A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio[1]

The Fundamental Legal Protection of Confidentiality and Integrity of Informational Technical Systems of Own Use

PROF. DR. WOLFGANG HOFFMANN-RIEM[2]
Bucerius Law School.

Italo Roberto Fuhrmann (Trad.)[3]

Jacqueline de Souza Abreu (Rev. Técnica)[4]

RESUMO: O artigo insere a decisão do Tribunal Constitucional Federal da Alemanha sobre a assim chamada busca online (Online-Durchsuchung) no contexto mais abrangente do desenvolvimento das tecnologias da informação e da sua utilização desde o julgamento do caso da Lei do Recenseamento, bem como elabora as especificidades do novo direito fundamental.

ABSTRACT: The article inserts the German constitutional court decision on the so-called Online Search in the broader context of the development of information technology and its use since the Census Case, as well as elaborates on the specifics of the new fundamental right.

SUMÁRIO: I – O início da jurisprudência do censo e o seu significado contínuo; II – Mudanças dos riscos e das oportunidades por meio das tecnologias da comunicação; II.1 Oportunidades e riscos; II.2 Necessidades e possibilidades de proteção; III – Em especial: proteção da confiança nos

1 O artigo é a versão revisada e ampliada de uma palestra na conferência de proteção de dados da Friedrich-Ebert-Stiftung, realizada em Berlim, em 1º de julho de 2008. Os agradecimentos por valiosas sugestões vão para Marion Albers, Matthias Bäcker e Ulf Buermeyer.

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

3 Orcid: https://orcid.org/0000-0002-3914-8200.

4 Orcid: https://orcid.org/0000-0003-0450-4102.

sistemas técnicos de informação de uso próprio; III.1 Proteção da confiança; III.2 Relevância da personalidade; IV – Abordagens para a proteção de direitos fundamentais; IV.1 Defesa e proteção; IV.2 Normas relevantes de direitos fundamentais; IV.2.a Sigilo das telecomunicações; IV.2.b Proteção do domicílio; IV.2.c Direito fundamental à proteção da personalidade; V – Em especial: a garantia jurídico-fundamental da confidencialidade e da integridade dos sistemas técnicos de informação de uso próprio; V.1 O ponto de partida; V.2 Novas dimensões da necessidade protetiva; V.2.a Amplitude da intervenção relativa à personalidade; V.2.b Sobre dados gerados pelo sistema; V.2.c Criação de novas imagens da personalidade de nova profundidade e amplitude; V.2.d Risco de falsificação de dados; V.2.e Neutralização das possibilidades de autoproteção; V.2.f Possibilidade de acesso de terceiros; V.2.g Grande variação de pessoas envolvidas; V.3 Esclarecimento da peculiaridade da situação de risco e da respectiva proteção de direitos fundamentais pelo Tribunal Constitucional Federal da Alemanha; V.3.a Diferenciação ao nível do âmbito de proteção; V.3.b Reação à especial qualidade do risco; V.3.c Delimitação com relação ao direito à autodeterminação informativa; V.3.d Necessidade de outras concretizações; VI – Limites aos direitos fundamentais; VI.1 Requisitos jurídicos materiais e processuais; VI.2 Núcleo da vida privada; VII – Concorrência com outras normas de direitos fundamentais; VII.1 Intervenção no âmbito do domicílio; VII.2 Concorrência com o sigilo de telecomunicação especialmente com as TKU-Fonte; Conclusão; Posfácio.

I – O INÍCIO DA JURISPRUDÊNCIA DO CENSO E O SEU SIGNIFICADO CONTÍNUO

15 de dezembro de 1983 – há um quarto de século – foi um grande dia para a ampliação da proteção dos direitos fundamentais na Alemanha: nesta data, foi proferida a decisão do censo pelo Tribunal Constitucional Federal da Alemanha[5]. Neste contexto, foi reconhecido o "direito à autodeterminação informativa" como inerente à proteção da personalidade pelo Tribunal Constitucional. Qualquer pessoa que leia hoje a decisão deve ficar surpreendida com o fato de que um recenseamento da população, isto é, de uma coleta estatística de informações como nome, endereço, meio de sustento, profissão e outros dados[6] análogos, poderia causar uma celeuma tão grande e, ao mesmo tempo, estimular uma decisão tão inovadora.

