo, englobando os provedores de acesso e os de conteúdo, isto é, como Intermediários da informação, tais como motores de busca, redes sociais ou portais de aplicativos, estão agora cumprindo uma função importante para a formação da opinião pública: além de outras funções, eles fornecem um ponto de acesso relevante para o desenvolvimento da informação. (cf., Wolfgang Schulz e Kevin Dankert, Die Macht der Informationsintermediäre Erscheinungsformen, Strukturen und Regulierungsoptionen, Bonn: Friedrich-Ebert-Stiftung Medienpolitik, 2016, https://bit.ly/2w3iKFu – nota dos tradutores).

[37] Sobre questões de regulação comportamental, veja, W. Schulz/K. Dankert, Die Macht der Informationsintermediäre: Erscheinungsformen, Strukturen und Regulierungsoptionen, 2016; H. Hill, Scientific Regulation – automatische Verhaltenssteuerung durch Daten und Algorithmen, in H. Hill/U. Schliesky (Ed.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, 2015, 258-287; W. Homann-Riem, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, in: Archiv des öffentlichen Rechts (AöR) 2017, 1-42, 11 e ss. Sobre questões juridicas relacionadas, v. J.-U. Pille, Meinungsmacht sozialer Netzwerke, 2016; M. Oermann, Rechts(durch)setzung durch Informationsintermediäre: Big Data als Entscheidungs- und Handlungsressource, in: Hoffmann-Riem, W. (Ed.), Big Data – Regulative Herausforderungen, 2018, 145-155.

[38] Para a formação de opiniões usando algoritmos ver, entre outros, K. A. Zweig/O. Deussen/T. D. Krafft, Algorithmen und Meinungsbildung, in: Informatik- Spektrum 2017, 40 (4), 318-326.

criadas pela digitalização para a utilização de tecnologias preditivas. Estas são utilizadas, por exemplo, para decisões sobre a concessão de crédito ou sobre a determinação individual do montante das tarifas de seguro de saúde ou de vida ou a diferenciação de preços no negócio em linha e para muitos outros fins. Exemplos das muitas outras possibilidades de digitalização são: a utilização de sistemas móveis; a ligação em rede de instalações como a *Smart Home* ou a *Smart Factory*; e a motorização autônoma.

Essas atividades criam novas oportunidades e riscos. Elas poderão resultar de eventos de danos acidentais (tais como falhas no sistema ou infraestruturas defeituosas); no contexto anglo-saxónico, isto é referido como um perigo para a segurança. Além disso, existem riscos de ataques direcionados[39]. A pirataria, a espionagem cibernética e a sabotagem cibernética são descritores individuais. A este respeito, o termo segurança é traduzido como Security[*] no uso anglo-saxónico.

No entanto, deve salientar-se que os Big Data, em combinação com a inteligência artificial, podem não só constituir estímulos para os ataques, mas também oferecer simultaneamente possibilidades para a sua defesa (ver ponto 11.10 infra).

Esses e outros campos para o uso de Big Data já estão parcialmente legalmente regulamentados. No entanto, como já mencionado, é necessário indagar se os instrumentos existentes ainda são suficientes ou se, no interesse de proteger os interesses envolvidos, é necessário alterar o sistema jurídico para novas soluções. As oportunidades e necessidades de regulamentação devem ser analisadas setor a setor, tendo em conta as oportunidades e os riscos existentes em cada um dos domínios em causa e as condições de enquadramento que aí se aplicam. Respostas unificadas são necessariamente eliminadas. Essa análise específica do objeto não pode e não deve ser feita de forma abrangente aqui, mas pretende-se que problemas individuais sejam levantados e possíveis soluções sejam discutidas.

8. Proteção individual e coletiva de ativos jurídicos[*] significativos

O quadro jurídico para as reações ao desenvolvimento é prestado pelo menos pelos princípios constitucionais do estado de direito e do bem-estar social e, sobretudo, pela proteção das liberdades. Para poder utilizar as garantias de liberdade, a sua ancoragem normativa não é suficiente; também deve haver

[39] T. Wischmeyer, Informationssicherheitsrecht. IT-Sicherheitsgesetz und NIS-Richtlinie als Elemente eines Ordnungsrechts für die Informationsgesellschaft, in: Die Verwaltung 2017, 50, 155-188.

[*] Em inglês no original, na acepção de proteção, isto é, de proteção de uma pessoa, prédio, organização ou país contra ameaças como crimes ou ataques de terceiros sejam pessoas, organizações terroristas ou governos. (Nota dos tradutores).

[*] "Rechtsgüter", aqui tomada a expressão para incluir interesses legais e bens jurídicos (Nota dos tradutores).

maneiras de percebê-las em termos reais. A proteção da liberdade, portanto, também inclui a garantia das condições não-legais para o uso da liberdade.

Não é apenas o direito de exercer a liberdade que deve ser assegurado, mas também a proteção contra as consequências do uso da liberdade por outros. Isso inclui assegurar a proteção do uso de liberdades individuais, mas também de bens e interesses legais coletivamente significativos. Estes últimos incluem o funcionamento da democracia, uma ordem plural de comunicação, proteção contra manipulação, prevenção de assimetrias no poder, mas também evitar a fragmentação social, bem como evitar os efeitos de intimidação, que podem surgir através da vigilância. Nesse sentido, o Estado é responsável por garantir a possibilidade de proteção da liberdade[40].

8.1 Proteção à Liberdade

O pressuposto consiste no enquadramento da realização prática das liberdades. Assim, as garantias dos direitos fundamentais são de pouca utilidade se os pré-requisitos econômicos, tecnológicos, culturais e outros não forem cumpridos. A realidade é moldada por privilégios e concentração de poder. Especialmente no que diz respeito à proteção da liberdade, na área da digitalização é importante saber se, e em que medida, as oportunidades para o exercício das opções são distribuídas de forma justa.

Os direitos à liberdade são padronizados em particular nas constituições nacionais - como na Lei Fundamental da República Federal da Alemanha – Grundgesetz für die Bundesrepublik Deutschland (GG) – , mas também na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia sobre Direitos Humanos, bem como em acordos internacionais como os Pactos de Direitos Humanos da ONU. Eles não se limitam a formas específicas de geração de dados e métodos de tratamento de dados na área temática aqui tratada. Por conseguinte, as garantias de longa data - no que diz respeito à comunicação no sentido mais lato - referem-se a todas as formas de comunicação, incluindo a comunicação digital. Também protege a informação que não se destina a ser comunicada a terceiros, mas que se destina a permanecer no seu próprio computador. Os direitos humanos e as liberdades civis também são decisivos para a geração, análise e utilização de Big Data. Os direitos de liberdade são também uma bitola para a avaliação jurídica de consequências fora do próprio processo de comunicação, tais como as decorrentes do tratamento da seleção algorítmica e do

[40] Para a tarefa de garantia e as peculiaridades do estado de garantia, consultar, entre outros, G. F. Schuppert, Der Gewährleistungsstaat. Ein Leitbild auf dem Prüfstand, 2005; H. Schulze-Fielitz, Grundmodi der Aufgabenwahrnehmung, in: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle (Ed.), Grundlagen des Verwaltungsrechts, 2012, Bd. I, § 12, nota de margem 154 e ss. Allgemein zu Themenfeldern, auf denen auch kollektive Interessen in den Blick geraten: T. Rademacher/T. Wischmeyer (Ed.), Regulating Artificial Intelligence, 2020.

controle do comportamento ou as resultantes da utilização de modelos de negócio utilizados no setor das TI.

A proteção da dignidade humana, o princípio da igualdade, a liberdade de comunicação, a proteção da privacidade, a liberdade de ocupação, a liberdade de religião ou a garantia de propriedade são universais e não se limitam ao uso de tecnologias tradicionais. Consequentemente, não há razão para suplementar todas as normas de liberdade e proteção dos direitos humanos com a fórmula de que elas também abrangem comunicação digital, o uso de infraestruturas digitais e big data, bem como análise de big data ou especialmente o uso de ferramentas de controle de comportamento digital.

Além disso, nenhuma ordem jurídica especial exige que as autorizações de restrição da liberdade contidas nas constituições nacionais respectivas e nas garantias europeias dos direitos fundamentais possam e devam ser utilizadas no domínio das comunicações digitais para proteger as pessoas afetadas ou, de um modo mais geral: para prevenir os riscos associados à transformação digital. No entanto, há que perguntar também se, e em que medida, os domínios da proteção das liberdades cívicas, bem como as reservas de restrições e a sua utilização, por exemplo nas leis, fazem justiça às novas possibilidades de digitalização ou exigem alterações.

Em princípio, é útil que as normas dos direitos fundamentais, mesmo que se refiram a uma longa tradição, sejam interpretadas dinamicamente ao longo do tempo com o objetivo de que suas premissas permaneçam significativas mesmo diante de realidades em mudança[41]. Para o efeito, examina-se em que medida as premissas empíricas e prescritivas em que se baseiam os direitos de liberdade continuam a ser relevantes face às mudanças - aqui no contexto técnico, social ou econômico - e em que medida as mudanças nas premissas podem ou devem levar a ajustamentos na proteção dos direitos fundamentais[42]. Mas não é de modo algum seguro, a capacidade do sistema jurídico para reagir de forma flexível aos novos fenômenos que se encontram em plena sintonia com as transformações fundamentais, tal como são atualmente provocadas pela revolução digital da sociedade. Se não for esse o caso, há necessidade de uma mudança no sistema jurídico.

8.2 Especialmente: Efeito horizontal da proteção da liberdade e do mandato para o delineamento das possibilidades de exercício da liberdade

Na era moderna, os direitos fundamentais foram concebidos principalmente como direitos de defesa dos titulares de direitos fundamentais contra a intervenção

[41] Cf., I. Eisenberger, Innovation im Recht, 2016.

[42] Para o significado das premissas empíricas e normativas e como lidar com as suas mudanças, ver, por exemplo W. Hoffmann-Riem, Innovation und Recht, Recht und Innovation: Recht im Ensemble seiner Kontexte, 2016, 108-130 e *passim*.

do Estado. Este sentido é, evidentemente, ainda importante para a comunicação digital e as suas consequências. Além disso, porém, coloca-se a questão de saber se os direitos fundamentais também são significativos e eficazes na relação entre os particulares.

A transformação digital com as suas vastas possibilidades - incluindo a monitorização e o controle do comportamento humano - está atualmente a ser realizada em aspetos essenciais por empresas privadas, que podem exercer uma influência considerável nos espaços de liberdade de outros indivíduos privados e nas atuais condições de utilização da liberdade, e que o fazem tendo em conta os seus próprios interesses (legitimamente unilaterais)[43]. Alguns atores (como os grandes intermediários de informação) têm (também) o poder de prejudicar os direitos fundamentais de outros, o que pode ser funcionalmente comparável ao poder das agências estatais.

A extensão da proteção dos direitos fundamentais às relações dos particulares entre si[44] e, por conseguinte, também a favor de terceiros, cuja liberdade pode ser restringida pelo uso privado do poder, é particularmente importante para a realização da liberdade, se a responsabilidade de assegurar o bem comum tiver sido largamente deixada ao mercado econômico e, por conseguinte, a empresas relativamente poderosas. É o caso, por exemplo, das infraestruturas de telecomunicações e dos serviços que prestam. Mas, para além destas condições-quadro concretas, é particularmente importante que a transformação digital abranja toda a sociedade, ou seja, também os domínios que, até agora, se mantiveram relativamente inalterados em termos regulamentares, pelo que poderá ser necessário conceber o espaço de liberdade em conformidade com a nova situação.

Do ponto de vista jurídico, a questão, que há muito é fundamental na ciência do direito alemã e que tem sido tratada de forma sustentada e aprofundada pela jurisprudência, torna-se significativa: em que medida os direitos de liberdade em questão contêm, além de seu conteúdo subjetivo-legal para a proteção dos indivíduos, mandatos objetivos-legais aos detentores de soberania* para assegurar

[43] Cf., W. Christl, Kommerzielle digitale Überwachung im Alltag, Studie im Auftrag der österreichischen Bundesarbeitskammer, 2014

[44] Em relação ao alcance da obrigação de direitos fundamentais, comparar a redação das decisões do Tribunal Constitucional Federal - ainda que em outros contextos: "Os particulares (podem), evidentemente, através dos efeitos indiretos de terceiros nos direitos fundamentais, estar também sujeitos a uma obrigação semelhante ou igual ao Estado, independentemente dos seus próprios direitos fundamentais, especialmente se de fato se converterem numa posição comparável de obrigação ou garantidor como o Estado tem tradicionalmente observado". BVerfGE 128, 226, 248. No mesmo sentido BverfG, in: Neue Juristische Wochenschrift 2015, 2485, 2486.

* No direito alemão: *Träger von Hoheitsgewalt*. Os detentores da soberania são, por exemplo, o Estado, o Land, o município, a associação de municípios, a universidade ou a instituição de seguridade social. Os seus direitos e obrigações no que diz respeito aos atos soberanos na sua totalidade

a proteção específica da liberdade não apenas no sentido da defesa contra a interferência do Estado, mas também no efeito horizontal das relações entre indivíduos privados ou em relação ao desenvolvimento e, quando apropriado, à formação da ordem social de realização da liberdade mesmo sob condições alteradas?[45]

O direito constitucional alemão reconhece há muitas décadas que as normas de direitos fundamentais, além de sua função de direitos de defesa contra o Estado, contêm mandatos objetivos e legalmente fundamentados ao Estado para a estruturação mais detalhada da possibilidade do uso da liberdade e para a proteção da liberdade também em relação a ameaças de pessoas físicas (o denominado efeito entre terceiros, ou eficácia horizontal dos direitos fundamentais)[46]. Estes mandatos são dirigidos a todos os detentores de soberania no âmbito das respectivas áreas de responsabilidade e também ao legislador, que pode e deve criar disposições no sistema jurídico para a proteção e eficácia dos direitos fundamentais também no efeito horizontal.

Conteúdos jurídicos objetivos dos direitos fundamentais e dos direitos humanos e abordagens para seu efeito horizontal podem ser encontrados não apenas nas normas alemãs de direitos fundamentais[47], mas também, cada vez mais, em sistemas jurídicos estrangeiros, no âmbito da Carta dos Direitos Fundamentais da UE e, em parte, no Tratado sobre o Funcionamento da União Europeia (TFUE), bem como na Convenção Europeia dos Direitos Humanos. No entanto, também são reconhecidos em acordos internacionais individuais[48].

Exemplos atuais (embora tematicamente limitados) de uma lei destinada a garantir a liberdade são o RGPD, que está em vigor na UE desde maio de 2018, e -

resultam num direito público que pode ser dividido principalmente em (as quatro partes) direito constitucional, direito administrativo, direito processual e direito penal (Nota dos tradutores).

[45] Cf., W. Hoffmann-Riem (nota de rodapé 42) 538-542, 679-683, com sugestões adicionais de literatura.

[46] A decisão do Tribunal Constitucional Federal é fundamental, BVerfGE 7, 198, 203 e ss. Sobrepondo o tema ao chamado efeito entre terceiros ou eficácia horizontal, entre muitos, cf., H.-J. Papier, Drittwirkung, in D. Merten/ H.-J. Papier (Ed.), Grundrechte in Deutschland: Allgemeine Lehren I, 2006, 1331-1362.

[47] Aqui só podemos referir-nos ao exemplo da Áustria, ver, por exemplo, W. Heißl, Grundrechtskollisionen am Beispiel von Persönlichkeitseingriffen sowie Überwachungen und Ermittlungen im Internet, 2017, 34-38 e *passim*.

[48] Cf., T. Marauhn, Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 2015, Bd. 74, 373-403; A. Fischer-Lescano, Der Kampf um die Internetverfassung: Rechtsfragen des Schutzes globaler Kommunikationsstrukturen vor Überwachungsmaßnahmen, in: JuristenZeitung 2014, 965-974; U. Schliesky/ C. Hoffmann/A. Luch/K. C. Borchers, Schutzpflichten und Drittwirkung im Internet: Das Grundgesetz im digitalen Zeitalter, 2014; N. Marsch, Das europäische Datenschutzgrundrecht. Grundlagen – Dimensionen – Verflechtungen, 2018.

especialmente na Alemanha - a Lei Federal de Proteção de Dados (*Bundesdatenschutzgesetz*), que foi revista em 2017 e entrará em vigor ao mesmo tempo que o RGPD - a seguir, simplesmente BDSG* (novo)[47]. Além disso (e até agora) a Diretiva Privacidade e Comunicações Eletrônicas[48] , que, no entanto, deverá ser substituída pelo Regulamento relativo à privacidade e às comunicações eletrônicas atualmente em curso no parlamento da UE, mas que provavelmente só entrará em vigor no início de 2019*. No entanto, este regulamento não abrangerá

* Cf., versão em inglês em: https://www.gesetze-im-internet.de/englisch_bdsg/index.html (link permanente) (Nota dos tradutores).

47 Para estas novas bases jurídicas, ver os elementos de prova na nota 7. O RGPD e a BDSG devem ser tratados no contexto. É provável que isto conduza a dificuldades práticas consideráveis na futura proteção de dados, nomeadamente devido à complexidade das construções e a muitos requisitos pormenorizados e em aberto, bem como a muitas cláusulas de abertura. Para este último, ver, por exemplo, A. Roßnagel, Gesetzgebung im Rahmen der Datenschutz-Grundverordnung, in: Datenschutz und Datensicherheit 2017, 277 et seq.

48 Richtlinie 2009/136/EG (Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009 , que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n. o 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor – nota dos tradutores).

* Até a data de tradução deste texto (05/10/2019) ainda não foi completado o procedimento para votação e entrada em vigor da Proposta de Regulamento relativo à privacidade e às comunicações eletrônicas, a que se refere o autor: Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrônicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrônicas), cf., versão em português, em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42693 (link permanente). De todo modo, a proposta de Regulamento "ePrivacidade" aplica-se em substituição Diretiva "ePrivacidade" (2009) e em paralelo com o Regulamento Geral de Proteção de Dados (RGPD). Os preceitos da Comunidade Europeia não têm o carácter de lei imediatamente efetiva e vinculativa, mas são diretivas que devem ser aplicadas às leis nacionais, para que cada um dos países disponha de um período mais longo. O caso dos regulamentos é diferente, porque estes, tal como o RGPD, constituem uma lei aplicável a toda a UE, vinculativa, portanto, para todos os Estados-Membros. A intenção é que a "ePrivacidade" concretize o que está estipulado na RGPD. Este novo sistema, também conhecido como "ePV", constitui uma *lex specialis*, o que significa que tem prioridade sobre o RGPD, concebido como uma *lex generalis*. O RGPD é um documento mais geral que se torna mais inteligível em algumas partes com as regras de "ePrivacidade". Os Regulamentos Gerais de Proteção de Dados, no entanto, não foram concebidos exclusivamente para a Internet e, neste sentido, a Privacidade Eletrônica oferece uma proteção mais notável. A aplicação destes dois Regulamentos não significa que outros regulamentos sejam esquecidos. Isto já foi decidido no RGPD, e o ePV deve também incluir cláusulas de abertura: as regras locais também influenciam alguns pontos do regulamento no que se refere aos pormenores da sua aplicação. A modificação

todos os domínios da proteção de dados. Trata-se de um regime especial relativo às atividades dos prestadores de serviços de comunicações eletrônicas e, por conseguinte, diz respeito a comunicações como chamadas telefônicas, acesso à Internet, serviços de mensagens instantâneas, correio eletrônico, telefonia na Internet ou mensagens pessoais. Tal como as outras regras em matéria de proteção de dados, também se centra na proteção dos dados pessoais, pelo que é limitada.

As particularidades do Big Data e das aplicações que as moldam são refletidas apenas parcialmente nos padrões que foram emitidos até o momento[49]. As características especiais do Big Data e das suas aplicações só são tidas em conta de forma limitada nas normas emitidas até à data. Continua a ser uma tarefa a ser dominada a adaptação dos direitos de liberdade (não apenas os direitos de proteção de dados) às novas potencialidades - ou seja, também às possibilidades inovadoras - da digitalização e, em particular, da utilização de megadados, tendo simultaneamente em conta, também, os possíveis riscos para os bens e interesses jurídicos. Isto pode ser feito, em parte, pela interpretação de normas já editadas (como o RGPD) ou - se não for suficiente - pela alteração de normas antigas ou pela criação de novas normas (ver sugestões nas notas 10, 11).

Tendo em conta a importância da digitalização em quase todas as áreas da sociedade, a utilização de algoritmos em diferentes domínios coloca muitas questões desiguais, ou seja, não se limita apenas aos Big Data. Estas incluem questões sobre a necessidade de novos regulamentos jurídicos. Eles são apenas mencionados aqui, mas não aprofundados. São afetados o princípio da neutralidade da rede[50], o direito de anonimizar a comunicação pessoal[51] e a proteção contra a desanonimização, a redefinição da relação entre as esferas privada e pública, mas também várias aplicações nas diversas áreas sociais. Particularmente importante na transformação digital é a garantia da autonomia individual e coletiva[52].

ou adaptação de pontos que contradizem as leis europeias é da responsabilidade dos legisladores nacionais. (Nota dos tradutores)

[49] Cf., G. Hornung/C. Herfurth, Datenschutz bei Big Data. Rechtliche und politische Implikationen, in: C. König/ J. Schröder/E. Wiegand (Ed.), Big Data – Chancen, Risiken, Entwicklungstendenzen, 2017, S. 149-184; sowie G. Hornung, Erosion traditioneller Prinzipien des Datenschutzrechts durch Big Data, in: W. Hoffmann-Riem (nota de rodapé 27), 81-98.