5 BVerfGE 65, 1.

6 No julgamento do censo, o Tribunal Constitucional usou o termo "dados" em um contexto para o qual a literatura de tecnologia da informação usa parcialmente o termo "informação"; sobre isso, ver, por todos, Albers, Informationelle Selbstbestimmung, 2005, p. 87 e ss.; Vesting, in: Hoffmann-Riem/Schmidt-Aßmann/Vosskuhle (Org.), Grundlagen des Verwaltungsrechts vol. 2, II (2008), § 20 número de margem 11 e ss. A seguir, o termo dados continuará a ser utilizado de acordo com o exercício na literatura jurídica, mesmo na medida em que o termo informação seja utilizado na literatura de tecnologia da informação/ciência. Dados são caracteres objetivados, informações com conteúdos significativos formados pelos destinatários ou em sistemas de comunicação (Cf., por exemplo, Albers, op. cit., p. 141 e ss.). A proteção de dados é uma dimensão protetora do direito fundamental à autodeterminação informativa, bem como o direito fundamental à proteção da confidencialidade e da integridade dos próprios sistemas de tecnologia da informação, porém, em última análise, os dados são protegidos em virtude da informação transportado com ele.

Nesta senda, pode ter desempenhado um papel a circunstância de que o ano de 1984, o mesmo que Orwell tinha escolhido como título de seu livro numa perspectiva futurista acerca dos perigos do Estado de vigilância através do "Big Brother", estava por vir e inspirou as fantasias. Naquele tempo, a tecnologia computacional ainda estava no seu início. O processamento de dados era realizado em grande medida por grandes computadores centrais, que eram pesados e volumosos, caros e, sobretudo, lentos e com pouca capacidade de armazenamento se comparados aos dias de hoje. Um computador com boa capacidade funcional e de preço acessível para todos – como hoje o PC – estava apenas no começo do desenvolvimento, e as utilizações, tal como hoje o smartphone possibilita, eram, quando muito, objeto de fantasia. Para o armazenamento de dados, que hoje um pendrive pode realizar, eram necessárias grandes máquinas imóveis. Por conseguinte, a consciência ainda não tinha se formado acerca das grandes oportunidades comunicativas de ação que o computador viria a possibilitar nos próximos anos, especialmente graças à rede internacional também de computadores privados e ao desenvolvimento da internet. O que estava em primeiro plano na discussão pública não eram tais oportunidades, mas as ameaças à liberdade por meio do levantamento de dados e seu processamento pelo Estado. Embora os dados levantados através do censo devessem permanecer anônimos, foi discutido o risco de sua individualização e o perigo associado de sua utilização indevida.

Na dogmática dos direitos fundamentais, tratava-se de uma ativação da proteção de um direito fundamental de defesa, que primeiro necessitaria ganhar contornos. O Tribunal Constitucional Federal da Alemanha conseguiu resumir, em poucas palavras, a reflexão fundamental, que, neste meio-tempo, não perdeu em nada do seu significado[7]: o direito geral da personalidade garantido no art. 2º, § 1º, c/c art. 1º, § 1º, da LF[8] poderia

> igualmente ganhar significado em relação aos modernos desenvolvimentos e às novas ameaças à personalidade humana a eles associadas. As concretizações realizadas até então pela jurisprudência não descreviam de forma conclusiva o conteúdo do direito de personalidade. Ele abrange também a

7 As seguintes citações são derivadas do BVerfGE 65, 1, 41-44 (supressões não são registradas).

8 Se é necessário e adequado usar também o art. 1º, § 1º, da Lei Fundamental como uma justificativa para o direito geral de personalidade, faz-se referência aos argumentos consideráveis em Britz, Freie Entfaltung durch Self-Presentation, 2007, em especial p. 25 e ss. Em qualquer caso, deve ser necessário derivar a proteção de dados do art. 2º, § 1º, da Lei Fundamental, na medida em que a proteção da personalidade relacionada com a dignidade humana não seja afetada, a menos que outros direitos fundamentais – como os arts. 12 e 14 da Lei Fundamental – não sejam aplicáveis.

> prerrogativa do indivíduo, decorrente das reflexões da autodeterminação, de decidir por si mesmo quando e dentro de quais limites os fatos pessoais da vida são revelados. Este direito à "autodeterminação informativa" não é garantido sem limites. O indivíduo não tem um direito no sentido de um domínio absoluto e ilimitado sobre "seus" dados; ele é, ao contrário, uma personalidade que se desenvolve dentro da comunidade social e que depende da comunicação.

A dogmática da decisão baseada nos direitos de defesa classificou a atividade do Estado como uma intervenção numa posição jurídica individual do sujeito, que, em última análise, funcionou como um direito a um dado próprio[9], cuja divulgação e utilização o indivíduo deveria poder livremente decidir – ainda que fosse reconhecida uma vinculação a contextos sociais. Uma vez que se tratava da defesa contra uma intervenção estatal, a decisão se assentou na relação entre o Estado e o cidadão.

Tendo em vista a necessidade aparentemente ilimitada de informações do Estado, ainda há aqui uma necessidade contínua de proteção. Isto é demonstrado, por exemplo, pelas muitas autorizações de acesso aos dados no interesse de garantir a segurança pública e a persecução criminal, que são encontrados em número crescente nas leis policiais e de proteção da constituição, bem como nas normas de processo penal e, em particular, as que foram criadas como resultado do 11.09.2001 como um meio (também) de combate ao terrorismo. O fato de que uma série dessas autorizações, ou pelo menos o tratamento delas no caso concreto, foram vistas nos últimos anos como inconstitucionais pelo BVerfG – e, em especial, como uma violação do direito fundamental à autodeterminação informativa[10] – sinaliza a contínua importância da proteção dos direitos de defesa.

---

9 De modo crítico, por exemplo, Hoffmann-Riem AöR 123 (1998), 513, 520 f.m.w. Indicações. Crítica fundamental da construção do Tribunal Constitucional, especialmente em Albers (nota 2), por exemplo, p. 238 e passim. A ideia do direito aos próprios dados é ainda mais inadequada quando se trata de dados sobre informações relativas ao comportamento de várias pessoas sem que os interesses de uma das pessoas em causa sejam juridicamente dignos de proteção. Torna-se ainda mais difícil com a atribuição de um dado a uma pessoa se o seu valor informativo deriva da combinação com outros dados que são ou foram gerados por outras pessoas.

10 Cf., em especial, BVerfGE 115, 320 e ss. (busca computadorizada) e BVerfG, acórdão de 11 de maio de 2008 – 1 BvR 2074/05, 1 BvR 1254/07 = NJW 2008, 1505 e ss. (registro automático de placas).

II – MUDANÇAS DOS RISCOS E DAS OPORTUNIDADES POR MEIO DAS TECNOLOGIAS DA COMUNICAÇÃO

II.1 Oportunidades e riscos

Em comparação com a época do julgamento do caso do censo, o nível de risco da situação mudou intensamente, assim como aumentaram enormemente as oportunidades de uso comunicativo da eletrônica para o desenvolvimento individual e coletivo. Praticamente qualquer pessoa hoje tem acesso a computadores com boa capacidade; cerca de 35 milhões de alemães utilizam o sistema global de rede da internet. Em julho de 2008, havia no mundo mais de 860 milhões de usuários de internet.

O que é característico não é mais o armazenamento centralizado de dados, mas sim usos descentralizados e a rede de sistemas de computação altamente eficientes muitas vezes de acesso global. A digitalização em conjunto com a tecnologia computacional – também em vista da globalização – trouxe uma evolução comunicativa, cuja importância para o desenvolvimento social não é inferior à da revolução industrial do século XIX. Computadores grandes e pequenos e as respectivas infraestruturas comunicativas das técnicas de informação se tornaram em forças produtivas centrais em praticamente todas as esferas da vida, seja para o desenvolvimento da vida privada, seja para o cumprimento de tarefas por parte do Estado e da economia por parte de empresas. As tecnologias de comunicação moldam o exercício real dos direitos fundamentais em praticamente todos os ambientes sociais[11]. Muitas das tecnologias e dos serviços eram desconhecidos à época da decisão do censo, por exemplo, ISDN, RFID, WLAN, UMTS; serviços como o e-commerce, o governo eletrônico, os sistemas de navegação; as redes sociais, como StudiVZ, comunidades virtuais como o Second Life, ou mesmo os métodos de investigação como o kfz-Scanning ou a busca on-line.