[50] Cf., C. Werkmeister/Y. Hermstrüwer, Ausnahmen vom Grundsatz der Netzneutralität – Wer darf auf die Überholspur im Internet? Warum das europäische Recht der Netzneutralität noch keine Rechtssicherheit schafft, in: Computer und Recht 2015, 570-576 (com dicas interessantes). A Comissão Federal dos EUA abandonou esse princípio em dezembro de 2017, cf., G. Dietz, Ende der Netzneutralität. Die Abschaffung der Demokratie, in: SPIEGEL ONLINE vom 7.12.2017.

[51] Para o problema de criptografia, cf., R. Petrlic/K. Manny, Wie sicher ist der Zugriff auf Websites im Internet? in: Datenschutz und Datensicheheit 2017, 88-92.

[52] Para o significado de autonomia em geral, consulte C. Bumke/A. Röthel (Ed.), Autonomie im Recht, 2016. Siehe dort etwa M. Eifert, Autonomie und Sozialität: Schwierigkeiten rechtlicher

8.3 Especialmente: Inovações em matéria de direitos fundamentais para a proteção dos bens jurídicos

Existem formas de proteger os bens jurídicos individuais e coletivos na interpretação e aplicação das normas constitucionais, em particular as normas de direitos fundamentais. Isto significa que as mudanças sociais e as ameaças à liberdade podem ser enfrentadas de forma inovadora. Isso pode ser observado de forma particularmente intensa na jurisprudência do Tribunal Constitucional Federal (BVerfG*). Assim esse Tribunal, ao reconhecer o conteúdo objetivo dos direitos fundamentais ampliou o seu âmbito da proteção[53]. Por conseguinte, para a maioria dos direitos fundamentais na Alemanha também se aplica o efeito horizontal entre atores não estatais, mas, em princípio, apenas na medida em que tal seja expressamente referido e especificado em maior pormenor pelas leis vigentes ou pela interpretação das leis existentes.

O Tribunal Constitucional Federal também tem sido inovador na sua interpretação e aplicação dos direitos fundamentais individuais[54]. Assim, interpretou a garantia da liberdade geral de ação (artigo 2.º, n.º 1, da Lei Fundamental) não só no sentido da garantia do livre desenvolvimento da personalidade, mas também como um direito fundamental independente que preenche as lacunas remanescentes: deve ter-se sempre em conta quando uma determinada esfera da vida não é abrangida por um dos direitos fundamentais particularmente garantidos[55]. No contexto atual, o reconhecimento do "direito geral de personalidade" com base numa síntese da proteção do livre desenvolvimento da personalidade (artigo 2.1 da Lei Fundamental) com a proteção da dignidade humana (artigo 1.1 da Lei Fundamental) é particularmente importante[56]. Esta construção foi posteriormente utilizada, também, como base do "direito fundamental à autodeterminação informativa"[57]. Em particular, esse direito fundamental abrange o poder do indivíduo de determinar, em princípio, a divulgação e o uso de seus dados pessoais[58]. Esta proteção dos direitos fundamentais tornou-se a base para o desenvolvimento mais próximo da legislação moderna de proteção de dados na Alemanha, especialmente em resposta a novos

Konzeptionalisierung ihres Wechselspiels am Beispiel der informationellen Selbstbestimmung, 365-384

* No original, acrônimo utilizado pelo autor (Nota dos tradutores).

53 Ver nota 44.

54 Para inovações em direitos fundamentais, consulte G. Hornung, Grundrechtsinnovationen, 2015; W. Hoffmann-Riem (nota de rodapé 42), §§ 34, 35.

55 Cf., BVerfGE 6, 32, 37.

56 Cf., BVerfGE 34, 238, 245 e ss.

57 Cf., BVerfGE 65, 1.

58 Cf., BVerfGE 65, 1, 41 e ss.

desenvolvimentos tecnológicos[59]. Ao mesmo tempo, também influenciou a evolução de outros sistemas jurídicos, incluindo o direito da UE e as disposições da Carta dos Direitos Fundamentais da UE (em especial o seu artigo 8.).

No entanto, uma vez que este direito fundamental ainda apresentava lacunas na proteção, o Tribunal Constitucional Federal decidiu em 2008 por ocasião da revisão de uma lei para permitir buscas estatais online ou obter vigilância de telecomunicações - combinada com a possibilidade de transferência de vírus (Malware) em computador com o propósito de sua espionagem e possivelmente manipulação - formulou uma nova concretização constitucional. Descreveu isto como um "direito fundamental de garantir a confidencialidade e integridade dos sistemas de tecnologia da informação"[60]. Frequentemente abreviado como IT-Grundrecht[*] (às vezes também, mas na minha opinião de modo restrito, de Lei Fundamental do Computador).

O tribunal havia assumido que as premissas empíricas da tradicional proteção dos direitos fundamentais haviam sido alteradas pelas novas tecnologias e que o direito fundamental à autodeterminação informacional, voltado principalmente para a proteção contra invasões de bens individuais de proteção individual, não era mais suficiente. Na opinião do BVerfG, ao utilizar novos sistemas de tecnologia da informação que estão se tornando mais complexos e ampliando as possibilidades de análise, a proteção da liberdade também deve ser efetiva no nível do sistema e, em particular, estendida para garantir a integridade e a confidencialidade dos próprios sistemas de tecnologia da informação, independentemente de intervenções individuais concretas na comunicação.

Deste modo, a funcionalidade técnica e social dos sistemas de tecnologia da informação deve ser assegurada como requisito prévio para a sua utilização autônoma para diferentes fins. Em 2016, em decisão sobre a constitucionalidade da Lei relativa ao Serviço Federal de Polícia Criminal e à cooperação do Governo

[59] Sobre a interação entre as mudanças tecnológicas e as reações aos direitos fundamentais, ver W. Hoffmann-Riem (Cit. Nota de rodapé 42), § 35.

[60] BVerfGE 120, 274, 313; 141, 220, 264 f.; 220 e ss., 268 e ss., 303 e ss. A partir da rica literatura sobre este direito fundamental, cf., M. Hauser, Das IT- Grundrecht. Schnittfelder und Auswirkung, 2015; J.-C. Wehage, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das bürgerliche Recht, 2013.

[*] Integralmente: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Direito fundamental sobre a garantia da confidencialidade e integridade dos sistemas de tecnologia da informação. Trad. Livre). Também abreviado IT-Grundrecht, direito fundamental de computador ou direito fundamental à privacidade digital, válido como direito fundamental da República Federal da Alemanha, servindo principalmente para proteger dados pessoais que são armazenados ou processados em sistemas de tecnologia da informação. Cf., Urteil des Bundesverfassungsgericht: L e i t s ä t z e zum Urteil des Ersten Senats vom 27. Februar 2008 (- 1 BvR 370/07 -) (- 1 BvR 595/07 -), in: https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html - link permanente (Nota dos tradutores).

Federal e dos Estados em matéria de polícia criminal (Bundeskriminalamtgesetz - BKAG[*61]), o tribunal afirmou ainda que os sistemas de tecnologia da informação protegidos incluem não apenas os computadores utilizados pelas próprias pessoas envolvidas, mas também os sistemas de tecnologia da informação que funcionam em rede com outros computadores, por exemplo, ao utilizar as chamadas "nuvens"[62]. Ao fazê-lo, enfatizou explicitamente que os dados que são terceirizados para servidores externos em uma confiança legítima de confidencialidade são cobertos pela proteção.

Essas garantias de direitos fundamentais acima mencionadas não são consideradas como "novos" direitos fundamentais, idealizados, por assim dizer, livremente pelo Tribunal, mas como concretizações e, ao mesmo tempo, novos desenvolvimentos de uma garantia de liberdade que, em princípio, já está contida nos artigos 1º e 2º da Lei Fundamental, preservando o sentido da proteção tradicional dos direitos fundamentais, também à luz das novas possibilidades tecnológicas. Tal como estas normas de direito fundamental, o direito fundamental delas derivado de garantir a confidencialidade e a integridade dos sistemas de tecnologia da informação contém dimensões de proteção jurídica subjetiva e objetiva[63].

Embora o conteúdo básico de garantia legal foi confirmada pelo Tribunal Constitucional Federal, na sequência de uma decisão de reclamações constitucionais, que foram dirigidas à proteção dos dados pessoais, tem a garantia de direito fundamental reflexivamente também afetar a proteção de informações não pessoais: é o sistema de tecnologia da informação a partir de um suporte legal contra intervenções como a instalação de malware ou outras formas de manipulação de software, como reflexo, também limita a possibilidade de acessar os dados não pessoais disponíveis no sistema[64].

O Tribunal de Justiça Europeu (TJE)[*] também utilizou uma construção inovadora - alargando a proteção da liberdade - para fundamentar uma nova concretização dos direitos fundamentais na sua decisão Google, que foi emitida em

[*] Cf., Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG), que pode ser acessada em: https://www.gesetze-im-internet.de/bkag_2018/BJNR135410017.html, link permanente (Nota dos tradutores).

[61] BVerfGE 141, 220, 303 e ss.

[62] BVerfGE 141, 220, 304.

[63] Cf., W. Hoffmann-Riem (nota de rodapé 42), 575-576.

[64] Além disso, deve salientar-se que o conceito de dados pessoais no domínio dos grandes volumes de dados deve ser alargado de qualquer modo (ver 11.1 *infra*) - com a consequência de que o âmbito da proteção do *IT-Grundrechts* (veja nota * do tradutor logo abaixo da nota 60 supra) deve também ser entendido em sentido lato.

[*] Cf., Court of Justice of the European Union (CJEU), in: https://curia.europa.eu/jcms/jcms/j_6/en/ (link permanente) (nota dos tradutores).

resposta a uma decisão da autoridade espanhola de proteção de dados *(Agencia Española de Protección de Datos*) e aí tratada como uma expressão do artigo 8º da Carta dos Direitos Fundamentais da UE (desde então frequentemente referida como "direito fundamental ao esquecimento")[65]. O Art. 8º refere-se à proteção dos dados de carácter pessoal.

Também podemos, noutros contextos, colocar a questão de saber se, tendo em conta as alterações técnicas, sociais ou econômicas, a proteção da liberdade só pode ser assegurada através de instrumentos jurídicos convencionais ou se são necessárias novas medidas de proteção. O que é particularmente necessário é uma proteção das liberdades coletivas que vá além da proteção tradicional dos direitos fundamentais e da proteção dos titulares de direitos fundamentais, nomeadamente a proteção da autonomia, que inclui o tratamento das assimetrias de poder. Na medida em que tal proteção não pode ser derivada unicamente dos direitos fundamentais, os objetivos do Estado são acrescentados como orientações normativas, em particular os princípios da democracia, do Estado de Direito e do Estado de Bem-Estar Social (artigo 20 da Lei Fundamental). Estes, por sua vez, incluem mandatos para garantir o funcionamento da ordem constitucional, no interesse da proteção dos ativos jurídicos coletivos e individuais.

Continuará a haver no futuro a necessidade de decisões inovadoras como as mencionadas pelo BVerfG. Haverá sempre ocasiões para perguntar se, e em que medida, as mudanças técnicas e sociais podem conduzir, por um lado, a novas oportunidades de utilização dignas de promoção, mas também a novos riscos que não podem ser geridos, ou já não podem ser adequadamente geridos, com os instrumentos jurídicos convencionais de proteção da liberdade, mesmo com uma interpretação dinâmica.

Os candidatos a tais considerações são atualmente, por exemplo, procedimentos automatizados[66] para intervenções em interesses jurídicos ou, de um modo mais geral, para decisões juridicamente vinculativas (para um exemplo ainda que insatisfatório) de definição de perfis, ver artigo 22º do RGPD). Os regulamentos relativos aos procedimentos administrativos automatizados também foram incorporados no direito processual administrativo alemão, no direito fiscal e no

[65] Cf., EuGH. Urteil vom 13.05.2014, Rs. C-131/12, in: Europäische GRUNDRECHTE-Zeitschrift (EuGRZ) 2014, 320 e ss. Cf., agora o também Art. 17 RGPD.

[66] Cf., M. Martini/D. Nink, Wenn Maschinen entscheiden … Persönlichkeitsschutz in vollautomatisierten Verwaltungsverfahren, in: Neue Zeitschrift für Verwaltungsrecht 2017, 10, 681-682. Cf. também C. Ernst, Algorithmische Entscheidungsfindung und personenbezogene Daten, in: JuristenZeitung 2017, 21, 1026-1036; N. Braun Binder (nota de rodapé 11); W. Hoffmann-Riem, Die digitale Transformation als Herausforderung für die Legitimation rechtlicher Entscheidungen, in: A.Ungern-Sternberg/S. Unger, Demokratie und künstliche Intelligenz, 2019, p. 129-159.

direito social para além do domínio da proteção de dados[67], mas não parecem, de modo algum, ser a última palavra.

Especialmente na literatura de língua inglesa, há intensas discussões sobre "tomada de decisão algorítmica" ou "regulação algorítmica"[68], mas também sobre uma "ameaça de algocracia"[69]. Além disso, existem muitos campos com problemas não resolvidos, tais como o uso de robótica, o uso controlado remotamente de telediagnósticos e teleterapia, mas também o controle automatizado ou mesmo autônomo de veículos motorizados. Devem também ser mencionadas as muitas possibilidades de fundir os mundos físico e virtual ("onlife") e de (frequentemente) controlar inconscientemente o comportamento das pessoas afetadas[70]. É de esperar que haja aqui regulamentação jurídica adequada. Não se pode excluir que os tribunais também tenham de participar em soluções inovadoras.

9. As dificuldades em conceber uma proteção jurídica eficaz

O direito é, naturalmente, apenas um dos vários meios possíveis de influenciar o desenvolvimento. Mas mesmo em tempos de digitalização, a eficácia do direito não pode ser dispensada. Os novos desafios surgem devido às características especiais da tecnologia e à sua utilização em diferentes domínios de atividade e na sua utilização para fins específicos, bem como no âmbito de modelos de negócio específicos. As razões para as dificuldades de uma regulamentação bem-sucedida e, por conseguinte, as razões para os desafios especiais serão discutidas a seguir, embora apenas a título de exemplo. Os problemas aqui abordados também dizem respeito ao tratamento de grandes volumes de dados, mas não se limitam de todo a isso.

9.1 Convergências e delimitações

As tecnologias digitais e as infraestruturas disponíveis para a sua utilização, bem como os serviços que prestam, são por vezes utilizadas de forma espacialmente limitada (por exemplo, regional ou nacional), mas, em muitos casos, também de forma transnacional e globalmente em rede[71]. O mesmo se aplica a muitos dos serviços prestados por tecnologias digitalizadas.

---

[67] Em particular deve ser feita menção aos §§ 3a, 24 Secção. 1, 35a, 37 Secção. 2-4 e § 41 Secção 2 Def. 2 IIa Verwaltungsverfahrensgesetz. Além disso em especial § 155 Secção 6 do Abgabenordnung e § 31a do Sozialgesetzbuches X para referir. Decisões automatizadas também são abordadas no RGPD (Art. 22). [Atente-se que o livro X do Socialgesetzbuch (SGB X) trata da Administração Social e Proteção de Dados Sociais, notadamente com a redação de 15 de agosto de 2019 (Nota dos tradutores)].

[68] Cf., as indicações na nota de rodapé n. 11.

[69] Cf., J. Danaher (nota de rodapé 34).

[70] Para o mundo "onlife" confira a nota de rodapé 31 supra.

[71] Para as manifestações de desterritorialização e possível reterritorialização e os problemas que lhe são associados (nomeadamente em matéria de direito público), ver M. Cornils,

Para além destas (e outras) delimitações, há que ter em conta uma variedade de convergências[72], o que também dificulta encontrar o ponto de partida certo para as intervenções regulamentares. No setor de TI, por exemplo, as fronteiras entre hardware, software e orgware[*], entre fornecedores e consumidores e entre serviços e seu transporte usando infraestruturas de TI tornam-se difusas. A comunicação privada e pública estão cada vez mais interligadas. As ideias convencionais sobre privacidade e publicidade estão diminuindo, e a necessidade de uma proteção específica da privacidade é até parcialmente colocada em causa pelos partidários do denominado movimento pós-privacidade[73].

Acima de tudo, os fenômenos de delimitação podem levar a margens abertas consideráveis na proteção jurídica, na medida em que - como é habitual - o direito está vinculado à definição de fronteiras, por exemplo a nível regional (seja a nível nacional ou da UE), e na medida em que seja também objetivamente limitado. Em princípio, o direito transnacional ou globalmente aplicável, como o direito internacional, também está disponível. O seu âmbito territorial pode ser amplo. No entanto, o direito internacional só é relevante para setores individuais - como o direito comercial mundial e questões individuais do direito autoral - e muitas vezes é limitado[74] em sua natureza vinculante e sancionabilidade.

Entterritorialisierung im Kommunikationsrecht, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer 2017, Vol. 76, 391-442; no que respeita às conclusões das delimitações, ver também - neste contexto, entre outros - T. Vesting, Digitale Entgrenzung, in B. Lomfeld (Ed.), Die Fälle der Gesellschaft. Eine neue Praxis soziologischer Jurisprudenz, 2017.

[72] Sobre esses, em vez de outros (utilizando o exemplo da Internet), ver J.-U. Pille (nota de rodapé 37), 55-58.

[*] Orgware delineia categorias fundamentais para projetos de TI que não concernem ao campo do hardware ou do software, mas são indispensáveis para alcançar os objetivos do projeto. Este "espaço de organização" inclui, entre outros, guias do usuário, críticas de concepções e projetos de TI, bem como requisitos de segurança. Em algumas situações muito específicas, os métodos na gestão de projetos na área de TI podem ser denominados de orgware (Nota dos tradutores).

[73] C. Heller, Post-privacy: Prima leben ohne Privatsphäre, 2011. Crítico em relação a tal posição, P. Schaar, Das Ende der Privatsphäre, 2007. De modo diverso, M. Klar, Privatsphäre und Datenschutz in Zeiten technischen und legislativen Umbruchs, in: Die öffentliche Verwaltung 2013, 103-113; V. Boehme-Neßler, Zwei Welten? Big Data und Datenschutz. Entwicklungslinien des Datenschutzes in der digitalen Gesellschaft, in: Archiv für Urheber- und Medienrecht 2015, 19, 24-27.A respeito do problema v. também as contribuições em H.Hill/U. Schliesky (Ed.), Die Neubestimmung der Privatheit, 2014.

[74] Os efeitos no campo da sociedade e, portanto, também os impactos nas estruturas sociais não podem ser descritos mais detalhadamente aqui, comparar W. Christl (nota de rodapé 43). Veja também do ponto de vista da ciência política I. Schneider, Bringing the state back in. Big Data-based capitalism, disruption and novel regulatory approaches in Europe, in. R. Saetnan/I. Schneider/N. Green (eds.), The Politics of Big Data – Big Data, Big Brother? 2018, 129-175. Deve também ser feita referência às outras contribuições neste volume.

O direito internacional não cobriu todos os desafios relevantes neste domínio e, especialmente no domínio da regulamentação aqui abordado, e é presentemente relativamente pouco funcional. Os pontos de contatos territoriais, incluindo nacionais, para a regulamentação jurídica estão frequentemente presentes, mas nem sempre, em relação às atividades transnacionais ou globais das empresas de TI. É de saudar - mas de modo algum suficiente - que o artigo 3º do RGPD alargue o âmbito de aplicação territorial da legislação europeia em matéria de proteção de dados e, ao fazê-lo, em especial no inciso 1, o ligue na medida em que o tratamento de dados pessoais "ocorra no âmbito das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante na União, independentemente de o tratamento ter lugar na União"[75]. Este princípio – o assim chamado princípio do local do comércio/mercado - não deve limitar-se à legislação em matéria de proteção de dados, mas deve também ser alargado a outros riscos para os interesses jurídicos associados à digitalização, incluindo a lesão de interesses jurídicos coletivos[76].

No entanto, a regulamentação estatal no domínio da digitalização encontra geralmente uma resistência considerável por parte das empresas de TI, que tentam impedir ou desativar, tanto quanto possível, a regulamentação. Eles também têm a oportunidade de contornar as regras que foram criadas, por exemplo, escolhendo a sede da empresa ou dividindo-a, deslocando o foco de suas atividades para outras partes de um grupo corporativo, tornando suas práticas de negócios não transparentes ou tornando o design de tecnologia difícil de ser visto por terceiros. Esta última também não é regularmente sujeita a controle público e, portanto, não está sujeita a qualquer rastreabilidade concreta.

9.2 Concentração de poder

As possibilidades transfronteiriças de transformação digital facilitaram a criação de posições de poder globais e a sua concentração em poucos grupos. Isto aplica-se em particular aos chamados "Cinco Grandes"* (Facebook, Google,

[75] Para obter mais informações M. Klar, Kommentierung zu Art. 3, in: J. Kühling/B. Buchner (Ed.), Datenschutz-Grundverordnung: Kommentar, 2ª ed., 2018; G. Hordnung, Kommentierung zu Art. 3, in: S. Simitis/G. Hornung/I. Spiecker genannt Döhmann (Ed.), Datenschutzrecht, 2019. Uma limitada ampliação do âmbito territorial de aplicação do direito de proteção de dados europeu, já havia sido reconhecida pelo Tribunal de Justiça da União Europeia na decisão Google (nota de rodapé 67).

[76] Os efeitos no campo da sociedade e, portanto, também a influência sobre as estruturas sociais, não podem ser descritos aqui, para mais detalhes, cf., W. Christl (nota de rodapé 43). Veja também na ciência política I. Schneider, Bringing the state back in. Big Data-based capitalism, disruption and novel regulatory approaches in Europe, in. R. Saetnan/I. Schneider/N. Green (eds.) (nota de rodapé 131-177. Nesse volume deve também ser feita referência às outras contribuições.

* No original o autor expressou em inglês: "Big Five" (nota dos tradutores).

Microsoft, Amazon, Apple)[77]. Eles conseguiram formar oligopólios globais em sub-mercados-chave e ocupar segmentos de mercado adicionais - inclusive os de comunicação entre mídias[*].

Explicações para o sucesso das ações para alcançar a superioridade no poder de mercado podem ser encontradas na economia de rede e Internet, entre outras[78]. A este respeito, deve ser feita referência às características especiais dos bens de informação - tais como a "não rivalidade no consumo" de dados - bem como aos respectivos efeitos diretos e indiretos sobre as redes. A natureza multilateral dos mercados é igualmente importante. Trata-se da possibilidade de relacionar de forma inteligente a atuação de diferentes atores em diferentes campos de trabalho. Tendo em conta as elevadas margens de lucro - também aumentadas por medidas de evasão fiscal - as empresas poderosas têm também boas oportunidades de penetrar em segmentos de mercado vizinhos ou dos mais distantes, de adquirir empresas bem sucedidas e especialmente inovadoras, de utilizar o seu know-how e patentes e, desta e de outras formas, de reforçar as suas respectivas posições no mercado[79]. Por conseguinte, tais efeitos conglomerais podem ser utilizados para encerrar os mercados, ou seja, para impedir a concorrência. Outras características especiais dos dados acima mencionadas (4) reforçam igualmente a possibilidade de acumulação de poder de mercado, como a ubiquidade da disponibilidade de dados e as múltiplas possibilidades de aperfeiçoamento dos produtos. Na medida em que estes e outros fatores aumentam os processos de concentração e evitam possibilidades de intervenção contrária, a economia de mercado falha como meio de limitar o poder.

A legislação antitruste, que é normalmente usada como um direito de limitar o poder, está disponível apenas até certo ponto no setor de TI para contramedidas. Não existe legislação antitrust global e eficaz e a legislação antitrust nacional e comunitária só se revelou eficaz de forma limitada no setor das TI devido às suas características especiais. É verdade que a UE e algumas autoridades nacionais de proteção de dados instauraram processos antitrust contra empresas individuais - por exemplo, a Google - e - na medida em que não foram encontradas soluções

[77] No entanto, existem outros atores poderosos, como o Grupo Chinês Alibaba, que vem se especializando, há alguns anos, em comércio eletrônico.

[*] No original, o autor utilizou a expressão em inglês "crossmidia". Midia cruzada, ou crossmedia é um termo que vem da comunicação de marketing e trata da expressão de uma mídia feita através de diferentes mídias. Um bom exemplo é um programa de televisão que se refere a um site em que o usuário pode responder ao programa. Esta referência usa várias mídias para experimentar todo o conceito. Portanto, esse conceito circular entre mídias (nota dos tradutores).

[78] Cf., entre outros, R. Peters, Internet-Ökonomie, 2010; R. Clement/D. Schreiber, Internet-Ökonomie: Grundlagen und Fallbeispiele der vernetzten Wirtschaft, 2016.

[79] Expressivo sobre o tema, A. Rolf/A. Sagawe, Des Googles Kern und andere Spinnennetze. Die Architektur der digitalen Gesellschaft, 2015.

amigáveis - aplicaram sanções pecuniárias[80]. No entanto, muitas aquisições ou fusões com empresas em fase de arranque ou empresas inovadoras de média dimensão pelas "Cinco Grandes" continuam fora do âmbito da legislação antitrust, por exemplo, se - como é normalmente o caso das aquisições habituais - os critérios para o controle das concentrações não forem preenchidos[81].

No entanto, mesmo quando a lei antitruste é aplicável, sua preocupação básica no setor de TI é que ela só pode ser usada de forma limitada para fins de regulação, incluindo a limitação de poder[82]. É um direito de salvaguardar o funcionamento dos mercados e de impedir o abuso de poder econômico. Utiliza as precauções previstas no direito concorrencial e, por conseguinte, constitui um meio de limitar a utilização abusiva do poder econômico. Mas não é um direito específico de limitar outro poder (por exemplo, político, cultural, social etc.). A realização de objetivos de bem-estar público como a proteção da autonomia (por exemplo, a liberdade de manipulação), o acesso equitativo, a prevenção da discriminação ou a formação da opinião pública orientada para a representação e a promoção da pluralidade social não são objetivos específicos do direito antitrust. A realização destes objetivos também não é automaticamente assegurada por precauções antitrust. No entanto, um mercado em funcionamento pode contribuir para a sua realização - mas apenas no quadro da sua eficiência, que é limitada de acordo com as condições da transformação digital global. O êxito da regulamentação neste domínio exige novos conceitos e instrumentos para a contenção do poder, e não apenas do poder de mercado econômico, e para a criação de melhores possibilidades para a implementação dos objetivos de bem-estar público.

Para realizar esta tarefa, os instrumentos do direito da concorrência devem interagir com os de outro direito regulamentar, que permite ou, pelo menos, pode permitir a proteção de interesses jurídicos em outras dimensões (ver também 12 infra). A utilização das tecnologias digitais deve, pois, ter em conta a

[80] Notas sobre o processo contra a Google em J.-P. Schneider, Innovationsoffene Regulierung datenbasierter Dienste in der Informationsgesellschaft. Datenschutz, Regulierung, Wettbewerb, in: E. Körber/J. Kühling (Ed.), Regulierung – Wettbewerb – Innovation, 2017, 156-159. No entanto, a lei antitruste só pode ser usada em determinadas situações.

[81] No entanto, a 9ª alteração da Lei Contra as Restrições de Concorrência (Gesetz gegen Wettbewerbsbeschränkungen - GWB) melhorou a proteção contra o abuso de poder de mercado na Alemanha, tendo em vista as consequências da digitalização e do controle reforçado das concentrações. Assim, o § 18, n. ° 2, a, 3, da GWB, com a redação que lhe foi dada em 1º de junho de 2016, prevê que a assunção de um mercado não exclui a prestação de um serviço sem encargos. Além disso, serão alargados os critérios aplicáveis aos mercados e redes multifacetados para a avaliação da posição do mercado. No entanto, estes são apenas os primeiros passos de um mais aperfeiçoado controle antitruste. (Uma versão em inglês da GWB em: http://www.gesetze-im-internet.de/englisch_gwb/index.html – nota dos tradutores)

[82] Sobre as possibilidades (limitadas) para o efeito, cf., T. Höppner, Medienkartellrecht – die aktuelle Fallpraxis. Kommunikation & Recht, 2016, 59-62.

multipolaridade e multidimensionalidade específicas dos objetivos e instrumentos consagrados no sistema jurídico[83].

9.3 Coleta e utilização de dados

A legislação em matéria de proteção de dados continuará, contudo, a ser de particular importância enquanto parte integrante do direito à proteção de dados pessoais e, por conseguinte, enquanto parte da proteção jurídica da autonomia. Alguns dos seus problemas e a necessidade de reavaliar o seu âmbito de aplicação serão discutidos a seguir (para o conceito de dados pessoais, ver supra 3).

As possibilidades de coleta de dados e processamento subsequente pelas empresas são muitas. Um exemplo disso é o método de rastreamento on-line, que é importante para a coleta de Big Data. Refere-se à observação eletrônica (registro e avaliação) do comportamento digital de uma pessoa. As fontes para rastreamento são conteúdos de comunicações, mas também metadados (como o Hypertext Transfer Protocol [HTTP], endereços IP). O rastreamento[84] é usado em particular como uma preparação para a criação de perfil[85], mas também para direcionamento. O termo direcionamento refere-se a uma forma de se dirigir para grupos-alvo, tal como uma mensagem publicitária "personalizada", em especial para os efeitos de controle da informação[86]. Isso pode ser feito pela própria empresa que coleta os dados ou por outra empresa que tenha adquirido os dados para seu próprio uso[87].

[83] Cf., J.-P. Schneider (nota de pé-de-página 80), 113-141. Schneider reivindica nomeadamente por uma lei multifinal e multidimensional relativa ao tráfego de dados. Ao fazê-lo, há que ultrapassar uma limitação da ênfase na proteção de dados e ter em conta outros objetivos regulamentares. A abordagem parece-me correta, mas, na minha opinião, o termo "lei de tráfego de dados" é demasiado restrito. Ver também 12 abaixo.

[84] O artigo 8º do Projeto de Regulamento relativo à Privacidade e Comunicações Eletrônicas prevê que o rastreio através de cookies deve ser limitado pelo fato de que uma proibição com reserva de permissão também se aplica a este respeito e que o consentimento deverá ser previsto por meio de uma opção de adesão (opt-in). Isto também corresponde à posição assumida pelos comissários alemães para a proteção de dados, que é considerada decisiva pela RGPD (sujeita a outra disposição do Regulamento de Privacidade e Comunicações Eletrônicas ainda a ser promulgado), ver a declaração de posição de 26 de abril de 2018.

[85] Uma definição de Perfil pode ser lida no artigo 4 (4) do RGPD. Lê-se: «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

[86] Cf., A. Klever, Behavioural Targeting. An Online Analysis for Efficient Media Planning? 2009.

[87] Uma lista de dados que o Facebook recolhe para fins publicitários direcionados foi compilada por V. Tischbein, netzpolitik org, zuletzt aktualisiert 18.3.2017, https://netzpolitik.org/2016/98-daten-die-facebook-ueber-dich-weiss-und-nutzt-um-werbung-auf-dich-zuzuschneiden/. Esta lista é mostrada abaixo (12).

Como resultado da avaliação dos dados, podem também ser abertas possibilidades de uma filtragem das informações adicionais prestadas pelos usuários e, assim, também possibilidades de influência indireta nas suas experiências pessoais, atitudes e padrões de comportamento.

Os dados coletados dessa forma são frequentemente combinados (agregados) com outros conjuntos de dados e também são utilizados para fins de análise e aplicação de Big Data em outros setores do sistema. Os dados também são frequentemente transmitidos a outras empresas - incluindo agentes de dados especiais, que podem comercializá-los juntamente com outros elementos -, possivelmente também para agências governamentais, em parte devido a obrigações legais.

Tendo em conta as múltiplas possibilidades de coleta e tratamento de dados, a proteção de dados continua a desempenhar um papel importante como direito à proteção de dados pessoais e, por conseguinte, como parte da proteção jurídica da autonomia.

9.3.1 Requisitos gerais para a licitude da coleta e tratamento de dados

A legislação em matéria de proteção de dados constitui uma abordagem tradicional da proteção - embora mais estreito no conteúdo - dos interesses jurídicos e, por conseguinte, também da limitação do uso do poder. O objeto é o "tratamento" (art. 4.º, n.º 2, RGPD) de dados pessoais, ou seja, em particular, a coleta, armazenamento e outros usos. A este respeito, aplica-se, em princípio, uma proibição com reserva de autorização. A proibição é quebrada se uma disposição legal permitir essas atividades ou se o titular dos dados tiver consentido. Constitui mais uma porta de acesso à licitude do tratamento se tal for necessário para a execução de um contrato no qual a pessoa em causa é parte, ou para a execução de medidas pré-contratuais tomadas a pedido da pessoa em causa (artigo 6.º, n.º 1-B do RGPD). No caso da Alemanha, o tratamento de dados pessoais, nomeadamente por uma autoridade pública, está sujeito à condição de ser necessário para o desempenho da tarefa pela qual a pessoa competente é responsável ou no exercício da autoridade pública atribuída à pessoa responsável (§ 3 BDSG (novo)[*]). Dentro de certos limites, o consentimento é também utilizado para a coleta de dados pelas autoridades públicas[88].

[*] Cf., § 3 BDSG - Tratamento de dados pessoais por autoridades públicas. O processamento de dados pessoais por uma autoridade pública é permitido se for necessário para o desempenho da tarefa sob a responsabilidade do responsável pelo tratamento ou no exercício da autoridade oficial delegada do responsável pelo tratamento. [Artigos adequados do RGPD Art. 6 RGPD Legalidade do processamento (nota dos tradutores)].

[88] Ver, também. para a Alemanha - relacionado com o tratamento de dados pela polícia e pelo sistema judiciário, S. Schwichtenberg, Die "kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz, in: Datenschutz und Datensicherheit 2016, 605-607.

Evidentemente, essa regulamentação também se aplica ao tratamento de dados pessoais na área de Big Data (ver também 11.1 abaixo), ou seja, dados que desde o início foram considerados como dados pessoais, mas também dados que podem ser (re)construídos individualmente com base na analítica. Big Data Analytics, entretanto, também coleta dados para os quais uma referência pessoal não é dada ou não é produzida. A este respeito, os regulamentos gerais de proteção de dados não se aplicam[89].

Deve-se ter em mente que as aplicações de Big Data também utilizam dados pessoais, mas não apenas de caráter pessoal, e combinam dados pessoais com outros dados, muitas vezes também com dados de outras pessoas. Também a este respeito surgem questões relacionadas com a proteção da personalidade.

Um problema particular surge quando os dados de uma pessoa são combinados com dados de outras pessoas e possivelmente outros dados no curso da análise de Big Data e utilizados para formar grupos de pessoas com características comparáveis. Tal afetação a este grupo através de métodos estatísticos e do registo de correlações pode ser utilizada para atribuir as características atribuídas a este grupo também a outras pessoas, sem que tenham sido efetuados inquirições a este respeito[90]. Caso se utilizem, com base nessas classificações, características presumidas para a seleção personalizada e para influenciar o comportamento, por exemplo, os efeitos são comparáveis aos que ocorrem com uma ligação a levantamentos específicos de dados pessoais. O fato de que os dados de origem utilizados para a formação de grupos tenham sido tornados anônimos para tratamento posterior não tem um efeito positivo sobre as pessoas em causa.

9.3.2 Revogação da vigência da lei nos Termos e Condições Gerais, em particular: à exigência de consentimento

Como acabou de ser referido, o requisito do consentimento para a coleta, tratamento e armazenamento de dados dos usuários por parte de provedores de

[89] Em 13 de setembro de 2017, a Comissão Europeia propôs um regulamento relativo à livre circulação de dados não pessoais na União Europeia (COM (2017) 495 final), a fim de tornar os dados não pessoais mais facilmente acessíveis e, por conseguinte, promover também as aplicações de dados de grande dimensão no mercado digital interno (mas não, por exemplo, para os proteger da interferência das aplicações de dados de grande dimensão). Este regulamento serve a livre circulação de mercadorias e, por conseguinte, não é concebido como uma lei de proteção de dados.

[90] Tais procedimentos analíticos - que são realizados com base em fatores como idade, sexo, estado civil, profissão, local de residência e afins - põem em perigo a autodeterminação das pessoas em causa, que normalmente não têm conhecimento disso, mas que, em última análise, são tratadas como se os dados pessoais tivessem sido coletados pelo sistema. Aferir a problemática em A. Roßnagel, Datenschutz: Eine Zukunft ohne Selbstbestimmung?, in: Spektrum der Wissenschaft kompakt online v. 4.10.2016, 41-49; derselbe/ M. Nebel, (Verlorene) Selbstbestimmung im Datenmeer – Privatheit im Zeitalter von Big Data, Datenschutz und Datensicherheit, in: Datenschutz und Datensicherheit 2015, 455-459.

serviços privados - que é o único a ser tratado aqui - é um dos requisitos essenciais da sua legalidade.

Por consentimento, define o artigo 4.º, nº 11, do RGPD: [...] «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Esse consentimento[91] pode ser dado como uma medida isolada, mas é muitas vezes necessário durante o processo de acordo com os TERMOS E CONDIÇÕES GERAIS (TCG) elaborados unilateralmente pelas empresas.

Art. 7.º, n.º 4, do RGPD ao examinar o conceito de carácter voluntário:

> [...] Ao avaliar se o consentimento foi dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

Os considerandos do RGPD tratam de alguns dos pormenores do requisito de consentimento. Parte do texto dos *considerandos* nº 42 estabelece o seguinte:

> [...]. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado. O que se contém no nº 43 acrescenta: A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato,

[91] Para condições de consentimento legalmente efetivo, ver artigo 4 (11) GDPR. Para mais informações sobre a legalidade, ver entre outros, J. Buchner/J. Kühling, in: J. Kühling/B. Buchner (nota de rodapé 77), Kommentierung zu Art. 7.

> incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

A natureza voluntária do consentimento é um elemento importante para a proteção da autonomia dos usuários. No entanto, se determinados serviços para os usuários forem praticamente indispensáveis por razões profissionais e pessoais importantes - por exemplo, para a ação no mundo do trabalho ou para a participação social na comunicação - e se não houver ofertas concorrentes de qualidade comparável, os usuários não têm praticamente outra alternativa senão dar o seu consentimento. Isto também deve ser tido em conta na interpretação do RGPD. É igualmente importante determinar se a coleta e o processamento dos dados pelo provedor estão relacionados ao conteúdo do uso pretendido. Há também razões para interpretar os requisitos do RGPD de forma restritiva, no sentido de que são impostas exigências elevadas à voluntariedade.

No entanto, não está claro se ou em que medida a padronização no RGPD deve ser entendida como uma proibição de vinculação[*92]. Os requisitos não são muito precisos e são susceptíveis de suscitar uma controvérsia considerável no futuro. Por exemplo, o nº 4 do artigo 7º do DSGVO não define os requisitos voluntários propriamente ditos, mas apenas designa um indicador para a sua avaliação que não é descrito de forma muito precisa. Uma vez que as empresas divulguem a coleta, tratamento e armazenamento de dados pessoais pelos TCG em troca da concessão do direito de uso de um serviço, ainda é necessário esclarecer se isso, por si só, pode ser suficiente para estabelecer que esse consentimento é necessário para o cumprimento do contrato. Estritamente falando, isto deve ser negado. O consentimento para o processamento de dados não é necessário para oferecer ou utilizar estes serviços como tal. Contudo, as empresas indicarão que elas próprias fizeram do processamento de dados o objeto do contrato - nomeadamente em

[*] No original Koppelungsverbot. A expressão do direito alemão *Koppelungsverbot* não tem exata tradução para o direito brasileiro, mas pode ser encontrado seu conteúdo nos princípios de *proibição de subordinação* ou de *vinculação contratual*. A fonte do princípio está no § 56 da Verwaltungsverfahrensgesetz (VwVfG) [*Lei de Procedimentos Administrativos*]. Observe-se que a jurisprudência tem expressado que a proibição de vinculação (ou subordinação) significa, por um lado, que um contrato de serviço público não deve vincular nada que ainda não esteja em um contexto interno e proíbe decisões soberanas sem a autorização legal correspondente de compensação econômica fazer, sendo irrelevante se as partes reconheceram ou mesmo reconheceram a inadmissibilidade do serviço (cf., BVerwG 20.03.2003 - 2 C 23/02).

[92] Sobre Koppelungsverbot, cf., J. Buchner/J. Kühling, in: J. Kühling/B. Buchner (nota de rodapé 77), nota de margem 52 f. Sobre o artigo 7º; A. Wolff/ S. Brink, BeckOK, Datenschutzrecht 2018, 28ª ed., Rn. 40 e ss. Sobre o artigo 7º do Regulamento Geral de Proteção de Dados; B.P. Paal/ D.A. Pauly, Datenschutzgrundverordnung. Bundesdatenschutzgesetz, 2018, Rn. 18 e ss. Sobre artigo 7º. Também, U. Dammann, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, in: Zeitschrift für Datenschutz 2016, 307 e ss., 311. Os pormenores não foram dados aqui, ver também nota de rodapé 142 abaixo.

contrapartida. Se isto for reconhecido, o requisito voluntário não será cumprido em grande medida.

É igualmente importante para a proteção jurídica dos usuários que o âmbito do consentimento exigido pelas empresas vá muitas vezes além da isenção das obrigações em matéria de proteção de dados no que diz respeito aos dados necessários para o tratamento dos seus dados. A maioria das empresas exige o consentimento para o uso de dados adicionais e, em alguns casos, até mesmo para a exploração de todos os dados disponíveis no sistema de tecnologia da informação do usuário. Além disso, normalmente não se distingue se o consentimento também pode levar à divulgação de dados pessoais de terceiros, como o parceiro de comunicação, ou seja, dados sobre os quais a parte que dá o consentimento não tem direito de dispor.

O grau de utilização de dados de terceiros é ilustrado - a título de exemplo - pelo chamado escândalo dos dados do Facebook, descoberto na primavera de 2018. Trata-se da transferência de dados de mais de 87 milhões de usuários do Facebook para a Cambridge Analytica. Esses dados, coletados com a ajuda de um aplicativo de pesquisa, provavelmente foram usados pelo presidente dos EUA, Trump, para apoiar sua campanha eleitoral. Os dados diziam respeito não só aos utilizadores de serviços concretos do Facebook, mas também, na sua maioria, a dados sobre pessoas com quem esses utilizadores tinham comunicado, como os chamados amigos do Facebook, cujos dados eram transmitidos através do envio de "likes"[93].

Devido à possibilidade de coletar vários dados, o consentimento dá às empresas que coletam e avaliam os dados a oportunidade prática de interferir com os direitos pessoais de terceiros sem que seja obrigatório que elas saibam disso e se protejam legalmente. A dimensão do problema está a alargar-se tendo em conta as novas possibilidades de interação, como na casa inteligente ou na utilização de sistemas de assistência linguística como o "Alexa". Aqui não se pode excluir que os dados sobre todos os usuários de uma moradia possam ser coletados, mesmo que eles mesmos não tenham dado o seu consentimento.