O Estado é apenas, de forma limitada, o promotor e garante da capacidade funcional das infraestruturas técnicas de informação, de resto, e mesmo principalmente, são as empresas privadas, incluindo aquelas com poder global – como Google, Microsoft ou as grandes empresas de telecomuni-

11 Sobre a computação ubíqua (o processamento de dados ubíquo), ver, por todos, Kühling Die Verwaltung 40 (2007), 153 e ss. Da mesma forma, as contribuições em Roßnagel/Sommerlatte/Wienand (Org.), Digitale Visionen – zur Gestaltung ubiquitous information technologies, 2008 e em Mattern (Org.), The Informatization of Everyday Life – Living in Smart Environments, 2007.

cações. Entre as várias empresas, e em relação ao cidadão, mas também na relação entre as empresas e o Estado, existem consideráveis assimetrias de poder. O fato de que o uso do poder, e, portanto, os riscos do abuso de poder não estão de forma alguma limitados ao Estado, está se tornando cada vez mais aparente para o público, por exemplo, quando é discutida a profusão de dados e possibilidades de seleção que o Google, por exemplo, tem à sua disposição[12], ou quando escândalos são descobertos, como o uso dos dados de conexão dos clientes da Deutsche Telekom para a vigilância dos próprios funcionários[13], ou a venda ilegal de dados bancários[14]. Ao mesmo tempo, no entanto, o Estado tem acesso aos dados, especialmente no âmbito da prevenção e combate a perigos, bem como da persecução penal, de modo que a proteção contra tais violações também deva ser garantida.

II.2 Necessidades e possibilidades de proteção

Os direitos fundamentais, em particular a proteção dos direitos da personalidade, a liberdade de comunicação e a proteção da residência, são orientados para a proteção contra intervenções do Estado, mas também contra intervenções da liberdade através de privados. Em especial, a liberdade de desenvolvimento comunicativo está afetada. A liberdade de comunicação é uma liberdade que é usada em combinação com outras liberdades[15]. A este respeito, a posição individual só pode ser descrita a partir da relação social. Um pensamento dogmático dos direitos fundamentais centrado no indivíduo "solitário" não poderia captar adequadamente as dimensões sociais da liberdade de comunicação e, portanto, as exigências de proteção a ela relacionadas.

Na medida em que a comunicação pessoal é estruturada em termos tecnológicos, esta requer uma proteção de direitos fundamentais efetiva também no que se refere à proteção da infraestrutura tecnológica da comunicação e da sua utilização concreta, uma vez que isso está relacionado com a liberdade do indivíduo. A capacidade funcional não tem apenas um lado técnico, mas também um lado social, que pode ser influenciado de forma normativa, por exemplo, assegurando a liberdade de acesso, a liber-

12 Cf., por todos, Maurer Informatik Spektrum 30 (2007), 273 e ss.

13 Acerca do assim chamado escândalo da Telekom, v. Süddeutsche Zeitung em 29.05.2008, p. 2, assim como do dia 30.05.2008, p. 1, e Scherer MMR 2008, 433 e ss.

14 Cf., por todos, Dams Die Welt em 18.08.2008.

15 Para obter informações gerais sobre este conceito, ver, em especial, Suhr, Entfaltung des Menschen durch die Menschen, 1976; (Org.), EuGRZ 1984, 529, 537. Cf. igualmente Albers (nota 2) e Britz (nota 4), p. 45 e ss.

dade de manipulação, e geralmente através de proteção contra o uso ou mesmo abuso de poder. As diversas dimensões da capacidade funcional referem-se a diferentes potenciais de perigo e vulnerabilidades, assim como a diferentes atores que salvaguardam ou põem em perigo a capacidade funcional. Por isso são necessários conceitos multipolares e multidimensionais de proteção da liberdade.

O Estado só pode assegurar de maneira limitada o funcionamento das infraestruturas de comunicação – não apenas por conta do alcance global da rede, mas também pelo domínio de atores privados na criação e manutenção das redes mediante prestação de serviços. Também se situam, neste contexto, os atores que estabelecem suas próprias leis (como, por exemplo, ICANN)[16]. Nada obstante, o Estado pode utilizar o seu poder regulamentar dentro do âmbito das normas por ele estabelecido e ampliado, eventualmente, por atos jurídicos interestatais.

A asseguração das condições reais da liberdade de conduta, em especial da liberdade comunicativa em relações conectadas tecnologicamente, não pode ser alcançada tão somente por meio do controle normativo estatal (ou privado) da conduta, mas igualmente por meio de outras medidas[17], como, por exemplo, através de exigências legais que afetem a forma como o sistema de comunicação é configurado, ou que possibilitem a proteção de dados e a autoproteção tecnológica, por exemplo, através da criptografia. Neste contexto, o Estado pode conceder incentivos, se necessário também por meio de proibições e imperativos que podem levar à ativação de funções distintas de proteção. Isto porque a proteção de dados direcionada, tanto quanto possível, para o paradigma da autodeterminação, e não apenas na definição do objetivo de proteção, mas também nas precauções de proteção, atinge seus limites factuais – e normativos – onde o indivíduo carece dos meios de proteção ou conscientização da necessidade de proteção de seus dados pessoais[18].

16 A "Internet Corporation for Assigned Names and Numbers", com sede em Marina del Rey (Califórnia), administra as principais estruturas da internet, nomeadamente, entre outras, a atribuição de blocos de endereços IP (os chamados espaços de endereço) e o servidor DNS central, que atua como uma "lista telefônica" da internet, convertendo as informações de endereço textual (por exemplo, www.bundesverfassungsgericht.de) em endereços IP (no exemplo: 134,96. 83. 81).

17 Cf. Albers (nota de rodapé 2), por exemplo, p. 466 e ss., 544 e ss.

18 A diferença entre a motivação das massas que se opunham ao censo dos anos oitenta, por um lado, e a vontade que hoje é generalizada de divulgar até os detalhes mais privados nas redes sociais (como alunos/StudiVZ), nos programas de fidelização (por exemplo, Payback) e portais de internet, além disso, limita as chances de realização de auxílio estatal para autoproteção, mas não o torna dispensável como uma oferta – ver também abaixo V 2 d.

III – EM ESPECIAL: PROTEÇÃO DA CONFIANÇA NOS SISTEMAS TÉCNICOS DE INFORMAÇÃO DE USO PRÓPRIO

Atualmente, pode-se observar que as infraestruturas técnicas da informação[19] e comunicação coletam e processam[20] cada vez mais dados pessoais, mesmo em computadores de uso próprio, que são utilizados, por exemplo, como arquivo para informações a serem retidas, como um auxílio ao realizar suas próprias tarefas (escrita, aritmética, de gestão), como meio de entretenimento (jogos de computador, biblioteca digital, biblioteca de áudio, biblioteca de vídeo) ou para controle (remoto) de sistemas de gestão doméstica em "casas inteligentes"[21], bem como para criar os chamados veículos inteligentes[22] ("Internet das Coisas")[23]. No uso online, o computador está conectado em rede com outros computadores, e os dados contidos ou gerados nele podem ser eventualmente utilizados em outros computadores. A integração em redes, em particular na internet global, permite, para além do acesso aos dados lá disponíveis, os serviços oferecidos ao trabalhar com o próprio computador, embora muitas vezes não seja conhecido do usuário qual software ainda está "a seu serviço" ou o que é utilizado para acesso às suas informações. Se – como é de se esperar – cada vez mais no futuro crescerem juntos os usos fornecidos com o software no computador utilizado (a chamada "cloud computing"[24] ou "services in the cloud"), sua propagação e diversidade, assim como a falta de controle, continuarão aumentando para

19 Para as perspectivas de desenvolvimento, ver, por todos, Roßnagel, Datenschutz im IT, 2007, especialmente p. 26 e ss. Sobre a necessidade de uma estrutura transdisciplinar, ver Rolf, Mikropolis 2010, 2008, p. 95 e ss.