O requisito de consentimento é também frequentemente utilizado pelas empresas não só para tratar de questões de proteção de dados, mas também para condicionar a validade de uma série de outras obrigações jurídicas existentes para as empresas, reduzindo assim a proteção jurídica dos usuários. Isto aplica-se, por exemplo, ao âmbito da proteção dos direitos de autor ou da responsabilidade, mas também à redução da proteção jurídica através da designação de um local de

[93] O Facebook também não apagou esses dados quando soube do uso indevido dos dados pela Cambridge Analytica. A empresa ficou satisfeita com a promessa não cumprida de que a Cambridge Analytica apagaria os dados. Entretanto, de acordo com declarações feitas pelo Facebook, a prática de transmitir esses dados foi interrompida.

jurisdição estrangeira[94] ou de um sistema jurídico estrangeiro como único fator decisivo para as disputas judiciais[95].

Os sistemas jurídicos normalizam requisitos mais pormenorizados para os Termos e Condições Gerais (ver no caso da Alemanha sobre os §§ 305 e seguintes do Código Civil Alemão [BGB]) e muitas vezes também contêm possibilidades legais de um controle dos Termos e Condições Gerais. No entanto, essas normas não são regularmente adaptadas às particularidades da utilização dos Termos e Condições Gerais no âmbito de modelos empresariais específicos das TI ou especificamente à utilização de Big Data, especialmente não aos problemas especiais da criação e utilização de Termos e Condições Gerais por empresas com um oligopólio global. Os Termos e Condições Gerais normalmente utilizados no setor das TI permitem geralmente aos usuários limitar o âmbito do consentimento até certo ponto, mas normalmente apenas marginalmente. O recurso a esta possibilidade é também parcialmente complexo do ponto de vista técnico. Uma alternativa à utilização de serviços sem autorização para renunciar amplamente a direitos - como a possibilidade de proibir a utilização de dados não necessários para o tratamento do processo de comunicação concreto - quase nunca é concedida.

Do ponto de vista da política legal, seria justificável, se não necessário, obrigar os provedores a pagar aos usuários uma taxa justa se consentirem na coleta e no uso de dados que são particularmente valiosos para o processamento[96]. No entanto, é verdade que nem todos os dados têm um valor econômico elevado[97]. Mas como mostram as consideráveis margens de lucro de muitas empresas de TI, que se (co)financiam através do processamento de dados, o acesso aos dados pode ser muito lucrativo de um ponto de vista econômico e muitas vezes é assim. Se tais operações de processamento de dados forem afetadas, regulamentos vinculativos fariam sentido para que as operações de processamento só sejam permitidas contra pagamento para aqueles cujos dados sejam utilizados comercialmente pelas empresas. O mesmo se poderá fazer exigindo que os usuários concordem em reduzir a proteção dos direitos autorais ou os requisitos de responsabilidade dos provedores.

[94] Em 2017, o Supremo Tribunal canadense invalidou uma regra semelhante no domínio da lei canadense.

[95] Veja, por exemplo, o item 4.4 dos termos de uso do Facebook alterados em 2018 (enfraquecido como resultado do RGPD).

[96] Este estudo não aborda a questão, que é intensamente discutida em direito se, e em que medida, há um direito exclusivo comparável ou idêntico ao da propriedade. Para obter uma visão geral, consulte entre outros, B. Schütze/S. Hänold/N. Forgó, Big Data – eine informationsrechtliche Annäherung, in: B. Kolany-Raiser et al. (nota de rodapé 7), 239-248.

[97] Sobre a questão da determinação do valor dos dados, ver A. Picot/Y. Berchtold/R. Neuburger, Big Data aus ökonomischer Sicht: Potentiale und Handlungsbedarf, in: Kolany-Raiser (nota de rodapé 7), 395-399.

9.3.3 Dificuldades na aplicação dos princípios básicos de proteção de dados em aplicativos de Big Data

Os princípios tradicionalmente contidos no regulamento sobre a proteção de dados pessoais, em qualquer caso, e atualmente em particular os de limitação da finalidade e minimização de dados (Art. 5, parágrafo 1 RGPD), podem ser um obstáculo para os aplicativos de Big Data: Para dados agregados, é típico que os dados de origem devam ser utilizados para vários fins e que não seja possível desde o início - como para o titular dos dados no momento do consentimento - identificar que informação deve ser gerada pelo tratamento no domínio dos grandes volumes de dados e qual o seu significado. Além disso, os objetivos da utilização subsequente dos dados ainda não são geralmente claros, pelo que a exigência da finalidade pretendida (artigo 6.º, n.º 1-A, primeiro parágrafo, em conjugação com o artigo 5.º, n.º 1-B, RGPD) não tem praticamente quaisquer consequências[99]. Além disso, quanto mais dados de diferentes tipos estiverem disponíveis, mais bem-sucedida é, em princípio, a análise de Big Data, mais dados podem ser avaliados de diferentes modos e os resultados podem ser usados em diferentes contextos. Isto também contradiz o princípio da minimização dos dados. Por conseguinte, não é surpreendente que a relevância dos princípios de proteção de dados para as aplicações de Big Data seja criticada pelas empresas em causa como um obstáculo e uma inibição da inovação. A este respeito, salientam que as oportunidades associadas ao Big Data são reduzidas ou mesmo frustradas.

No entanto, não se justifica, por si só, que se abandone a validade dos princípios da proteção. Isto porque tal derrogação favoreceria unilateralmente a prossecução dos interesses dos processadores de dados e poderia levar à prevenção de formas de evitar ameaças à proteção jurídica das pessoas em causa em domínios que são frequentemente muito visíveis para elas. A este respeito, existe um potencial de conflito fundamental como resultado da utilização de Big Data, para cuja resolução a lei anterior - incluindo o RGPD e na Alemanha a BDSG (nova) - ainda não oferece quaisquer bem distribuídos resultados.

Em vista dos mandatos de garantia e proteção contidos no direito constitucional da UE e nacional que já foram mencionados várias vezes, são indispensáveis metas e instrumentos de proteção com segurança legal no setor de TI, incluindo aplicativos de Big Data. Sem a substituição por especificações que garantam funcionalmente uma proteção legal comparável à da lei de proteção de dados, não se justifica excluir a validade dos princípios mencionados em relação aos aplicativos de Big Data. Em particular, a justificativa de que esses princípios

[99] Para mais informações sobre estas e outras questões, ver as contribuições de G. Hornung, Erosion (nota de rodapé 51) e Y. Hermstrüwer (nota de rodapé 27). Ver também, Autoridade Europeia para a Proteção de Dados (Ed.), Bewältigung der Herausforderungen in Verbindung mit Big Data. Ein Ruf nach Transparenz, Benutzerkontrolle, eingebautem Datenschutz und Rechenschaftspflicht, 2015, obtido em: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_de.pdf,

estabelecem limites à agregação de dados e, portanto, ao uso do potencial de Big Data não é suficiente. Em vez disso, são necessárias abordagens adicionais para equilibrar os interesses dos usuários de Big Data e aqueles que podem ser afetados adversamente pelos aplicativos de Big Data (consulte 11.3 abaixo).

9.3.4 A proteção também dos interesses jurídicos coletivos

Os problemas de proteção adequada de interesses juridicamente importantes no decurso das aplicações de Big Data, incluindo a utilização de inteligência artificial, também surgem para além da proteção da personalidade. Embora a importância da proteção de dados continue a ser fundamental, é atualmente cada vez mais relegada para necessidades de proteção que não estão exclusivas ou principalmente relacionadas com o indivíduo, mas que dizem respeito a interesses coletivos e questões éticas. Trata-se também das condições-quadro para a participação pessoal no desenvolvimento social, bem como do conjunto da sociedade (ver 7. supra).

O crescimento dos grandes bancos de dados e a expansão e desenvolvimento das opções de avaliação, bem como a aplicabilidade dos resultados, nomeadamente devido ao aumento da comunicação apoiada pelas TI, podem ter consequências consideráveis para partes ou para toda a sociedade, incluindo a expansão das assimetrias de poder. Os debates públicos também abordam o risco de uma clivagem societal dos Big Data.

Os riscos da exploração ou mesmo do abuso de poder estão relacionados com as possibilidades dos intermediários de informação para a avaliação automatizada dos muitos e variados dados de usuário disponíveis para eles e para comunicação personalizada. A seleção personalizada de informações, como o feed de notícias, também oferece grandes oportunidades para influenciar a abordagem orientada da publicidade política e comercial. A dinâmica dos preços dos produtos também pode ter consequências sociopolíticas. Embora tais práticas tenham inicialmente apenas um impacto nas pessoas individualmente afetadas, têm também um impacto no tipo de fornecimento de informações ou no funcionamento do mecanismo de preços nos mercados.

Com a ajuda de Big Data Analytics, análises de tendências também são possíveis, que permitem estratégias coordenadas para a utilização da tendência, também para influenciar a opinião pública e as atitudes e experiências dos usuários. O microdirecionamento também pode ser importante para o comportamento eleitoral[100].

Gostaríamos particularmente de chamar a atenção para o problema da utilização de *bots* sociais[101]. Estes são programas de computador que usam perfis semelhantes aos de pessoas físicas e usam formulários de rede típicos, por exemplo,

[100] Cf., G. Hornung, Erosion (Fn.49), 92-93; K. Dankert, Verfälschung von Datenbeständen durch Social Bots, in: W. Hoffmann-Riem (Ed.) (nota de rodapé 27), 157, 158-160.

[101] Cf., K. Dankert (nota de rodapé 102 supra).

participando do discurso online. Eles podem disseminar desinformação ou falsificar opiniões maioritárias na Internet e, assim, manipular a formação de opinião individual e pública.

Nos casos em que o tratamento de dados permite o desenvolvimento do poder político ou social de uma forma problemática do ponto de vista democrático, jurídico e social, é importante que sejam criados mecanismos eficazes de contramedidas legais. Em todo o caso, tal não pode ser alcançado pela legislação em matéria de proteção de dados, que se baseia no direito de proteção individual.

9.3.5 Défices de transparência

A transformação digital criou novos espaços e métodos para a geração, coleta e utilização de informações. No entanto, os procedimentos utilizados e os resultados obtidos só são acessíveis às pessoas afetadas ou ao público em geral numa medida limitada. Muitas empresas, como os influentes intermediários de informação, evitam tanto quanto possível a transparência, excluem em grande medida a possibilidade de terceiros reproduzirem os procedimentos e, assim, impedem oportunidades para um controle externo eficaz - por exemplo, para descobrir seleções unilaterais ou para assegurar a responsabilização e a responsabilidade. No entanto, pode ser importante tanto para os usuários como para as autoridades de controle e para o público em geral, enquanto portadores de corresponsabilidade democrática, que o tratamento de dados, incluindo a sua utilização no contexto da análise de Big Data, seja compreensível e controlável na medida em que interesses jurídicos individuais ou coletivos possam ser negativamente afetados[102]. Os requisitos de transparência referem-se não só à possibilidade de perceber a superfície da comunicação, mas também ao conhecimento dos fenômenos que são importantes para compreender o funcionamento do controle baseado em algoritmos. Isso se aplica, por exemplo, ao design técnico e aos critérios e conceitos do uso de algoritmos.

A transparência é um pré-requisito para garantir, em particular, a responsabilização. Grandes problemas de intransparência estão associados ao uso de sistemas baseados em algoritmos de aprendizagem (ver 5. acima).

A eliminação dos déficits de transparência pressupõe requisitos legais que garantam a disponibilidade de informação suficiente sobre o campo regulatório a ser influenciado, não apenas sobre os dados na posse de atores públicos ou privados, mas também sobre a forma como eles são gerados e utilizados e a medida em que cumprem os requisitos legais.

O RGPD melhorou as possibilidades de obter informações sobre o tratamento de dados pessoais. Seção 2 do RGPD e §§ 32 e seguintes. O BDSG (novo)[103] prevê determinadas obrigações, em parte muito pormenorizadas, para os detentores de dados, de informar (individualmente) os titulares dos dados e os seus direitos de

[102] Para estas três dimensões de transparência, ver G. Hornung, Erosion (nota de rodapé 51), 97.
[103] Ver também a secção 55 e ss., BDSG (novo) - na aplicação da Diretiva (UE) 2016/680.

acesso[104]. Trata-se da coleta e tratamento - incluindo o tratamento para fins diferentes daqueles para os quais os dados foram coletados - e da transmissão de dados pessoais[105]. No entanto, apenas são registadas informações sobre dados pessoais especificamente obtidos, mas não, por exemplo, sobre todos os dados gerados e utilizados ou recentemente gerados pela utilização de tecnologias de informação ou pela análise de Big Data. As tarefas de monitorização e os poderes conferidos às autoridades independentes de proteção de dados (ver Capítulo VI do RGPD), incluindo os direitos de acesso (artigos 57º - 58º), também se limitam à proteção de dados pessoais.

Embora o RGPD descreva as obrigações básicas das empresas de forma relativamente pormenorizada, deixa uma margem considerável para interpretação e é particularmente reticente em saber exatamente para que fins os dados são utilizados, a fim de satisfazer os interesses dos usuários. De acordo com o Art. 14 do RGPD, os destinatários ou categorias de destinatários de dados pessoais só devem ser indicados "se necessário". A restrição "se aplicável" abrange igualmente as intenções dos responsáveis de transferir dados pessoais para um destinatário num país terceiro ou numa organização internacional (nº 1, alínea f), do artigo 14º). Estas e outras disposições tornam claro que a legislação em matéria de proteção de dados atualmente em vigor diz principalmente respeito à coleta de dados, mas apenas de forma limitada à utilização dos dados. No entanto, uma proteção de dados eficaz teria de dizer respeito, em grande medida, ao seu nível de utilização.

Existem também requisitos de transparência no que respeita ao tipo de algoritmos e à sua utilização. Por exemplo: Que máximas são utilizadas para a programação, que critérios são utilizados como base ou mesmo que informações são introduzidas como input, se os algoritmos forem utilizados para a seleção e controle em casos concretos - por exemplo segmentação ou definição de perfis (ver acima 7.3.2) ou pontuação*?[106]

O RGPD contém regras legais para melhorar a transparência, mas apenas parcialmente - e isso também se aplica à proteção de dados pessoais. Afinal, o art. 13 par. 2f. e art. 14 par. 2g do RFPD - fornece informações significativas sobre a lógica envolvida, bem como sobre o escopo e os efeitos pretendidos de tal processamento como parte do direito de acesso aos titulares de dados de uma subárea, nomeadamente tomada de decisão automatizada, incluindo criação de

[104] Para os limites da eficácia de tais informações, ver Y. Hermstrüwer (nota de rodapé 27).

[105] Art. 13-15 GDPR no sentido de nº 60 e segs., dos Considerandos. Para mais detalhes, por favor, consulte o comentário de J. Kühling/B. Buchner (nota de rodapé 77) e de B. P. Paal/D. A. Pauly (nota de rodapé 94).

* No original Scoring.

[106] O Scoring [pontuação] é a utilização de um valor de probabilidade sobre uma determinada conduta futura de uma pessoa singular; é utilizado, por exemplo, para avaliar a solvabilidade ou, de um modo mais geral, como base para uma decisão de celebrar, executar ou rescindir um contrato. Para os requisitos relativos a esse valor de probabilidade, ver § 13 BDSG (novo).

perfil (mas com a adição "pelo menos nesses casos")[107]. O que se entende especificamente por "lógica envolvida"[108] permanece em aberto. Na literatura, é descrito no sentido de "métodos e critérios"[109], mas sem especificar isso em mais detalhes. O RGPD carece de mais especificações, por exemplo, no que diz respeito às categorias de dados que podem ser utilizadas para aplicações especiais, como a pontuação. Por exemplo, poderia considerar-se a possibilidade de limitar a utilização de dados na pontuação ao histórico de crédito até à data da pessoa em causa e - por analogia com o direito a ser esquecido - poderiam ser previstos prazos para a utilização de determinados dados. Note-se apenas que tais restrições também seriam úteis em certos domínios da definição de perfis, como a limitação das categorias de dados para a definição de perfis no domínio dos procedimentos de aplicação, mas também na comunicação comercial. As particularidades dos algoritmos de aprendizagem também terão de ser abordadas, como a questão de saber em que medida a divulgação da "lógica envolvida" também inclui o procedimento nos programas de formação incorporados nos sistemas de aprendizagem algorítmica.

Não só na definição de perfis, mas também em outras áreas da tomada de decisão automatizada, surgem problemas para os quais ainda é necessário desenvolver soluções. Isto aplica-se, em particular, a uma área em rápido desenvolvimento como a da tecnologia jurídico-legal[49].

Há ainda outras questões por esclarecer, como a medida em que os deveres de informação e os direitos de informação, bem como as opções de monitorização anteriormente justificadas por lei, têm impacto no domínio das aplicações de Big Data. De qualquer forma, as pessoas afetadas por aplicações de Big Data nesta área - por exemplo, quando usam tecnologias preditivas - ainda não sabem regularmente quais os dados que as empresas realmente usam, que dados elas efetivamente ligam a outros dados da mesma forma e, portanto, fornecem outros usos possíveis, ou quais dados que elas passam para outras divisões do grupo, a outras empresas para seu uso de Big Data ou para os corretores de dados. Na medida em que existem direitos de informação dos usuários e deveres de informação das empresas, sua realização prática não é apenas complexa, mas também a administração dos resultados é difícil. Se as empresas cumprirem plenamente as suas obrigações de informação, os usuários ficam regularmente sobrecarregados com montanhas de dados, que, aliás, contêm muitas abreviaturas

[107] Isso sugere que o esquema só descreve um padrão mínimo. Sobre a questão de saber se a pontuação também está incluída, consulte J. Taeger, Scoring in Deutschland nach der EU-Datenschutzgrundlagenverordnung, in: Zeitschrift für Rechtspolitik (ZRP) 2016, 72, 75.

[108] Na literatura, a opinião é frequentemente expressa de que apenas os pressupostos básicos da lógica algorítmica devem ser comunicados, não os próprios algoritmos; ver, B. P. Paal/D. A. Pauly (nota de rodapé 94), parágrafo 31 ao art. 13.

[109] Cf., M. Bäcker, em J. Kühling/B. Buchner (nota de rodapé 77), n. ° 27 a Art. 15.

[49] Cf., as evidências a respeito na nota de rodapé 34.

e termos que são amplamente desconhecidos, de modo que informações significativas só podem ser obtidas praticamente por especialistas.

Não só os usuários individuais enfrentam problemas de informação. As instituições responsáveis pelo controlo do cumprimento da lei - como as autoridades responsáveis pela proteção de dados - também enfrentam problemas de informação consideráveis. Em qualquer caso, eles também sabem apenas excepcionalmente como e com quais objetivos as empresas usam Big Data e análise de Big Data relacionados (como descritiva, preditiva e prescritiva analítica).

Resta saber se, e em que medida, os novos regulamentos das leis de proteção de dados dos Estados-Membros da UE irão eliminar ou reduzir de forma sustentável os consideráveis défices de transparência. O fator decisivo será a aplicação das normas pertinentes e das orientações suplementares contidas nos considerandos do DSGVO e nos outros regulamentos pertinentes da UE.

9.3.6 Especialmente: Estado de Vigilância

As tarefas de proteção e os défices de transparência também existem na medida em que os dados e a análise de Big Data são utilizados para a a monitorização estatal, por exemplo, pelos serviços secretos, pelas autoridades de proteção constitucional, mas também pela polícia[50]. O RGPD não é relevante para este domínio problemático, mas a "Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou de execução de penas e à livre circulação desses dados"[51]. Esta Diretiva - que não é diretamente aplicável, mas deve ser preenchida pelo legislador nacional - foi (recentemente) transposta para o direito alemão pela Parte 3 da BDSG. A situação problemática regulamentada nestas bases jurídicas e que exige um tratamento independente não é aqui tratada em pormenor[52].

Note-se apenas em termos gerais que esta diretiva e a sua aplicação no BDSG (novo) também excluem os problemas regulamentares especiais com os megadados, embora estes também sejam utilizados de forma proativa e reativa para o cumprimento das tarefas aqui em causa, por exemplo, na vigilância estatal para efeitos de prevenção de riscos ou de ação penal[53].

Os problemas de falta de transparência e de responsabilização acima referidos (9.3.5) também se colocam aqui. No interesse da sua efetividade, a vigilância estatal é muitas vezes legitimamente dependente do sigilo. No entanto, isso não a isenta

[50] Cf., M. Bäcker (nota de rodapé 33); e, T. Singelnstein (nota de rodapé 27)

[51] Cf., Diretiva (UE) 2016/680 de 27 de abril de 2016, JO L 119 de 9 de maio de 2016, 89 e segs.

[52] Para o conteúdo da Diretiva, ver, entre outros, S. Schwichtenberg (nota de rodapé 90), 605-609

[53] Cf., T. Singelnstein (nota de rodapé 27); J.C. Joerden, Big Data und Kriminalität, in: W. Hoffmann-Riem (Ed.) (nota de rodapé 75), 173-178.

de obrigações legais[54]. É importante dispor de disposições eficazes de controle pelos tribunais, parlamentos e o público para garantir que estas sejam respeitadas. Na medida em que o controle judicial seja limitado e/ou confiado a um organismo de controle especial (como na Alemanha, nos termos do artigo 10.2, segundo parágrafo, da Lei Fundamental)[55], deve ser assegurada suficiente transparência - pelo menos em relação a esse organismo. Isso também se aplica aos aplicativos de Big Data.