20 Cf., por todos, Kutscha NJW 2008, 1042, 1044.

21 Em sua decisão sobre buscas online, o julgamento de 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822 (disponível em: www.bundesverfassungsgericht.de), número de margem 202, já mencionado – para uma visão prática: Bayerlein-Hoppe Elektrobörse Handel 02/2004, 12 e ss. Certamente não é por acaso que a exposição internacional de rádio em Berlim fez uma reorientação conceitual em 2008, de modo que as precauções eletronicamente estruturadas para "casas inteligentes" agora também foram integradas em uma feira de comunicações.

22 Ver, especialmente, a iniciativa da União Europeia apresentada, por exemplo, no comunicado da Comissão "Para uma mobilidade mais segura, mais limpa e mais eficiente no âmbito europeu: primeiro relatório sobre a iniciativa 'Veículo Inteligente'", COM (2007), 541. Os sistemas de transporte inteligentes destinam-se, em particular, a aumentar a segurança do tráfego e a eficiência energética e a proporcionar uma maior utilização de tecnologias de informação e comunicação, que, ao mesmo tempo, transferem informações de veículo para veículo, entre veículo e infraestrutura, de veículo para sistemas de chamada de emergência (incluindo precauções com controle de localização exata). Veja também Dencker zfs 2008, 423 ff.; Vieweg, in: 45. VGT, 2007, p. 292 e ss.

23 Ullinger/ten Hompel (Org.), Internet der Dinge, 2007; Fleisch/Mattern (Org.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, 2005. Cf. também acima na nota de rodapé 7.

24 Sobre o tema, cf. David Chappell, A Short Introduction to Cloud Platforms. An enterprise-oriented view, 2008, disponível em: www.davidchappell.com. A "nuvem" representa uma metáfora para as infraestruturas complexas opacas e em constante movimento que a comunicação baseada em rede acessa sem que o usuário saiba ou mesmo seja capaz de controlá-la.

o usuário. A perda de controle é inevitável. Princípios normativos como minimização de dados e prevenção de dados (Seção 3a (1) BDSG) não se tornarão supérfluos, mas perderão parte de sua eficácia, se a infraestrutura de rede for acessada – o que é praticamente inevitável com o uso online.

O disco rígido de muitos PCs já oferece uma imagem espelhada dos interesses e das inclinações pessoais, da situação econômica, assim como do bem-estar físico e psicológico, ou mesmo do comportamento de seus usuários[25]. Porém, as informações confidenciais não estão apenas no seu próprio computador "armazenadas", mas também estão localizadas na própria rede. Quem tem acesso ao sistema de tecnologia da informação pode, em certa medida – pelo menos em parte – ter acesso ao "cérebro externalizado"[26] ou mesmo à "psique externalizada", mas também a muitas outras informações importantes da personalidade afetada. Essa "vulnerabilidade" do direito da personalidade leva a demandas por proteção, inclusive (ainda) no que diz respeito aos dados e coletas de dados a princípio conhecidos pelo usuário, mas também em relação aos dados de conteúdo gerados durante o processo de uso, bem como aos dados voláteis ou gerados permanentemente (os dados funcionais) e suas possibilidades de uso, muitas vezes não conhecidos pelo usuário. As garantias ganham relevância em termos de direitos fundamentais, na medida em que sejam necessárias para proteger a personalidade (relevância da personalidade).

III.1 Proteção da confiança

Uma proteção eficaz de tais dados e da comunicação divulgada por eles não requer apenas a proteção contra acesso, mas também abrange a confiança[27] de que o hardware e o software utilizados e, no geral, as infraestruturas comunicacionais técnicas da informação funcionem não só em termos técnicos, mas igualmente nos contextos de aplicação[28], assim como

25 Assim, por exemplo, Kutscha NJW 2008, 1043.

26 Hassemer Süddeutsche Zeitung, aos 11.06.2008, formulou: "O computador é uma parte externalizada do corpo".

27 Basicamente sobre confiança e suas dimensões, ver as contribuições de Klumpp et al. (Ed.), Informationelles trust for the information society, 2008. As muitas facetas do conceito de confiança e as teorias sobre a construção da confiança não podem ser tratadas aqui. Para diferentes perspectivas disciplinares, consulte Möllering, in: Max-Planck Institute for Social Research, anuário 2007/2008, p. 73 e ss.

28 A este respeito, trata-se também de proteção funcional, ver Hornung CR 2008, 299, 302. Do ponto de vista dos direitos fundamentais, a proteção funcional deve ser entendida como um meio de proteger a privacidade pessoal.

o usuário pode esperar[29], de modo que ele possa, nesse contexto, confiar na proteção de dados técnicos de informação armazenados ou comunicados (confiança relacionada ao sistema). Às expectativas protegidas normativamente relacionadas à confiança pertence a confidencialidade fundamental do próprio sistema de tecnologia da informação[30], que é a própria base da confidencialidade da comunicação, portanto uma proteção em face do acesso do Estado ou de terceiros[31]. As expectativas de proteção também incluem a integridade do sistema de tecnologia da informação, ou seja, a proteção contra a superação de obstáculos que protegem contra intrusões, bem como contra avarias e manipulações[32], por exemplo, contra falsificações, contra complementações por meio de outros dados ou por meio de softwares que podem manipular o manuseio de dados[33]. Também há necessidade de proteção contra manipulação do hardware utilizado, bem como contra a infiltração e manipulação dos programas que (como o sistema operacional ou o software do usuário) habilitam a funcionalidade ou oferecem acesso a terceiros ao sistema.

O Tribunal Constitucional Federal da Alemanha utiliza o conceito dos sistemas técnicos de informação como juridicamente constitucional, cujos contornos ainda precisam ser desenvolvidos, e que, em hipótese alguma, pode ser extraído de forma isolada da literatura técnica informacional. Isto deixa claro que as necessidades de proteção especial só se aplicam a sistemas complexos de tecnologia da informação, o que não ocorre com os dispositivos de controle eletrônicos que não estão em rede de tecnologia doméstica[34], mas sim com computadores pessoais em rede, telefones celulares mais complexos ou assistentes digitais pessoais (PDAs)[35]. Os requisitos de complexidade suficiente também podem ser preenchidos por um pen-

29 Cf. Volkmann DVBl. 2008, 590, 592.

30 O termo sistemas de tecnologia da informação ainda não foi definido em termos legais. O Tribunal Constitucional (nota 17) retomou-o da literatura de informática, cuja terminologia constava do regulamento jurídico impugnado na decisão em questão. Uma das futuras tarefas dogmáticas será descrever as estruturas juridicamente relevantes dos "próprios sistemas de tecnologia da informação" em mais detalhes, de uma forma que seja voltada para a relevância pessoal da proteção do sistema. Mesmo quando o Tribunal Constitucional fala em sistemas de tecnologia da informação "próprios" (ou melhor: autoutilizados), o contexto deixa claro que a proteção da personalidade é um ponto de referência decisivo para a proteção do sistema de direitos fundamentais.

31 Cf., igualmente, Britz (nota de rodapé 4), p. 77.

32 Trata-se, neste sentido, na terminologia técnica da informática também de "Security" no sentido da segurança de TI. Sobre o tema, cf. Kubicek, in: Klumpp u. a. (nota de rodapé 23), p. 17, 25 e ss.

33 Acerca da proteção da "exatidão informativa", cf. Albers (nota de rodapé 2), p. 119 e ss.; Britz (nota de rodapé 4), p. 52 e ss.

34 Cf. BVerfGE (nota de rodapé 17), número de margem 202.

35 Cf. BVerfGE (nota de rodapé 17), número de margem 194.

drive conectado ao computador ou por um disco rígido externo conectado a ele[36].