10. Conclusão provisória: necessidade de revisão da lei existente

O poder associado ao acesso aos dados e ao seu tratamento, incluindo o poder de influenciar o comportamento e a consequente possibilidade de violar as liberdades civis, mas também de influenciar a evolução social, não pode ser aceito como não controlado nos Estados democráticos de direito. Os mandatos protetores e organizacionais do Estado, que estão ancorados não só nos direitos de liberdade, mas também nos objetivos do Estado, legitimam e exigem medidas legais de proteção, por exemplo, para proteger a autonomia das pessoas potencialmente desfavorecidas e seus outros direitos fundamentais, mas também no interesse do funcionamento dos processos sociais, bem como das infraestruturas controladas digitalmente e para a realização de outros fins de bem-estar público. O direito é um meio fundamentalmente adequado e seguro para fornecer e conceder proteção.

Ainda que a digitalização e, em particular, os Big Data não suscitem qualquer questionamento de todo o sistema jurídico, continua por esclarecer se e em que medida são necessárias alterações. Há muita discussão sobre isto. Como exemplo de tais tentativas de esclarecimento, faz-se aqui referência às negociações da 71ª Conferência dos Advogados Alemães em 2016. Por exemplo, o Departamento de Direito Civil testou uma parte substancial do Direito Civil sob o tema "Economia Digital - Direito Análogo: O Código Civil Alemão precisa de uma atualização?"[56] O Departamento de Direito Laboral e Social escolheu o tema "Digitalização do mundo do trabalho - desafios e necessidades regulamentares"[57]. Nos pareceres de

[54] Ver também, entre outros, M. Bäcker, bem como W. Hoffmann-Riem (em cada caso nota de rodapé 35).

[55] É uma Comissão de controle parlamentar chamada Comissão G10.

[56] Cf., F. Faust, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update? in: Verhandlungen des 71. Deutschen Juristentages Essen 2016, Band I, Gutachten, Teil A. Cf., ainda, ver também os artigos apresentados por M. Bartsch, H. Hummelmeier, E. I. Obergfell, Volume II/1 Sitzungsberichte - Referate und Beschlüsse K. Também, o artigo de T. Hoeren, Big Data und Zivilrecht, em: Hoffmann-Riem (nota de rodapé 27. Ver também, entre outros, A. Dix, Daten als Bezahlung - Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht, em: Zeitschrift für Europäisches Privatrecht 2017, 1-5.

[57] CF. R. Krause, Digitalisierung der Arbeitswelt - Herausforderungen und Regelungsbedarf, in: Verhandlungen des 71. Deutschen Juristentages Essen 2016, Volume I, Gutachten, Teil B; ver também os trabalhos apresentados durante o Juristentag por A. Seifert, G. Thüsing, V. Barth, T. Kremer, Volume II/1 Sitzungsberichte - Referate und Beschlüsse.

especialistas, apresentações e contribuições para a discussão, muitas tentativas foram feitas para interpretar as regras existentes de tal forma que elas possam ser mantidas na medida do possível e, se necessário, possam também satisfazer novos requisitos, alterando a sua interpretação. Foram igualmente formuladas propostas de alteração. Todas as sugestões foram cautelosas e de qualquer forma não estavam relacionadas com todas as áreas problemáticas que necessitavam de regulamentação.

As sugestões para novas abordagens regulatórias também podem ser encontradas em outros documentos - embora (apenas) de perspectivas específicas. Um exemplo é o relatório do Conselho Alemão de Especialistas em Consumo: "Verbraucherrecht 2.0"[58] (Direito do Consumo 2.0). É igualmente feita referência ao relatório especial da Comissão dos Monopólios sobre os desafios colocados pelos mercados digitais[59].

Quanto à tarefa de adaptar o sistema jurídico ao avanço da digitalização e à utilização da análise dos Big Data e dos seus resultados, importa, no entanto, sublinhar uma vez mais (ver 8.1 supra): no que respeita à proteção das liberdades civis existe - porque é evidente - a necessidade de expandir todas as regulamentações existentes à comunicação digital, utilização das infraestruturas digitais, utilização de Big Data e inteligência artificial ou de instrumentos de controle digital do comportamento. Também não exige uma ordem especial para que as autorizações já contidas na Lei Fundamental e nas Garantias Europeias dos Direitos Fundamentais possam também ser utilizadas no setor das TI para restringir as liberdades e, se necessário, devem ser utilizadas para evitar riscos associados à transformação digital. No entanto, continua a existir uma necessidade considerável de rever a legislação no sentido de a tornar adequada e, se necessário, de alterar um sistema jurídico existente e eventualmente obsoleto.

As razões para rever a legislação existente não se limitam, de modo algum, aos aspectos tecnológicos da transformação digital. Paralelamente, a ordem social está também em constante mudança e as condições de vida individual e social começam e redefinir-se[60]. Assim, a utilização de algoritmos digitais - como já referido no ponto 7 - pode alterar a percepção de acontecimentos reais, e ser utilizada para influenciar atitudes, valores e comportamentos, bem como para influenciar processos em matéria de tomada de decisões sociopolíticas[61].

---

[58] Cf., Sachverständigenrat für Verbraucherfragen, Verbraucherrecht 2.0. Verbraucher in der digitalen Welt, 2016. (Este documento pode ser consultado em: http://www.svr-verbraucherfragen.de/wp-content/uploads/Gutachten_SVRV-.pdf – nota dos tradutores).

[59] Cf., Monopolkommission, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015.

[60] Teoricamente em adição - também sob classificação no contexto do desenvolvimento histórico - F. Stalder (nota de rodapé 22).

[61] Nesse sentido, foi para muitos um sinal quando, no final de 2017, vários ex-altos funcionários do Facebook criticaram as estratégias do Facebook, incluindo os métodos de fidelização de usuários; a autocrítica também dizia respeito à exploração da da vulnerabilidade da psique humana e

O desenvolvimento da inteligência artificial reveste-se de particular importância para as necessidades de uma proteção jurídica abrangente na utilização de Big Data. Deve ser destacada também a criação de sistemas ciberfísicos nas áreas de produção e distribuição, que atualmente está sendo fomentada intensamente não apenas na Alemanha[62]. Estão também a ser criados novos requisitos para a regulamentação jurídica através de novas formas de conexão em rede - como por exemplo na *Smart Home*[63] - e novas possibilidades no domínio da mobilidade, como o smartphone, a computação em nuvem ou a condução automática ou autônoma de automóveis. Os problemas surgem também pelo fato de que uma grande quantidade de dados é gerada, processada e explorada. Novas formas de influência comunicativa (tais como *bots* sociais[64] ou a disseminação de notícias falsas[65]) também devem ser mencionadas. Existem

suscitou a expressão de preocupação de que o procedimento tinha ajudado a "romper o tecido social". Ver A. Kreye, When Facebook's Creators Warning against Facebook. Disponível em: http://www.sueddeutsche.de/digital/soziale-medien-wenn-facebooks-schoepfer-vor-facebook-warnen-1.3793266.

[62] No que diz respeito aos critérios regulatórios conexos - em particular, mas não só, no domínio da proteção de dados – ver G. Hornung/K. Hofmann, Industrie 4.0. und das Recht: Drei zentrale Herausforderungen, 2017. (A propósito, o excelente artigo aqui mencionado pelo autor, pode ser consultado online em: https://bit.ly/2IWU6Nl [link encurtado] – nota dos tradutores).

[63] Cf., H. Skistems, Smart Homes. Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2016.

[64] Neste sentido ver K. Dankert (nota de rodapé 37). Cf., J. Minkler, Social Bots im Meinungskampf, in: Zeitschrift für Urheber- und Medienrecht 2016, 216-222; do mesmo modo, Social Bots: Gesetzgeberische Maßnahmen auf dem Prüfstand, in: Zeitschrift für Innovations- und Technikrecht 2017, 199-207. Milker propõe, entre outros, requisitos de rotulagem para *bots* sociais, 205.

[65] Ver M. Oermann (nota de rodapé 37), 145-155. Veja também a - muito controversa - Netzwerkdurchsetzungsgesetz. Sobre esta lei, para mais informação, ver N. Guggenberger, Das Netzwerkdurchsetzungsgesetz in der Anwendung, in: Neue Juristische Wochenschrift 2017, S. 2577-2582. Para a versão preliminar, consultar M. Eifert, Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen. Zur Veränderung des Umgangs von Recht und Politik mit dem Internet, in: Neue Juristische Wochenschrift 2017, S. 1450-1454. [Nota dos tradutores: Relativamente a Netzwerkdurchsetzungsgesetz - NetzDG de 1º de setembro 2017: - Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Lei para a melhoria da aplicação da lei nas redes sociais (Lei de Execução de Redes de 1º de setembro de 2017 - NetzDG), pode ser consultada em Bundesgesetzblatt Teil I (BGBl. I) (Diário Federal da República Parte I) 2017 Nr. 61/07.09.2017, on-line em: https://bit.ly/35EEDLJ (link encurtado). De início é importante esclarecer que a NetzDG não cria novas categorias de conteúdo ilegal. Seu objetivo é fazer cumprir disposições no espaço on-line que já existiam no código penal alemão e responsabilizar grandes plataformas de mídia social por sua aplicação. As disposições incluem categorias como "incitação ao ódio", "disseminação de representações de violência", "formação de organizações terroristas" e "uso de símbolos de organizações inconstitucionais". O NetzDG também se aplica a outras categorias, como "distribuição de pornografia infantil", "insulto", "difamação", "difamação de religiões, associações religiosas e ideológicas de uma maneira que seja capaz de perturbar a paz

também campos de aplicação particularmente sensíveis[66], como o diagnóstico médico[67]. Entre outras coisas, temos de reagir às possibilidades acrescidas e mais diferenciadas da vigilância estatal e privada, mas também à espionagem e à sabotagem, que também têm lugar utilizando grandes volumes de dados (Big Data) e inteligência artificial.

11. Abordagens para possíveis soluções

O que vem a seguir são sugestões[68] para o tratamento legal de problemas selecionados ao fazer uso de Big Data[69]. Deve-se ter igualmente em conta que as propostas acima descritas (em particular o ponto 8.2), de que os direitos de liberdade e as disposições juridicamente vinculativas para a UE e para os Estados-

pública", "violação da privacidade íntima mediante fotografias", "ameaça a comissão d crime" e "falsificação de dados destinados a fornecer prova". O NetzDG tem como alvo grandes plataformas de redes sociais, com mais de 2 milhões de usuários localizados na Alemanha. Exige que essas plataformas forneçam um mecanismo para que os usuários enviem reclamações sobre conteúdo ilegal. Depois de receber uma reclamação, as plataformas devem investigar se o conteúdo é ilegal. Se o conteúdo for "manifestamente ilegal", as plataformas deverão removê-lo dentro de 24 horas. Outros conteúdos devem ser removidos dentro de 7 dias. Plataformas que não cumprem correm o risco de multas de até € 50 milhões. E conhecida também como Lei do FaceBook.]

[66] Cf., Considerando 51 do RGPD.

[67] Cf., Sobre o uso de Big Data em saúde K. Wiegerling, Big Data im Gesundheitswesen, in: B. Kolany-Raiser (nota de rodapé 7), 28-47.

[68] As referências feitas neste artigo não devem ser entendidas como significando que outras dimensões não são importantes para o significado em campos de inovação, especialmente as dimensões éticas (pela sua importância em campos de inovação ver W. Hoffmann-Riem (nota de rodapé 42), 253 - 259. Em particular, há uma necessidade de expandir a ética digital. Sobre o significado da ética e sua imbricação com a ordem jurídica, v. o parecer sobre a comissão de ética em matéria de dados (Gutachten der Datenethikkomission), 2019.

[69] Cf., B. J. Koops, Criteria for Normative Technology, in: R. Brownsword/K. Yeung (Ed.), Regulating technologies: Legal futures, regulatory frames and technological fixes, 2008, 167 e ss.; F. Saurwein/N. Just/M. Latzer, Governance of algorithms: Options and limitations, in: info 2015, 17 (6), 35-49; M. Martini, Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, in: Deutsches Verwaltungsblatt 2014, 1481-1489; K. Crawford/J. Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, in: Boston College Law Review 2014, 55, 93-128; Cf., também as contribuições de K. Schrader, D. Klein, S. Telle, G. Kalouta, in: J. Taeger (Ed.), Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, 2016.; Council of Europe, Draft Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, in: T-PD-BUR, 12 Rev 4, vom 07.11.2016; J.-U. Pille (nota de rodapé 37); U. di Fabio, Grundrechtsgeltung in digitalen Systemen, 2016, de modo sistematizador, 93-95. Ver também o parecer do Sachverständigenrats für Verbraucherfragen (Conselho Consultivo dos Consumidores), (nota de rodapé 121); L. F. Andersson/A. Alaja/D. Buhr/Ph. Fink/N. Stöber, Policies for Innovation in Times of Digitalization. A comparative report on innovation policies in Finland, Sweden and Germany, 2017; Hoeren (nota de rodapé 23); Parecer da Comissão de Ética e Dados (nota de rodapé 68), 159 - 224. Cf., ainda as contribuições da Parte II de W. Hoffmann-Riem (nota de rodapé 27).

Membros contêm regimes de proteção e garantia, cujo cumprimento exige um quadro jurídico correspondente[70].

Tanto a legislação tradicional em matéria de proteção de dados como o RGPD e o Projeto de Regulamento "Privacidade e Comunicações Eletrônicas" (e-Privacy-Verordnung)* contêm abordagens utilizáveis com o propósito de proteger as pessoas mais vulneráveis, mesmo que essas abordagens sejam demasiado limitadas no âmbito de aplicação e na profundidade dos efeitos. Em particular, deve ser feita referência às regras em matéria de responsabilidade e transparência, aos direitos e obrigações de informação, às possibilidades de certificação, por exemplo, por organismos acreditados, e à tarefa de controlo. Existem também regras sobre as autoridades de supervisão e os seus poderes. O RGPD contém muitos detalhes sobre isso, mas também muitas regras flexíveis que requerem interpretação e exceções. Resta saber até que ponto se irá concretizar na prática.

No caso vertente, porém, há que salientar mais uma vez que essas regras apenas dizem respeito à proteção de dados pessoais - e isto apenas em algumas áreas de risco. A legislação em matéria de Proteção de Dados não é um direito abrangente à liberdade, nem um direito universal à autonomia. Por exemplo, não se centra no tratamento de dados não pessoais e em qualquer interferência que daí possa resultar, e muito menos na proteção de bens públicos de interesse coletivo ou mesmo na proteção contra o abuso de poder - jornalístico, político, econômico, etc. - para além da violação de direitos pessoais com a ajuda de tecnologias digitais.

[70] Diferentes sistemas jurídicos contêm diferentes requisitos, cuja adaptação à transformação digital desencadeará, sem dúvida, uma necessidade considerável de debate. Como exemplo de uma possível nova abordagem, consulte W. Christl/S. Spiekermann, Networks of control: A report on corporate surveillance, digital tracking, big data & privacy, 2016, 139 e ss. Em particular, os autores consideram transferir os princípios do devido processo de direito contido na lei dos EUA para restrições de liberdade por empresas privadas de TI. No ordenamento jurídico alemão, um paralelo seria estender os requisitos constitucionais desenvolvidos para a interferência estatal nos direitos fundamentais relevantes aos entraves à liberdade emanados de particulares cujo poder de intervenção seja funcionalmente comparável ao das entidades estatais.

* e-Privacy-Verordnung (ePrivacy Regulation - ePR pelo acrônimo em inglês. O Projeto de Regulamento completo do Parlamento Europeu e do Conselho no que respeita à privacidade e a proteção de dados pessoais nas comunicações eletrônicas, deverá revogar a Diretiva 2002/58 / CE (Diretiva Privacidade e Proteção Eletrônica). O Regulamento de Privacidade Eletrônica vai se constituir em um texto especializado (Lex Specialis), que visa especificar o RGPD para o setor de comunicações eletrônicas. Além disso, o Regulamento ePrivacy complementa o GDPR com disposições que vão além do escopo do GDPR. O principal objetivo do ePrivacy é proteger a confidencialidade das comunicações eletrônicas. O texto também analisa a confidencialidade dos dispositivos eletrônicos, regulamentando cookies e outras tecnologias de rastreamento. O Regulamento de Privacidade Eletrônica também rege as regras de inclusão / exclusão e exclusão ativa para marketing direto e propõe uma definição de marketing direto. Por fim, o texto também inclui algumas disposições para o setor de telecomunicações. Encontra-se até a data da publicação deste ensaio em tramitação no Conselho Europeu. (Nota dos tradutores).

Considerando o volume crescente e a heterogeneidade das existências de dados processáveis e as muitas formas como podem ser interligadas e tratadas, os problemas regulamentares devem ser abordados em relação a diferentes áreas problemáticas. Isto afeta as possibilidades de influenciar o comportamento utilizando Big Data e inteligência artificial, tais como o desenvolvimento de orientações socioculturais, desenvolvimentos na sociedade como um todo e a gestão de tarefas concretas como o controlo das infraestruturas de transporte ou energia ou dos processos de produção. Isso requer conceitos jurídicos e precauções que incluam a proteção de interesses jurídicos que vão além da proteção de dados pessoais.

11. 1 Redefinição do conceito de dados pessoais

Ainda que a lei de proteção de dados possa continuar a ser aplicável na área de Big Data, podem ser necessárias alterações, algumas das quais podem resultar de alterações na interpretação ou de novas disposições legais.

Uma importante questão aqui é a definição do conceito de dados pessoais. Consideravam-se como tal, até agora, os dados relativos a uma pessoa singular identificada ou identificável. A identificabilidade é definida - como no artigo 4.º, n.º 1, do RGPD - com base em determinados critérios (restritos). Esta descrição é novamente citada aqui (ver já acima 3). Uma pessoa singular é considerada identificável " que possa ser identificada direta ou indiretamente, nomeadamente por referência a um identificador como um nome, um número de identificação, dados de localização, um identificador em linha ou uma ou mais características especiais que exprimam a identidade física, fisiológica, genética, psicológica, econômica, cultural ou social dessas pessoas singulares"[71]. Os dados deixam de ser pessoais se tiverem sido tornados anônimos e não puderem mais ser desanonimizados[72]. Isso também se aplica a dados usados em contextos de Big Data.

Além disso, os dados que não são coletados de uma pessoa específica, mas que podem ser usados para filtrar pessoas específicas e submetê-las a medidas específicas, também devem ser classificados como pessoais. Esse é o caso, por exemplo, se alguém for atribuído a um grupo de pessoas (um cluster) formado no decorrer da análise de Big Data usando métodos estatísticos sem interferir com seus próprios dados pessoais[73] e a pessoa for atribuída a características adicionais somente por causa dessa atribuição. Podem incluir questões de saúde, recursos financeiros, orientação sexual e muito mais. Ao atribuir essas características, é

[71] Consultar as informações suplementares no Considerando 26 do RGPD. Para uma compreensão do conceito de dados pessoais pelo TJCE, ver TJCE, Processo C-582/14, Ecli: EU: C: 2016: 779, ponto 49.

[72] Ver o Considerando 26 do RGPD.

[73] Ver acima, no texto, a nota de rodapé 92.

possível acionar consequências atuais ou potencialmente estressantes para as pessoas atribuídas a esse grupo[74].

Do mesmo modo, não se pode continuar a afirmar que a referência pessoal é sempre omitida através da anonimização dos dados[75]. A atual expansão do poder das técnicas de desanonimização justifica que não se considere suficiente uma anonimização inicial por si só, uma vez que existem inúmeras possibilidades de desanonimização, especialmente se esta for utilizada[76]. Em consequência, é necessário ampliar o conceito de dados pessoais aos dados inicialmente anonimizados, mas que podem ser desanonimizados ou posteriormente desanonimizados.

Mesmo quando lidamos com dados agregados, não se pode excluir que se possam tirar conclusões sobre indivíduos específicos[77].

A ampliação do conceito de dados pessoais assim exigida também beneficia a proteção de dados no âmbito do direito individual na área de Big Data, sem, no entanto, ser capaz de cobrir todas as áreas problemáticas associadas a Big Data.

11.2 Aperfeiçoar a proteção jurídica do consentimento para o processamento de dados

As condições para a legitimidade para o processamento de dados (pessoais) (por exemplo, artigo 6.o do RGPD, ver supra 9.3) são problemáticas. Neste contexto, o elemento constituinte do consentimento como uma condição de legitimidade foi novamente tratado. O projeto de regulamento relativo à privacidade e às comunicações eletrônicas determina igualmente o consentimento para o importante critério da legalidade do tratamento de dados. Os défices de consentimento acima descritos (9.3.2) também existem aqui.

O consentimento voluntário constitui uma solução adequada, na medida em que respeita a autonomia das pessoas em causa e lhes permite decidir em que medida desejam autorizar o tratamento de dados. No entanto, na prática, em muitos casos, é duvidoso não só se a pessoa em causa está suficientemente informada, mas também se esse consentimento é voluntário[78]. Esse último - como já foi mencionado – diz, em especial, que sem o necessário consentimento não for possível o acesso a serviços ou quaisquer outros benefícios importantes ou mesmo

[74] Cf., W. Christl/S. Spiekermann (nota de rodapé 133), 143

[75] Para mais informações, ver P. Glas, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz. Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, 2017, 11-117; J. Hermstrüwer (nota de rodapé 29), 104 com nota de rodapé 14.

[76] Cf., A. Roßnagel, Big Data – Small Privacy. Konzeptionelle Herausforderungen für das Datenschutzrecht, in: Zeitschrift für Datenschutz 2013, 562 e ss.; V. Boehme-Neßler, Das Ende der Anonymität. Wie Big Data das Datenschutzrecht verändert, in: Datenschutz und Datensicherheit 2016, 419, 421 e s.

[77] Cf., P. Glas (nota de rodapé 138), 117–118.

[78] Cf., J. Hermstrüwer (nota de rodapé 27), Informationelle Selbstgefährdung; P. Radlanski, (nota de rodapé 24); W. Hoffmann-Riem (nota de rodapé 37), 21-23.

indispensáveis para as pessoas em causa do ponto de vista profissional ou pessoal. É de supor que existe aqui uma ausência paridade contratual, pelo que deve ser prevista uma compensação legal. Tal deverá garantir que a recusa de consentimento para o tratamento desses dados, que não é indispensável para a prestação dos serviços, não conduza à exclusão dos serviços oferecidos. Neste sentido, o nº 4 do artigo 7º do RGPD tem esta finalidade. Já foi explicado que é adequado interpretar esta norma como uma proibição estrita do sistema de acoplamento, quando possível (9.3.2)[79].

Deve ainda ter-se em conta que, muitas vezes, o consentimento não é concedido de forma isolada, mas - como acontece frequentemente com a utilização de serviços sociais na Internet, por exemplo - tem de ser exigido no contexto de condições gerais mais abrangentes e unilateralmente estruturadas que também restringem a proteção jurídica dos usuários em outros aspectos (ver 7.3.1 supra). Essas possibilidades têm de ser restringidas por lei.

Uma abordagem adequada para salvaguardar os requisitos de proteção seria um controle dos TCG(s) especialmente adaptado ao setor das TI, associado à participação das associações de defesa do consumidor. Um meio de controlar seria a certificação por organismos (acreditados) reconhecidos publicamente e/ou instituições oficiais especiais, em todo o caso, de TCG(s) particularmente importantes para a sociedade. No decurso da certificação, seria necessário verificar antecipadamente se os Termos e Condições Gerais cumprem os requisitos legais. A certificação pode ser concebida como uma obrigação ou como uma mera possibilidade. Neste último caso, porém, também teriam de ser previstas sanções no caso de as empresas renunciarem à certificação. Isto poderia, por exemplo, levar a uma inversão do ônus da prova ou - na medida em que o sistema jurídico contenha disposições em matéria de responsabilidade - a um aumento da responsabilidade na ausência de certificação[80].

Em termos de conteúdo, um controle dos TCG(s) teria não só de garantir que os TCG(s) não possam ser alterados pelas empresas sem informar as pessoas em causa, mas também que sejam claros e fáceis de compreender (cf. requisitos correspondentes de consentimento no artigo 7 (2) do RGPD) e que o conteúdo esteja relacionado com todos os requisitos de proteção significativos. Também teria que ser exigido para lidar com os usos de Big Data pretendidos e as condições da sua admissibilidade. Devem também ser especificadas precauções de proteção aquando da transmissão de dados para outras finalidades ou a outros agentes. Além disso, o direito das pessoas em causa à transferibilidade dos dados já consagrado no artigo 20 do RGPD deve ser expandido.

11.3 Aplicabilidade e reformulação dos Princípios Jurídicos da Proteção de Dados

[79] Veja as evidências retro, nota de rodapé 94.

[80] Cf., as considerações de A. Tutt (nota de rodapé 20), 105-123, e T. Wischmeyer (nota de rodapé 20), 393-400.

Como já foi referido (ver 9.3.3), a legislação em matéria de proteção de dados estabelece determinados princípios para a coleta e utilização de dados pessoais, tais como economia ou minimização de dados, limitação da finalidade e - como expressão do princípio da proporcionalidade - a necessidade. Contudo, a sua aplicação e, em especial, o seu controle são já difíceis nos domínios tradicionais da proteção de dados, sobretudo devido à falta de transparência já mencionada várias vezes (ver 9.3.5 supra), mas também devido às múltiplas delimitações no domínio das TI.

Já foi afirmado que esses princípios não foram desenvolvidos tendo em mente as particularidades do Big Data. Foi também referido que a aplicação desses princípios aos procedimentos relativos aos Big Data tem sido criticada, em especial pelas empresas em causa, como sendo hostil à inovação. No entanto, os possíveis efeitos inibidores da inovação não são, por si só, justificação suficiente para abandonar as preocupações suscitadas por estes princípios no domínio dos grandes volumes de dados. Servem a proteção de interesses jurídicos e, em especial, a observância do princípio da proporcionalidade quando são lesados interesses dignos de proteção jurídica. No entanto, uma vez que o princípio da proporcionalidade não visa unilateralmente proteger os interesses das pessoas afetadas por determinadas medidas, mas sim permitir um equilíbrio entre interesses diferentes, possivelmente no decurso da ponderação dos interesses, existem também possibilidades no domínio das aplicações de Big Data de ter em conta os vários interesses. Isto pode exigir uma diferenciação na determinação do conceito de conteúdo e do âmbito dos princípios de proteção da liberdade.

Na ponderação dos interesses, devem ser tidos em conta não só os interesses individuais das pessoas afetadas concretamente no decurso da garantia da proteção da liberdade, mas também os interesses de importância coletiva. Isto inclui a proteção fundamental contra a seleção unilateral na divulgação de informações ou contra a manipulação de valores pessoais, por exemplo, para controlar comportamentos, influenciar tendências sociais ou o voto em eleições.

A fim de encontrar fatores de conexão para a observação de princípios como a necessidade e a finalidade, pode ser aconselhável ou mesmo inevitável prever que certas categorias de análises de Big Data sejam utilizadas apenas para dados para os quais as marcações e a limitação da finalidade[81] são obrigatórias antes da sua utilização ou divulgação e para os quais são previstos períodos de exclusão ou bloqueio. Podem ser previstas obrigações de documentação para a transferência e

[81] Para considerações técnicas para proteger dados e documentos por meio de marcações imutáveis, compare G. Spyra/W. J. Buchanan Protecting documents with sticky policies and identity-based encryption, 2016. Obtido em: http://www.iidi.napier.ac.uk/binary/dl/file/publicationid/13387024.

a exploração dos dados[82]. Tais obrigações teriam também de ser estendidas para abranger novos dados criados pelas aplicações Big Data.

Dadas as oportunidades inovadoras associadas ao desenvolvimento da digitalização, desenvolver novas possibilidades para a realização de tais especificações, é uma tarefa que vale a pena, se necessário, apoiada por regulamentos estatais. "Forçar a inovação"[83]: Se os responsáveis por Big Data não conseguirem desenvolver as soluções inovadoras legalmente previstas para proteger terceiros, devem abster-se das utilizações de Big Data.

11.4 Aumentar a transparência no que respeita ao design técnico e aos algoritmos utilizados.

Para uma proteção de dados em geral, mas também para a proteção de outros interesses legais contra aplicações de Big Data, a garantia de transparência deve ser indispensável. Objetos de uma demanda por mais transparência não são apenas a coleta e o processamento[84] de dados em geral, mas também - como já mencionado - o design tecnológico (o projeto técnico) e os algoritmos utilizados em cada caso, ou melhor: os sistemas algorítmicos, inclusive com as precauções para "treinar" esses sistemas.

No entanto, a proteção dos segredos comerciais é contrária ao dever de divulgação. O Bundesgerichtshof (Tribunal Federal de Justiça) reconheceu, em princípio, tal proteção em uma decisão sobre a pontuação do SCHUFA*.[85] No entanto, há que ter em conta que a proteção dos segredos comerciais não constitui um fim em si mesmo, mas exige igualmente uma coordenação com a proteção de pessoas que não a empresa em causa e, por conseguinte, de interesses jurídicos diversos. Isto dá origem a diferenciações, que podem ter de ser feitas pelo legislador. O mesmo se aplica ao tratamento dos segredos oficiais. Esta questão só deve ser salientada aqui.

Um dever geral de divulgar o design tecnológico e os sistemas algorítmicos utilizados iria, contudo, interferir demasiado profundamente com a autonomia das empresas e afetar os seus legítimos interesses, nomeadamente ao impedir que os

[82] No entanto, não se deve esquecer que tais acordos podem também ter consequências problemáticas, nomeadamente uma maior facilidade de identificação das pessoas a quem os dados dizem respeito.

[83] Sobre esta categoria de regulamentação jurídica, ver W. Hoffmann-Riem, (nota de rodapé 42), 430-432. Trata-se de uma técnica através da qual são estabelecidos requisitos regulamentares que ainda não foram alcançados de acordo com o estado atual da técnica, mas que parecem ser exequíveis.

[84] No que diz respeito aos acordos de transparência para o próprio tratamento de dados, ver Considerandos 39 e 58 do RGPD.

* A Schufa Holding AG, fundada em 1927, é uma agência de crédito privada alemã, apoiada por credores. Tem sede em Wiesbaden, capital de Hessen, Alemanha. O objetivo da SCHUFA é proteger seus clientes contra riscos de crédito. Também oferece proteção contra insolvência para os mutuários. Site: https://www.schufa.de/de/ueber-uns/ (link permanente).

[85] Cf., Decisões do Tribunal Federal de Justiça em matéria civil (BGHZ) 200, 38. No entanto, é muito duvidoso se esta decisão cumpre os requisitos do Capítulo III RGPD.

algoritmos sejam acessíveis aos concorrentes que os utilizam como "free riders" ou a outras pessoas que possam utilizar esses conhecimentos para manipular determinados resultados. Justifica-se, no entanto, tornar possível a transparência e o controle, na medida em que, de outro modo, a proteção jurídica poderia fracassar. No caso dos algoritmos, a transparência deve, em qualquer caso, ser assegurada no que respeita às máximas e aos critérios, em especial os algoritmos cuja utilização pode prejudicar interesses jurídicos importantes que protegem os direitos fundamentais, nomeadamente contra a discriminação, a estigmatização e a manipulação. O mesmo se aplica se existir outro interesse legítimo na divulgação - minimamente limitado - que seja pelo menos equivalente à proteção de um segredo comercial. Isto pode ser prescrito para procedimentos específicos, tais como procedimentos de certificação ou tutela judicial, ambos, se necessário, com a criação do correspondente procedimento sigiloso[86].

No entanto, a transparência não é importante apenas para o tratamento dos dados em si, mas sobretudo no que respeita à utilização dos conhecimentos gerados e processados com a ajuda de Big Data em domínios de aplicação sensíveis à liberdade, como é o caso do setor da saúde[87]. Por conseguinte, devem ser tomadas precauções para que a certificação da utilização de Big Data em áreas sensíveis da sociedade seja ainda determinada por organismos acreditados. A este respeito, a construção prevista nos artigos 42 e 43 do RGPD para a proteção dos dados pessoais teria de ser objetivamente ampliada e modificada. Tal deve igualmente ser complementado por procedimentos de verificação do cumprimento dos requisitos (como meio de monitorização contínua). A fim de poder executar controles de forma eficaz, as obrigações de registar/documentar a utilização de Big Data para certos usos também deve ser considerada. Exemplos de campos para obrigações de documentação relativas aos critérios de decisão utilizados são a utilização de Big Data no decurso da definição de perfis ou pontuação[88], por exemplo, no cálculo de tarifas de seguro ou na decisão de conceder crédito. Também seria importante limitar as opções de armazenamento.

Além disso, é importante prever proibições especiais quanto à utilização de dados, em especial para evitar discriminações com base em critérios cuja utilização seja declarada inconstitucional ou contrária ao direito comunitário pelo artigo 3º, nº 3, da Lei Fundamental, pelo artigo 21 da Carta dos Direitos Fundamentais da UE e pelo artigo 5º do RGPD.

11.5 Expansão da proteção sistêmica

Tendo em conta a complexidade dos domínios em que os dados podem ser utilizados e tratados por tecnologias como a análise de dados de grandes

[86] Para esse procedimento, ver 11.7.

[87] Cf., K. Wiegerling (nota de rodapé 130).

[88] Especialmente para este fim, T. Weichert, Scoring in Zeiten von Big Data, in: Zeitschrift für Rechtspolitik 2014, 168-171.

dimensões e estratégias para influir sobre as condições sociais, é incorreto considerar a proteção contra eventuais violações de direitos principalmente como uma tarefa para os usuários individuais. É ilusório poder proporcionar um nível adequado de proteção apenas através da proteção jurídica individual. Em primeiro lugar e acima de tudo, precisamos de um sistema de proteção proativo, abrangente e sistemicamente seguro[89]. As características especiais do uso de Big Data requerem a diferenciação e o desenvolvimento das possibilidades de proteção do sistema além da proteção sistêmica já prevista no RGPD.

A proteção sistêmica pode ser estimulada por lei, mas não é necessariamente de natureza jurídica. A proteção sistêmica inclui, em especial, a proteção de dados desde a concepção tecnológica ("Protection by Design"). O que é importante - numa direção proativa - é sobretudo a criação de arquiteturas de decisão adequadas à proteção e, em particular, a utilização das possibilidades da concepção tecnológica, por exemplo, através de especificações normalizadas e de definições de proteção por defeito ("Protection by Default") que conduzam à proteção jurídica. Art. 25 do RGPD e § 67 da BDSG (nova) criam abordagens para isto, mas novamente limitado ao tratamento de dados pessoais. Também não existem pontos de partida para a proteção sistêmica no que respeita às definições normalizadas adaptativas. Além disso, a proteção de dados desde a concepção tecnológica é também importante para garantir a segurança (Security by Design).

A proteção sistêmica pode ser estimulada por lei, mas não é necessária de natureza legal. A proteção sistêmica inclui, em particular, a proteção de dados através do design tecnológico ("Protection by Design"). O que é importante - em uma direção proativa - é sobretudo a criação de arquiteturas de tomada de decisão adequadas para proteção e, em particular, o uso de possibilidades de design tecnológico, por exemplo, através de especificações padrão e configurações padrão legalmente protegidas. ("Protection by Default"). O Artigo 25 do RGPD[90] e o § 67 da BDSG (novo) criam abordagens para esse fim[91], mas também neste caso limitado ao processamento de dados pessoais. Além disso, não há pontos de partida para proteção sistêmica em relação às configurações padrão adaptativas[92]. Além disso, o

[89] Cf., I. Spiecker gen. Döhmann, Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen, in: Computer und Recht 2016, 698-704.

[90] Cf., J. Kühling, in J. Kühling/B. Buchner (Ed.) (nota de rodapé 77), Nota de margem 14 e ss., 24 e ss., e o Art. 25.

[91] Para o conceito e as possibilidades de design cf., ENISA (European Union Agency for Network and Information Security), Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, Dez. 17, 2015; também, Privacy Enhancing Technologies: Evolution and State of the Art, 2017. (Este ultimo pode ser acessado em; https://www.enisa.europa.eu/publications/pets-evolution-and-state-of-the-art/at_download/fullReport – link permanente – nota dos tradutores).

[92] Cf., Y. Hermstrüwer (nota de rodapé 27), 114 com nota de rodapé 51.

design tecnológico também é importante para garantir a segurança ("Security by Design").

No entanto, deve-se ter em mente que a proteção pela tecnologia significa que um projeto de tecnologia realizado apenas pelas empresas, não influenciado por terceiros ou pelo menos controlado[93] por elas poderia ser uma tentação para a primeira minar, em vez de promover uma proteção legal efetiva.

As precauções sistêmicas também podem ajudar a ampliar a proteção da autonomia dos usuários no futuro. Uma forma de proceder desta forma seria obrigar os responsáveis pelo tratamento dos dados a fornecerem aos usuários interfaces programáticas padronizadas para posterior acesso e administração dos seus próprios dados pessoais.

As medidas de proteção sistêmica também podem incluir a redução de redes globais e a criação de redes e nuvens descentralizadas e autônomas para comunicações particularmente sensíveis, limitando assim seu uso. Uma conexão local pode ser recomendada para a avaliação e uso de dados, especialmente em áreas particularmente expostas a lesões. No entanto, devemos ter em conta – mas também questionar criticamente - o fato de que a UE é amplamente hostil aos requisitos de localização no que diz respeito aos dados não pessoais[94].

11.6 Ampliação da supervisão soberana[*]

Uma vez que a proteção jurídica individual não é de modo algum suficiente para evitar os perigos colocados pela digitalização, deve também ser assegurada uma supervisão soberana eficaz do cumprimento dos regulamentos. As instituições criadas até à data, como os responsáveis pela proteção de dados, não são suficientes para o efeito, pelo menos não na medida em que sejam responsáveis por mais do

[93] Para possibilidades de expandir o círculo de atores envolvidos para um "design participativo" em design técnico, cf., C. Ochs/Ph. Richter/M. Uhlmann, Technikgestaltung demokratisieren – partizipatives Privacy by Design, in: ZD-aktuell 2016, 05424.

[94] Por exemplo, a Comissão propõe que um projeto de regulamento (ver nota de rodapé 91 acima) revogue os requisitos de localização para o uso exclusivo de dados não pessoais, a fim de promover o livre fluxo de dados no interesse do mercado comum.

[*] "Atividades soberanas" ou tarefa soberana como supervisão ou monitoramento são aqueles encargos cujo cumprimento o Estado está sujeito pelo direito público. Esse cumprimento ocorre através da administração direta e indireta do Estado. O exercício de atividades oficiais encontra sua regulamentação legal no Art. 33 (4) da Lei Básica. De acordo com isso, deve ser transferido para membros da função pública, que estejam em uma relação de serviço público e lealdade. Segundo o Art. 33 (4) da Lei Básico, "[...] O exercício de funções de soberania será confiado, como regra geral de caráter permanente, a funcionários públicos, sujeitos a relações de serviço e de fidelidade ancoradas no direito público". (Nota dos tradutores).

que a proteção de dados pessoais. Os benefícios de tais instituições também são limitados, enquanto não dispuserem de equipamento suficiente - como é atualmente o caso, por exemplo, dos Comissários alemães para a Proteção de Dados.

No debate público há várias propostas para a criação de novos poderes e instituições [95]. Essas iniciativas incluem a ampliação dos poderes das atuais autoridades de proteção de dados ou a criação de uma especial "agência digital"[96]. Na Alemanha, foi proposto que as tarefas (funções) do Bundeskartellamt* fossem ampliadas para além da salvaguarda da concorrência, passando a incluir o monitoramento de serviços digitais[97]. Ao fazê-lo, deve poder ir além do exercício

[95] Essas propostas incluem também a criação de um Ministério Digital ao nível Federal e dos Länder. Ver, por exemplo, C. Djeffal, Deutschland braucht nicht ein Digitalministerium, sondern viele! in: Süddeutsche Zeitung, 18. September 2017. Obtido em https://bit.ly/2P0keLe (link encurtado. N.T.). Desde o início de 2018, um Ministro de Estado para a Digitalização (Dorothee Bär*) tem estado presente na Chancelaria Alemã. A sua principal tarefa é acelerar a digitalização e não assegurar as necessidades de proteção discutidas neste estudo. Há também Ministros Digitais a nível estatal, por exemplo, no Estado da Renânia do Norte-Vestefália. (* Dorothee Bar é Ministra de Estado da Digitalização na Chancelaria Federal – nota dos tradutores).

[96] No entanto, é duvidoso se os seus poderes vão tão longe quanto A. Tutt (nota de rodapé 20) propôs para os EUA, sugerindo a criação de uma instituição comparável à Federal Drug Administration.

[*] O Escritório Federal de Combate aos Cartéis (Bundeskartellamt - BKartA) é a autoridade antitruste, especializada em proteção da concorrência da Alemanha. É uma administração federal de nível superior que se reporta diretamente ao Ministério Federal de Economia e Tecnologia. O Bundeskartellamt funciona como uma autoridade federal superior independente e é designado para o Ministério Federal de Economia e Tecnologia. Foi fundado para impedir posições dominantes monopolistas. Portanto, as tarefas da agência federal consistem principalmente no controle de empresas dominantes e aplicação da proibição antitruste e implementação de controle de fusões. A autoridade federal tem a oportunidade de agir contra toda a formação ilegal de cartéis antitruste e também de impor multas ou condições. No Brasil, órgão semelhante é o CADE. Confira: https://www.bundeskartellamt.de/EN/AboutUs/aboutus_node.html (nota dos tradutores).

[97] Neste sentido: Conselho de Especialistas em questões de Consumo (nota de rodapé 121), 69-77. Há também referências a modelos estrangeiros, 71-74. No entanto, tenho dúvidas de que a autoridade responsável pelo combate aos cartéis, especializada na proteção da concorrência, esteja, dada a sua composição de pessoal e a sua cultura administrativa, em condições de oferecer proteção, mesmo na medida em que isso não possa ser alcançado com conceitos que limitem o poder de mercado. No entanto, é de saudar o fato de que o Departamento Federal de Combate a Cartéis da Alemanha já esteja examinando, no âmbito de suas competências existentes, se o Facebook usou seu acesso excepcional a dados relevantes em matéria de concorrência para utilizar o poder de mercado sob a forma de abuso de condições. Ver "Background information on the Bundeskartellamt's Facebook proceedings" publicado pelo Bundeskartellamt em 19 de dezembro de 2017. (* Para ler online, acesso o link: https://bit.ly/2NjB0B6, todavia, atualizando o tema, em 6 de fevereiro de 2019, o Bundeskartellamt - BKA adotou sua tão esperada decisão para o Facebook, impondo restrições abrangentes sobre como a rede social pode coletar e processar dados de usuários. A autoridade alemã, entendeu que *de acordo com os termos e condições do Facebook, os usuários até agora só conseguiram usar a rede social sob a condição prévia de que o Facebook pudesse coletar*

das competências de monitorização, por exemplo, financiar a investigação de terceiros ou outras atividades para ampliar os conhecimentos especializados sobre os riscos relacionados com os serviços digitais e desenvolver abordagens adequadas de proteção e prevenção de riscos.

Devemos também mencionar duas ideias desenvolvidas na literatura americana. Uma proposta visa a criação de uma agência federal especial, inspirada na relativamente poderosa Administração Federal de Medicamentos, em particular para o (pré-)controle de algoritmos com perigos potenciais; ela também deve ser equipada com um apropriado poder de sanção [98]. Uma outra proposta, especificamente voltada para o uso da inteligência artificial, tem por objetivo criar uma lei específica, a "Lei para o Desenvolvimento da Inteligência Artificial" (Artificial Intelligence Development Act - AIDA). As suas normas deverão ajudar a criar uma agência cuja missão seja certificar a segurança dos sistemas de inteligência artificial. No entanto, o seu poder de impor sanções não tem necessariamente de consistir em impedir a utilização de tais sistemas se a certificação for omitida. Pode fazer mais sentido - em especial através do tratamento de dados comportamentais e econômicos - prever a diferenciação das possibilidades de reação e, em particular, criar incentivos para o uso de tais possibilidades. Por exemplo, a utilização do procedimento de certificação poderia conduzir a uma limitação da responsabilidade das empresas[99].

A necessidade de estruturas de monitoramento adequadas só pode ser enfatizada aqui. Não devem ser consideradas aqui as considerações sobre a implementação competente e organizacional, bem como sobre as necessidades e possibilidades de ancorá-las no sistema multinível europeu.

11.7 Ampliação da proteção jurisdicional

dados do usuário também fora do site do Facebook na internet ou em aplicativos para smartphone e atribuir esses dados à conta do usuário no Facebook. Todos os dados coletados no site do Facebook, por serviços de propriedade do Facebook, como por exemplo WhatsApp e Instagram e em sites de terceiros podem ser combinados e atribuídos à conta de usuário do Facebook. A decisão da autoridade abrange diferentes fontes de dados: (i) serviços de propriedade do Facebook como WhatsApp e Instagram podem continuar a coletar dados. No entanto, atribuir os dados às contas de usuário do Facebook só será possível sujeito ao consentimento voluntário dos usuários. Onde o consentimento não é dado, os dados devem permanecer no respectivo serviço e não podem ser processados em combinação com os dados do Facebook. (ii) Coletar dados de sites de terceiros e atribuí-los a uma conta de usuário do Facebook também só será possível se os usuários derem seu consentimento voluntário. Se não for concedido consentimento para dados de serviços de propriedade do Facebook e sites de terceiros, o Facebook terá que restringir substancialmente sua coleta e combinação de dados. Para maiores esclarecimentos, ver Bundeskartellamt prohibits Facebook from combining user data from different sources Background information on the Bundeskartellamt's Facebook proceeding, 7 February 2019. Disponível online com acesso livre em: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf?__blob=publicationFile&v=6 – link permanente – Nota dos tradutores).

[98] Cf., A. Tutt (Nota de rodapé 20).

[99] Para mais informações, cf., M. Scherer (nota de rodapé), 393-398.

Devem igualmente ser previstas possibilidades de um eficaz controle judicial. Tal pode igualmente ser conseguido quando se justificar o reconhecimento de segredos comerciais de empresas ou de segredos oficiais de autoridades públicas. A este respeito, a proteção judicial das pessoas adversamente afetadas pela utilização de algoritmos não tem necessariamente de ser abandonada, mas pode ser possibilitada pela introdução nos tribunais dos denominados procedimentos sigilosos[100]: as empresas são obrigadas a revelar ao tribunal algoritmos sensíveis, em particular algoritmos que podem ser utilizados para pôr em perigo a liberdade - se necessário apenas as máximas e os critérios em que se baseiam, a informação utilizada como input e, no caso dos sistemas de aprendizagem, as regras de formação utilizadas, se necessário também o tipo de utilização da análise de Big Data. No entanto, essas informações não deverão tornar-se públicas e não deverão ser acessíveis às partes no processo, ou apenas o serão numa medida limitada, mas sim ao tribunal que aprecia os problemas, que pode, contudo, se necessário, mandar proceder a um exame por peritos independentes.

A fim de assegurar uma proteção jurídica efetiva, é igualmente necessário considerar as possibilidades de alterar as formas de proteção judicial. Uma forma é ampliar o uso da ação coletiva, conforme previsto nos artigos 80 e 82 do RGPD, nos termos dos artigos 77–79, bem como § 2 alínea 2 n.º 11 em conjunção com § 3º nº 1 da Unterlassungsklagengesetzes - UKlaG*. [101] Isso não só poderia ser desenvolvido em uma ação coletiva envolvendo algarismos ou mesmo uma ação coletiva de Big Data, mas também em uma extensão desse tipo de ação judicial para o controle judicial do uso da inteligência artificial. No entanto, a definição do âmbito de aplicação e das normas de auditoria deverá colocar problemas consideráveis. A proteção jurídica pelos tribunais também pode ser possibilitada por ações coletivas, cuja facilitação é recomendada pela Comissão Europeia[102]. Na

[100] Um exemplo da legalidade da admissão de tal procedimento é o § 99 do Regimento do Tribunal Administrativo.

[*] *Lei relativa às medidas cautelares em matéria de direito do consumo e outras infrações* (http://www.gesetze-im-internet.de/uklag/). A lei alemã relativa às medidas cautelares (UKlaG) foi adoptada como parte da modernização da lei das obrigações em 2002, a fim de colocar as disposições legais formais da Lei sobre as medidas cautelares, cuja parte substancial foi transferida para os §§ 305 - 310 BGB, na sua própria base jurídica. A UKlaG serve principalmente à proteção do consumidor. Uma vez que as ações intentadas por particulares podem ser insuficientes para garantir a proteção dos consumidores contra cláusulas e condições gerais abusivas, foi criado um direito de ação coletiva independente, que apenas excepcionalmente é admissível em processos civis alemães. A lei relativa às medidas cautelares nos termos do § 15 UKlaG não se aplica ao domínio do direito do trabalho. (Nota dos tradutores)

[101] Cf., G. Spindler, Verbandsklagen und Datenschutz – das neue Verbandsklagerecht, in: Zeitschrift für Datenschutz 2016, 114-119; A. Halfmeier, Die neue Datenschutzverbandsklage, in: Neue Juristische Wochenschrift 2016, 1126-1129.

[102] Recomendação 2013/396/UE, de 11 de Junho de 2013, relativa a "Princípios comuns para as ações coletivas de proteção e os processos de indemnização em caso de violação dos direitos garantidos

Alemanha, isto pode assumir a forma de um modelo de ação declaratória - embora se destine apenas a um âmbito de aplicação restrito[103].

Além disso, as possibilidades de procedimentos extrajudiciais de resolução de litígios [104] podem ser mais amplamente utilizadas e promovidas pelas tarefas soberanas em um Estado de Direito. Tais procedimentos deverão, no entanto, ser regulamentados de modo a assegurar que os justos interesses sejam tidos em conta.

11.8 Limitar as disparidades na distribuição do poder

Os problemas que precisam de soluções incluem não apenas a disparidade na distribuição de poder entre usuários individuais e empresas, mas também a disparidade na distribuição de poder de mercado entre diferentes empresas. O grau de oligopólio em submercados de tecnologias da informação de grande importância é preocupante. A fim de limitar a concentração de poder e os riscos de abuso de poder, é necessário utilizar e melhorar a legislação antitrust[105] nacional e europeia existente, mas também criar mais legislação antitrust trans e internacionalmente eficaz.

Impõe-se igualmente a necessidade urgente de medidas eficazes, não baseadas no direito antitrust, para alargar a limitação da utilização do poder não só ao funcionamento dos mercados, mas também à salvaguarda de outros objetivos de bem-estar público. Um exemplo é a proposta do Parlamento Europeu - que ainda não foi implementada - sobre a separação entre motores de busca e outros serviços comerciais[106]. O objetivo é reduzir os riscos de utilização abusiva do poder de seleção dos motores de busca no acesso dos usuários à informação e, portanto, a possibilidade de influência unilateral das empresas de motores de busca sobre as experiências e atitudes dos usuários ou sobre a formação da opinião pública em geral.

11.9 Avaliações de impacto

No que diz respeito à proteção de dados pessoais, a legislação em matéria de proteção de dados prevê uma avaliação do impacto da proteção de dados no § 35 RGPD - bem como no § 67 BDSG (novo) para as tarefas do § 45 BDSG (novo) não

pela legislação da União" (JO L 201 de 26.7.2013, 60) (Documento do Conselho 6043/18; Kom-Dok.COM (2018) 40, final).

[103] Lei de 12 de julho de 2018 que introduz um modelo processual civil de ação judicial declaratória.

[104] Para os procedimentos já existentes da Resolução de Litígios Online, ver as notas em M. Hartung/M.-M Bues/M. Halbleib (nota de rodapé 34), 215-225.

[105] No entanto, existem novos desafios para a teoria, a prática e a ciência do direito antitruste. Veja – neste caso, por exemplo – S. Telle, Big Data und Kartellrecht. Relevanz datenbasierter Geschäftsmodelle im europäischen und deutschen Kartellrecht, in: Innovations- und Technikrecht 2017, 3-17. Uma breve visão geral sobre a importância da legislação antitruste em relação ao Big Data, cf., B. Schütze/S.N. F Hänold/orgó (nota de rodapé 98), 287-299.

[106] Parlamento Europeu, resolução sobre o reforço dos direitos dos consumidores no mercado único digital, 2014, B8-0286/2014, n. º 15-18.

abrangidas pelo RGPD. Os responsáveis são obrigados a fazê-lo (ver artigo 4.º, n.º 7, do RGPD), ou seja, aqueles que decidem sobre as finalidades, os meios e o tratamento dos dados pessoais, e não as autoridades de supervisão soberanas. A presente avaliação de impacto diz apenas respeito à proteção de dados pessoais na medida do previsto na legislação em matéria de proteção de dados. O conteúdo das abordagens de análise e avaliação de impacto está listado no Art. 35 RGPD e §§ 45, 67 BDSG (novo). O mesmo não está orientado para as características especiais do Big Data nem para a proteção dos interesses públicos afetados pela sua utilização.

As avaliações de impacto são instrumentos importantes, em especial para a avaliação do risco[107]. Recomenda-se vivamente que sejam prescritas não só na legislação clássica em matéria de proteção de dados, mas também na utilização de megadados e, sobretudo, na utilização de inteligência artificial para aplicações que possam ser consideradas de risco. Além disso, deve ser ponderada a criação de disposições para a avaliação permanente dos riscos, uma vez que os futuros desenvolvimentos técnicos e as utilizações sociais da digitalização não são de modo algum previsíveis e, por conseguinte, exigem uma monitorização constante. No entanto, tais medidas não devem ser deixadas apenas aos responsáveis (por exemplo, artigo 35 do RGPD, embora associadas ao pedido de aconselhamento do responsável pela proteção de dados, artigo 35, nº 2, do RGPD). O resultado exige um controle público envolvendo representantes da sociedade civil.

11.10 Medidas para aperfeiçoar a cibersegurança

O desenvolvimento da digitalização e, em especial, da utilização de megadados está associado a riscos de pôr em perigo a cibersegurança, como a funcionalidade dos sistemas de tecnologias da informação[108], incluindo, em especial, as chamadas infraestruturas críticas (como hospitais, fornecedores de energia e água e sistemas de transporte). Tais riscos, que vão além do tratamento de riscos específicos de proteção de dados, podem ser justificados pelo fato de que o hardware e/ou software utilizado contém lacunas de segurança[109]. Há perigos especiais associados

[107] Cf., C. Böhret/G. Konzendorf, Handbuch Gesetzesfolgenabschätzung (GFA): Gesetze, Verordnungen, Verwaltungsvorschriften, 2001. A respeito dos riscos especiais com dados, que pode atrair a utilização da avaliação de consequências legislativas, v. também C.S. Conrad, Künstliche Intelligenz – Die Risiken für den Datenschutz, Datenschutz und Datensicherheit 2017, 744.

[108] Cf., H. Samsel, Risiken der Informationstechnologie, in: H. Pünder/A. Klafki (Ed.), Risiko und Katastrophe als Herausforderung für die Verwaltung, 2017, 121-137); T. Wischmeyer (nota de rodapé 20).

[109] Tais vulnerabilidades de segurança podem sempre ser encontradas no software. Como mostra a vulnerabilidade que ficou conhecida em janeiro de 2018 nos bilhões de processadores utilizados pela oligopolista Intel (mas também em alguns de seus concorrentes, segundo a AMD), o hardware também pode conter defeitos, mesmo aqueles que não podem ser simplesmente corrigidos por atualizações de software. Veja os relatórios no Süddeutsche Zeitung de 5 a 7 de janeiro de 2018, No. 4, 1, 27.

aos chamados ciberataques, ou seja, ataques dirigidos a redes informáticas que são importantes para infraestruturas importantes, como as que são essenciais para o fornecimento. Outra dimensão da cibersegurança é abordada quando organismos estatais ou privados organizam ciberataques para desinformar ou manipular processos decisórios (por exemplo, eleições políticas)[110].

Os ciberataques são frequentemente realizados utilizando Big Data e inteligência artificial. A este respeito, porém, a aplicabilidade dos Big Data e da inteligência artificial é bilateral: oferecem também um ponto de partida para melhorar a segurança das TI. A análise de Big Data, por exemplo, permite que sejam tomadas precauções rápidas, muitas vezes em tempo real, para detectar e combater um ataque a sistemas de TI ou processos de comunicação individuais e para limitar possíveis danos. O Big Data Analytics é particularmente capaz de detectar padrões de atividade que representam uma ameaça para o sistema de tecnologia da informação e permitir reações rápidas quando atividades incomuns são percebidas.

Os riscos à cibersegurança afetam não apenas indivíduos e empresas, mas também, e especialmente, agências governamentais. A cibersegurança não é apenas um problema nacional, mas também, e sobretudo, um problema transnacional e internacional.

Cada vez mais existem abordagens no sistema jurídico com o objetivo de aprimorar a cibersegurança. Uma vez que a circulação transfronteiras de bens, serviços e pessoas pode ser afetada por ciberataques, a UE impôs obrigações específicas aos Estados-Membros sob a forma de uma Diretiva[111]. Em termos de conteúdo, a mistura de diferentes precauções é notável. Nos termos do artigo 1º da Diretiva, devem ser tomadas várias medidas para alcançar um elevado nível comum de segurança das redes e dos sistemas informáticos na União. Estão previstas disposições para isto[*]:

- Estabelece a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação.
- Cria um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e de desenvolver a confiança entre eles.
- Cria uma rede de equipes de resposta a incidentes de segurança informática («rede de CSIRT») a fim de contribuir para o desenvolvimento da confiança entre os Estados-Membros e de promover uma cooperação operacional célere e eficaz.

[110] Para tornar mais difícil essas manipulações, Brad Smith, Presidente e Chefe do Departamento Jurídico da Microsoft, propôs uma internacional "Digital Geneva Convention", ver https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[111] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas informáticos na UE.

[*] Cf., https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148, para o texto em português (link permanente – nota dos tradutores).

- Estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais.
- Estabelece a obrigação de os Estados-Membros designarem as autoridades nacionais competentes, os pontos de contacto únicos e as CSIRT com atribuições relacionadas com a segurança das redes e dos sistemas de informação.

Na implementação da diretiva, o legislador federal alemão modificou a "Lei da Agência Federal para a Segurança da Informação" (BSI-Gesetz) através de uma alteração datada de 23.06.2017[112].

Convém sublinhar que estas bases jurídicas prevêem igualmente regras específicas para os operadores de "serviços essenciais", ou seja, organismos públicos ou privados que prestam um serviço informático essencial para a manutenção de atividades sociais e/ou econômicas críticas e que seriam manifestamente perturbados por um incidente de segurança. Isto aplica-se a setores como a aviação, o transporte ferroviário, o transporte marítimo e o transporte rodoviário. A sua vulnerabilidade aumenta significativamente com a utilização de Big Data. Ao mesmo tempo, porém, a utilização de megadados facilita - como já foi referido - a tomada de precauções adequadas para proteger a segurança das infraestruturas. Além disso, as possibilidades de criar precauções técnicas para aumentar a segurança devem ser desenvolvidas e implementadas, e o cumprimento dessas precauções deve ser controlado (segurança desde a concepção[*]).

Se as medidas de precaução acima descritas, criadas pela UE e pela República Federal da Alemanha, incluindo as competências do Serviço Federal de Segurança, são suficientes, ainda assim não podem ser negligenciadas. Avaliações contínuas e, se necessário, melhorias parecem ser indispensáveis neste contexto. Podem também ser considerados sistemas para a certificação de conceitos de segurança. Importa igualmente ter presente que estas medidas afetam apenas uma subárea da cibersegurança, ou seja, não são de modo algum suficientemente convincentes para resolver o problema.

11.11 Autorregulação e corregulação

As medidas de proteção acima referidas e outras podem ser tomadas não só através de medidas soberanas[*], mas também no âmbito da autorregulação do setor das TI ou da corregulação entre intervenientes soberanos e privados (especialmente

[112] Cf., BGBl. I 1885. (* Lei que transpõe a Diretiva [EU] 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativo a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação na União. Disponível online em: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html – nota dos tradutores).

[*] Em inglês "Security by Design" (nota dos tradutores).

[*] Veja nota dos tradutores (*) no título do item 11.6 *supra*.

privados)[113]. Até à data, porém, existem apenas abordagens limitadas para a proteção efetiva dos interesses jurídicos de terceiros ou a proteção dos interesses de ordem pública através da autorregulação do setor das TI ou da autorregulação híbrida (soberano-privada) - quer sob a forma de autorregulação social (apenas) acompanhada ou também regulada soberanamente.

Isso se aplica também às medidas de autorregulação para reduzir as deficiências de transparência acima mencionadas e para tornar mais possível a prestação de contas pública, ou às medidas para expandir os sistemas de garantia de qualidade. No entanto, a elaboração unilateral de princípios não vinculativos, bem como a elaboração unilateral de códigos de conduta pelas empresas, proporciona apenas uma proteção muito limitada ao seu cumprimento. A este respeito, a figura da "responsabilidade pelo folder" [114] (ou prospecto)* desenvolvida no contexto jurisprudencial do direito das inversões de bens & capitais poderia fornecer sugestões para uma forma de reforçar a relevância das regras de conduta publicadas pelas empresas (como as contidas nos princípios do Facebook).

Um outro elemento de proteção pode ser um código de conduta. No entanto, na medida em que decorrem exclusivamente de associações do setor das TI ou da interação de empresas individuais, existe o risco de que o seu conteúdo seja unilateral e seletivo em termos de interesses. Para contrariar esta situação, a

[113] Sobre as possibilidades de autorregulação, mas principalmente em relação à mídia tradicional, ver W. Schulz/ T. Held, Regulierte Selbstregulierung als Form modernen Regierens. Zu Fragen von Regulierung und Coregulierung, 2002; ver também, M. Latzer/N. Just/F. Saurwein/P. Slominski, Selbst- und Ko-Regulierung im Mediamatiksektor: Alternative Regulierungsformen zwischen Staat und Markt, 2002; W. Hoffmann-Riem, Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext, in: M. Fehling/U. Schliesky (Ed.), Neue Macht- und Verantwortungsstrukturen in der digitalen Welt, 2016, 27-51. Sobre a autorregulação especificamente em matéria de proteção de dados, ver R. B. Abel, Umsetzung der Selbstregulierung im Datenschutz – Probleme und Lösungen, in: Recht der Datenverarbeitung, 2003, 11-16; J. Bizer, Selbstregulierung des Datenschutzes, in: Datenschutz und Datensicherheit, 2001, 25 (1), 168 e ss.; M. Schröder, Selbstregulierung im Datenschutzrecht, in: Zeitschrift für Datenschutz 2012, 418-421.

[114] Sobre a responsabilidade pelo folder ou prospecto, cf., D. Leuering, Die Neuordnung der gesetzlichen Prospekthaftung, in: Neue Juristische Wochenschrift 2012, 1905-1910.

* Em alemão: *Prospekthaftung* (responsabilidade pelo prospecto). Obrigação estatutária dos titulares de folders (prospetos), normalmente emissores de valores mobiliários e instituições de crédito associadas, de ser solidariamente responsáveis se as informações relevantes estiverem incorretas ou incompletas no prospecto de valores mobiliários para avaliação de um valor. Cf., Gesetz über die Erstellung, Billigung und Veröffentlichung des Prospekts, der beim öffentlichen Angebot von Wertpapieren oder bei der Zulassung von Wertpapieren zum Handel an einem organisierten Markt zu veröffentlichen ist (Wertpapierprospektgesetz - WpPG), § 21, aliás, derivado do Regulamento (UE) 2017/1129 do Parlamento Europeu e do Conselho de 14 de junho de 2017, relativo ao prospeto a publicar em caso de oferta de valores mobiliários ao público ou da sua admissão à negociação num mercado regulamentado. Dito regulamento pode ser consultado em link permanente, em português, online em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32017R1129.

autorregulação pode ser sujeita a precauções materiais e processuais - quer por lei, quer por acordos internacionais - para garantir que os vários interesses em causa sejam tidos em consideração.

Para o desenvolvimento de códigos de conduta e de auto-regulamentações semelhantes, faria igualmente sentido envolver os representantes da sociedade civil que defendem os interesses dos usuários. Esses representantes poderiam igualmente dispor de poderes para controlar o cumprimento dos compromissos voluntários por parte das empresas.

O RGPD no Art. 40 – 42 fornece um conceito que pode basicamente ser usado como modelo. O objetivo é promover o desenvolvimento de regras de conduta destinadas a contribuir para a correta aplicação do regulamento pelas autoridades dos Estados-Membros e da UE. O Artigo 40º, nº 2 do RGPD enumera expressamente um grande número de áreas temáticas para as quais podem ser prestados esclarecimentos. Tais sugestões de esclarecimento pretendem ser orientações regulamentares para as regras de conduta a emitir, mas as associações ou federações não são obrigadas a emiti-las. Do mesmo modo, não são obrigados a recorrer à possibilidade adicional prevista no n.º 5 de apresentar o projeto de regras de conduta à autoridade de supervisão: Se for esse o caso, a autoridade de supervisão deve indicar num parecer se as regras de conduta são compatíveis com o regulamento. Caso existam garantias suficientes, o projeto de regras de conduta é aprovado pela autoridade (parágrafo 5). Subsequentemente, aplicar-se-ão procedimentos diferentes consoante o projeto diga respeito a atividades de tratamento em apenas um ou mais Estados-Membros (também pontos 6-8). Se os testes forem positivos, a publicação oficial terá lugar no final do procedimento (par. 6, 11). Relativamente às regras de conduta aplicáveis em vários Estados-Membros, a Comissão da UE pode mesmo decidir, através de atos de execução, que têm validade geral na UE (n.º 9). O artigo 41.o do RGPD prevê possibilidades de acreditação por organismos adequados para controlar o cumprimento das regras processuais. Para os processos de certificação de proteção de dados (bem como selos de proteção de dados e marcas de teste), ver Art. 42 RGPD.

Essas regulações, que se concentram exclusivamente na proteção de dados pessoais, podem e devem ser ampliadas, de maneira coordenada ao setor de análise e aplicação de Big Data e, em particular, às possibilidades particularmente arriscadas do uso de inteligência artificial, na medida do possível. que não digam respeito ao tratamento de dados pessoais.

11.12 Melhores Práticas, Benchmarking entre outros

Uma outra possibilidade - e isto só é mencionado em poucas palavras - é a criação de disposições, se necessário por instituições especiais, para o registo das melhores práticas e/ou o desenvolvimento de sistemas de benchmarking e, se necessário, de normas baseadas neles (por exemplo, normas para protocolos e

interfaces, mas também para a concepção de tecnologias)[115]. Os correspondentes meios de garantia da qualidade são igualmente recomendados no que se refere à observância dos interesses protegidos de terceiros, mas também do público em geral.

11.13 Proteção em relação a vigilância do Estado

A proteção contra as possibilidades específicas de coleta, análise e utilização de dados no contexto de Big Data também deve ser ampliada contra as ações das autoridades públicas, por exemplo, no que diz respeito à vigilância exercida pelas autoridades policiais e outras organizações, na Alemanha, em particular o Serviço Federal de Polícia Criminal, o Serviço Federal de Informações e o Serviço para a Proteção da Constituição[116]. Um exemplo de um domínio de proteção ainda insuficiente é a atual utilização de Big Data no domínio do policiamento preditivo (ver 6.2 supra). No entanto, há que ter igualmente em conta que a digitalização produziu novas formas de criminalidade, cuja perseguição coloca dificuldades especiais[117], pelo que devem também existir formas eficazes de prevenir e evitar perigos e de perseguir os criminosos que, ao mesmo tempo, cumpram os requisitos do Estado de Direito.

A obrigação de respeitar os imperativos do Estado de Direito em matéria de supervisão soberana continua a ser indispensável. Isto aplica-se não só às ações dentro da jurisdição nacional, mas também às intervenções relacionadas com os direitos fundamentais das autoridades nacionais fora da jurisdição nacional. Além disso, deve ser assegurado por lei ou por acordos trans- ou internacionais que tais intervenções de autoridades soberanas estrangeiras no espaço nacional ou da UE não sejam permitidas ou só sejam possíveis com as mesmas restrições, ou mesmo com restrições mais rigorosas, que as intervenções de autoridades soberanas dos Estados-Membros da UE. Devem igualmente ser impostas sanções em caso de infrações.

12. Associação com outros direitos de regulação e desenvolvimento de estruturas de governação adequadas

No início, foi feita referência à transformação digital em curso, abrangendo quase todas as áreas da vida. A análise subsequente reduziu a atenção às questões especificamente relacionadas com Big Data e Inteligência Artificial.

[115] Para a problemática da incorporação de software de código aberto em normas técnicas ou normas correspondentes, ver Aßmus/L. M. Keppeler/A. Amann, Rechtliche Implikationen der Einbettung von (Open Source-) Software in technischen Normen und Dokumenten, in: Innovations- und Technikrecht 2017, 79-85.

[116] Cf., M. Bäcker (nota de rodapé 35).

[117] Cf., C. Joerden, Big Data und Kriminalität, in: W. Hoffmann-Riem (nota de rodapé 27), 173-183; T. Singelnstein (nota de rodapé 27).

Deve sublinhar-se, no entanto, que tal abordagem significa uma redução da complexidade dos fenómenos e das necessidades e possibilidades regulamentares no domínio da digitalização. O tratamento dos dados conduz a oportunidades e riscos muito diferentes, consoante o local onde são tratados e onde e para que fins são utilizados os conhecimentos e as possibilidades de controle adquiridos com a ajuda dos dados: no domínio da administração pública e administração da justiça ou dos serviços jurídicos prestados a título privado, nos cuidados de saúde (telemedicina, utilização de nanotecnologias), na exploração de infraestruturas (eventualmente vitais) (por exemplo, para o aprovisionamento energético), na gestão dos fluxos de tráfego, na logística, na produção industrial, nas medidas para assegurar a sustentabilidade do consumo de recursos, em casa (casa inteligente, etc.), nas atividades dos intermediários de informação e na influência que exercem sobre as atitudes dos usuários ou no desempenho de tarefas militares.[118] Aqui e noutros locais não existem apenas problemas especificamente relacionados com o tratamento de dados. Pelo contrário, a transformação digital também afeta uma série de outros problemas que vão muito além da proteção de dados, alguns dos quais já estão abrangidos por legislação regulamentar específica ou para os quais faz sentido ou é necessário introduzi-la.

A este respeito, há uma grande necessidade de clarificar de que forma as diferentes áreas do direito regulamentar podem ser coordenadas de modo a não conduzirem a contradições ou bloqueios contraproducentes, mas serem utilizadas para se otimizarem mutuamente na medida do possível. A necessidade de ter em conta a multipolaridade e multidimensionalidade dos interesses que são decisivos nos respectivos domínios de atividade já foi mencionada. Uma interação coordenada do direito da proteção de dados e do direito da concorrência com o direito regulamentar específico (como o direito do tráfego, o direito da energia, o direito médico, o direito do mercado financeiro, etc.) faz sentido e pode ser necessária. Por um lado, pode ser aconselhável modificar os regulamentos de proteção de dados em relação ao assunto em questão. Acima de tudo, porém, é importante integrar as possibilidades de aplicação criadas pela digitalização e, em especial, pelo Big Data, no âmbito da respectiva legislação regulamentar, a fim de se poder ter em conta de forma coerente as especificidades de cada domínio no impacto da regulamentação sobre as oportunidades e os riscos.

Essas disposições regulamentares podem conduzir a estruturas regulatórias relativamente complexas[119]. Para além dos requisitos de proteção de conteúdo, podem também abranger responsabilidades e procedimentos, incluindo, por exemplo, a certificação e o controle; podem prever possibilidades de controle público, se necessário também através da participação de representantes da

[118] A respeito de tais possibilidades, v. também M. Hildebrandt (nota de rodapé 34).

[119] Para o conteúdo das estruturas regulatórias em geral, veja W. Hoffmann-Riem (nota de rodapé 42), 9-12.

sociedade civil, e podem desenvolver ainda mais os pré-requisitos para a proteção judicial e o controle do Estado.

A concepção, o desenvolvimento, a elaboração e a aplicação dessa regulamentação são difíceis devido à limitada previsibilidade do futuro desenvolvimento da digitalização e das suas consequências, mas, em última análise, colocam um desafio semelhante ao que existia e continua a existir noutras áreas da utilização dos direitos para influenciar os processos de inovação[120].

Também se espera que muitos intervenientes manifestem uma resistência considerável às medidas destinadas a regulamentar a utilização de Big Data, Inteligência Artificial e outras tecnologias digitais de alto risco. Os críticos da regulação neste domínio, por exemplo, apontam para aquilo que veem como restrições desnecessárias à liberdade, a complicação das inovações tecnológicas e sociais, o enfraquecimento das forças de autorregeneração do mercado, os riscos de burocratização e muito mais. Muitas vezes exigem que o desenvolvimento seja deixado à autodeterminação das empresas e de outros atores.

Por outro lado, há que dizer que, tendo em conta as oportunidades e os riscos associados à digitalização, bem como a possibilidade de afirmação unilateral de interesses e assimetrias de poder no setor das TI, não se podem esperar medidas de autorregulação eficazes que salvaguardem de forma equilibrada o bem-estar individual e público. O direito soberano responsável e aplicado é indispensável como contrapeso ao poder privado e para controlar o poder estatal no vasto âmbito dos megadados, incluindo a inteligência artificial. O direito do Estado pode e deve também ser utilizado para contornar a auto-organização ou a autorregulação das empresas ou associações (autorregulação regulada, ver ponto 11.11).

No entanto, as precauções regulatórias prometem pouco sucesso se dependerem principalmente das instituições de comando e coerção que tradicionalmente têm estado na vanguarda da regulação. Em alguns domínios (por exemplo, para prevenir e evitar situações de perigo), é indispensável um direito imperativo e transfronteiriço, mas só de forma limitada faz sentido e é eficaz em domínios inovadores que exigem criatividade e vontade de cooperação por parte dos intervenientes. Pelo contrário, devem ser previstos, sempre que possível, incentivos para uma melhor concepção tecnológica, a abertura do acesso e possibilidades de utilização de ensaios, como a certificação. O objetivo deve ser uma lei adaptada à respectiva área problemática, que respeite as suas condições contextuais e, se possível, seja sensível e adaptável às condições iniciais e de desenvolvimento[121]. Em muitos casos, recomenda-se uma governança em rede que usa diferentes modos de governação, para além do modo de coordenação-mercado, os modos-negociação, contrato ou rede, bem como a hierarquia suplementar, mas também o novo modo de governação em matéria de controle digital

[120] Cf., W. Hoffmann-Riem (nota de rodapé 42).

[121] Cf., K. Bizer/M. Führ/C. Hüttig (Ed.), Responsive Regulierung, 2002. Veja também o "clássico" P. Nonet/ P. Selznick, Law and Society in Transition: Toward Responsive Law, 1978.

(regulamentação algorítmica)[122] disponível através da utilização das possibilidades de digitalização, por exemplo através de um desenho tecnológico alinhado de forma correspondente.

As regras relativas ao desenvolvimento e à utilização de tecnologias, infraestruturas e serviços digitais têm um êxito limitado devido às aplicações transnacionais, se permanecerem limitadas ao nível nacional. No entanto, tais regras não são insignificantes, especialmente porque podem fazer uso das culturas de tomada de decisão e das instituições comprovadas desenvolvidas na legislação nacional. Eles também podem servir como um campo experimental para testar a adequação das abordagens regulatórias e como um possível modelo para regulamentos em outros sistemas jurídicos.

Os regulamentos da UE têm também um campo de atuação territorialmente delimitado, mas também afetam um campo de atividade atrativo para as empresas não europeias, devido à dimensão e eficiência do espaço econômico e tecnológico europeu. Isto deve ser utilizado pelos decisores nacionais e da UE para impor as normas jurídicas aplicáveis às empresas que estão sujeitas a requisitos legais menos exigentes nos seus "países de origem" - como, em alguns casos, as empresas americanas que dominam o setor das TI em particular. Se (têm de) se envolver na regulamentação da UE, isso também pode ser um incentivo para que observem essas regras noutras partes do mundo.

No entanto, devem ser envidados esforços adicionais para introduzir instrumentos regulamentares transnacionais e globalmente eficazes com base nas convenções internacionais correspondentes[123]. São necessários novos conceitos e instituições para a governação transnacional no setor das TI, orientados para a cooperação com as várias partes interessadas, ou seja, também para a cooperação entre atores e organizações estatais, associações e empresas do setor das TI, bem como organizações não governamentais (ONG)[124]. No entanto, isso deve ter lugar num quadro jurídico que vise a realização de uma salvaguarda equilibrada dos vários interesses em causa, cuja criação não é de esperar sem uma legislação de Estado, ou pelo menos corresponsável, associada a precauções de aplicação sustentáveis.

13. Anexo - Dados coletados pelo Facebook para fins de publicidade direcionada

01. LUGAR

[122] Cf., nota de rodapé 11 supra.

[123] Cf., A. Arnauld, Big Data, Internet und das Völkerrecht, in: W. Hoffmann-Riem (nota de rodapé 27), 117-124.

[124] Até à presente data, as abordagens a esta questão têm estado disponíveis apenas sob uma forma não vinculativa. Um exemplo é o NETmundial-Multistakeholder-Statement de 24 de abril de 2014, que estabelece um conjunto de regras para o "Internet Governance Principles", e um "Roadmap for the future Evolution of the Internet Governance Ecosystem", disponível para consulta online em: https://www.alainet.org/images/NETmundial-Multistakeholder-Document.pdf.

02. IDADE
03. GERAÇÃO
04. SEXO
05. LÍNGUA
06. NÍVEL DE INSTRUÇÃO
07. SETOR DA FORMAÇÃO
08 ESCOLA
09. FILIAÇÃO ÉTNICA
10. RENDIMENTOS E CAPITAIS PRÓPRIOS
11. PROPRIEDADE E TIPO DE HABITAÇÃO
12. VALOR DA HABITAÇÃO
13. DIMENSÃO DA PROPRIEDADE
14. TAMANHO DA CASA EM METROS QUADRADOS
15 ANO EM QUE A CASA FOI CONSTRUÍDA
16. COMPOSIÇÃO DO AGREGADO FAMILIAR
17. USUÁRIOS QUE TÊM UM ANIVERSÁRIO DENTRO DE 30 DIAS
18. USUÁRIOS QUE ESTÃO DISTANTES DA SUA FAMÍLIA OU CIDADE NATAL
19. USUÁRIOS QUE SÃO AMIGOS DE ALGUÉM QUE TEM UM ANIVERSÁRIO, É RECÉM-CASADO OU NOIVO, ACABOU DE SE MUDAR OU ESTÁ PRESTES A FAZER ANIVERSÁRIO
20. USUÁRIOS EM RELAÇÕES DE LONGA DISTÂNCIA
21. USUÁRIOS EM NOVOS RELACIONAMENTOS
22. USUÁRIOS COM NOVOS EMPREGOS
23. USUÁRIOS RECÉM-CONTRATADOS
24. USUÁRIOS RECÉM-CASADOS
25. USUÁRIOS QUE SE MOVERAM RECENTEMENTE
26. USUÁRIOS QUE ESTÃO PRESTES A TER UM ANIVERSÁRIO
27. PAIS
28. PAIS EXPECTANTES
29. MATRIZES DIVIDIDAS EM TIPOS ("FUTEBOL, MODA", ETC.)
30. USUÁRIOS COM PROBABILIDADE DE SEREM POLITICAMENTE ATIVOS
31. CONSERVADORES E LIBERAIS
32. ESTADO DA RELAÇÃO
33. EMPREGADOR
34. INDÚSTRIA
35. TÍTULO PROFISSIONAL
36. TIPO DE FUNÇÕES
37. JUROS
38. USUÁRIOS QUE POSSUEM UMA MOTOCICLETA
39. USUÁRIOS QUE PLANEJAM COMPRAR UM CARRO (QUE TIPO/MARCA E QUANDO)
40. USUÁRIOS QUE ADQUIRIRAM RECENTEMENTE PEÇAS OU ACESSÓRIOS PARA AUTOMÓVEIS

41. USUÁRIOS SUSCEPTÍVEIS DE NECESSITAREM DE PEÇAS OU SERVIÇOS PARA AUTOMÓVEIS
42. TIPO E MARCA DO CARRO QUE VOCÊ DIRIGE
43. ANO EM QUE O CARRO FOI COMPRADO
44. IDADE DO VEÍCULO
45. QUANTO DINHEIRO O USUÁRIO PODE GASTAR EM SEU PRÓXIMO CARRO
46. ONDE O USUÁRIO PROVAVELMENTE IRÁ COMPRAR SEU PRÓXIMO CARRO
47. QUANTOS TRABALHADORES TEM A PRÓPRIA EMPRESA
48. USUÁRIOS QUE TÊM PEQUENAS EMPRESAS
49. USUÁRIOS QUE SÃO GERENTES OU EXECUTIVOS
50. USUÁRIOS QUE DOARAM PARA CARIDADE (SUBDIVIDIDOS POR TIPO)
51. SISTEMA OPERATIVO
52. USUÁRIOS JOGANDO JOGOS DE BROWSER
53. USUÁRIOS QUE POSSUEM UM CONSOLE DE JOGOS
54. USUÁRIOS QUE CRIARAM UM EVENTO NO FACEBOOK
55. USUÁRIOS QUE USARAM PAGAMENTOS DO FACEBOOK
56. USUÁRIOS QUE GASTARAM MAIS DO QUE O NORMAL ATRAVÉS DE PAGAMENTOS DO FACEBOOK
57. USUÁRIOS QUE SÃO ADMINISTRADORES DE UMA PÁGINA DO FACEBOOK
58. USUÁRIOS QUE CARREGARAM RECENTEMENTE UMA FOTO NO FACEBOOK
59. NAVEGADOR DE INTERNET
60. PROVEDOR DE E-MAIL
61. "ADOTANTES PRECOCES" E "ADOTANTES TARDIOS" DE TECNOLOGIAS
62. EMIGRANTES (POR PAÍS DE ORIGEM)
63. USUÁRIOS PERTENCENTES A UM BANCO COOPERATIVO OU A UM BANCO NACIONAL OU REGIONAL
64. USUÁRIOS QUE SÃO INVESTIDORES (ORDENADOS POR TIPO DE INVESTIMENTO)
65. NÚMERO DE EMPRÉSTIMOS
66. USUÁRIOS QUE USAM ATIVAMENTE UM CARTÃO DE CRÉDITO
TIPO DE CARTÃO DE CRÉDITO
68. USUÁRIOS QUE POSSUEM UM CARTÃO DE DÉBITO
69. USUÁRIOS QUE TÊM CRÉDITO EM SEU CARTÃO DE CRÉDITO
70. USUÁRIOS OUVINDO RÁDIO
71. PROGRAMAS DE TV PREFERIDOS
72. USUÁRIOS QUE UTILIZAM UM DISPOSITIVO MÓVEL (POR MARCA)
73. TIPO DE LIGAÇÃO À INTERNET
74. USUÁRIOS QUE ADQUIRIRAM RECENTEMENTE UM TABLET OU SMARTPHONE
75. USUÁRIOS QUE UTILIZAM A INTERNET COM UM SMARTPHONE OU UM TABLET
76. USUÁRIOS QUE USAM CUPONS
77. TIPOS DE VESTUÁRIO COMPRADO PELO AGREGADO FAMILIAR DO USUÁRIO.
78. O PERÍODO DO ANO EM QUE O AGREGADO FAMILIAR DO USUÁRIO COMPRA MAIS

79. USUÁRIOS QUE COMPRAM "MUITO" DE CERVEJA, VINHO OU BEBIDAS ESPIRITUOSAS
80. USUÁRIOS QUE COMPRAM ALIMENTOS (E DE QUE TIPO)
81. USUÁRIO COMPRANDO PRODUTOS COSMÉTICOS
82. USUÁRIOS QUE ADQUIREM MEDICAMENTOS PARA ALERGIAS, GRIPE, ANALGÉSICOS E OUTROS MEDICAMENTOS NÃO SUJEITOS A RECEITA MÉDICA
83. USUÁRIOS QUE GASTAM DINHEIRO EM ARTIGOS DOMÉSTICOS
84. USUÁRIOS QUE GASTAM DINHEIRO EM PRODUTOS PARA CRIANÇAS OU ANIMAIS DE ESTIMAÇÃO (E QUE TIPO DE ANIMAL DE ESTIMAÇÃO)
85. USUÁRIOS CUJO AGREGADO FAMILIAR COMPRA MAIS DO QUE O HABITUAL
86. USUÁRIOS QUE TENDEM A FAZER COMPRAS ON-LINE (OU OFF-LINE)
87. TIPOS DE RESTAURANTES EM QUE O USUÁRIO COME
88. TIPOS DE LOJAS EM QUE O USUÁRIO FAZ COMPRAS
89. USUÁRIOS "SUSCETÍVEIS" A OFERTAS DE EMPRESAS QUE OFERECEM SEGURO AUTOMÓVEL ONLINE, ENSINO SUPERIOR OU HIPOTECAS, CARTÕES DE DÉBITO PRÉ-PAGOS E TELEVISÃO POR SATÉLITE
90. QUANTO TEMPO O USUÁRIO JÁ VIVEU EM SUA CASA
91. USUÁRIOS PROVAVELMENTE SE MUDARÃO EM BREVE
92. USUÁRIOS INTERESSADOS NOS JOGOS OLÍMPICOS, CRÍQUETE OU RAMADÃO
93. USUÁRIOS QUE VIAJAM COM FREQUÊNCIA (NEGÓCIOS OU PARTICULARES)
94. USUÁRIOS QUE SE DESLOCAM PARA O TRABALHO
95. QUE TIPO DE FÉRIAS OS LIVROS DO USUÁRIO
96. USUÁRIOS RETORNANDO RECENTEMENTE DE UMA VIAGEM
97. USUÁRIOS QUE USARAM RECENTEMENTE UM APLICATIVO DE VIAGEM
98. USUÁRIOS QUE TÊM DIREITO A UMA CASA DE FÉRIAS