III.2 Relevância da personalidade

No entanto, o sistema técnico de informação não é protegido em termos de direitos fundamentais por sua própria vontade[37], mas apenas na medida em que sua confidencialidade e integridade tenham relevância para a personalidade[38]. Isto, por sua vez, resulta do tipo de dados que são transportados com a ajuda do sistema ou que são ou podem ser armazenados nele. A proteção de dados pretendida por meio da proteção dos sistemas técnicos de informação também se estende aos dados de relevância para a personalidade que são mantidos na memória de trabalho e armazenados temporária ou permanentemente na mídia de armazenamento do sistema (possivelmente apenas de forma indireta)[39].

Entretanto, como o usuário em regra não sabe, e nem tem como saber, quais dados pessoais ou eventualmente quais dados relativos a sua personalidade nos atuais e complexos sistemas técnicos de informação são gerados durante o processo de uso, onde e por quanto tempo são registrados (armazenados), e em quais contextos de uso e por quem são utilizados, ele praticamente não pode exercer o seu direito de autodeterminação sobre a divulgação e a utilização de tais dados – com o qual ele até agora decidiu em que medida ele poderia confiar no sigilo. A possibilidade de disposição autônoma também deixa de existir quando houver ciência da natureza dos dados, se ele estiver sobrecarregado pela autoproteção ou a autoproteção levar a perdas funcionais inaceitáveis. O ganho em possibilidades técnicas

36 Sobre o tema, em mais detalhes, Bäcker, in: Brink/Rensen (Org.), Aktuelle Rechtsprechung des Bundesverfassungsgerichts, 2009 (na edição), sob III, 2a; Böckenförde JZ 2008, 925, 929 nota de rodapé 41.

37 Neste aspecto, existem proteções complementares através de outros direitos fundamentais, como art. 12, 14, da LF. Um conceito de sistema técnico de informação baseado na proteção da propriedade ainda necessita elaboração.

38 O risco temido por Eifert NVwZ 2008, 521, 522, de que a proteção da integridade transforme a proteção dos direitos fundamentais em direito fundamental não pessoal e tecnológico, não existe se, como alega o Tribunal Constitucional, a relação de proteção de integridade ao direito fundamental à garantia da personalidade do art. 2º, § 1º c/c o art. 1º, § 1º, da LF seja preservada, mesmo que se estenda ao nível de perigo pessoal. O componente relacionado à proteção pessoal também prevê Lepsius, in: Roggan (Ed.), Online-Durchsuchungen, 2008, p. 21, 32 e ss. Quando ele descreve a nova dimensão da proteção como a "proteção desindividualizada da funcionalidade" desses sistemas e a referência de personalidade exigida pelo tribunal apenas como "área de proteção de contorno, mas não individualizante" (Op. cit., p. 35).

39 Uma visão ilustrativa do potencial de perigo e as possibilidades de acesso estatal encoberto aos sistemas de computador são dadas por Buermeyer HRRS 2007, 154 e ss.

de intercâmbio de informações corresponde a uma perda estrutural de autonomia informacional[40]. No entanto, a proteção funcional relacionada ao sistema permite – dentro de certos limites – precauções para a compensação desta perda de autonomia, porém dificilmente para a restauração da possibilidade de decisão autodeterminada sobre o tratamento dos seus próprios dados.

O paradigma[41] de assegurar a liberdade por meio da possibilidade fundamental de tomar decisões autônomas sobre acesso e uso[42] de dados, no qual o Tribunal Constitucional Federal baseia o direito de autodeterminação informacional, indica inicialmente um objetivo de proteção da liberdade, mas também se refere a possíveis formas de alcançar o objetivo por meio da autodeterminação. O direito de proteção de dados assumiu isso através de certos instrumentos, como a função do consentimento (§ 4 para. 1, § 4a BDSG), ou o pedido para utilizar as possibilidades de anonimização e pseudonimização (§ 3a BDSG). Na referência a tais instrumentos, entretanto, a proteção da personalidade se baseia em premissas empíricas que estão cada vez mais em erosão devido ao desenvolvimento da tecnologia informática, de constelações de redes e de muitos novos serviços. O direito de proteção de dados deve lidar com isso. Isto tem – apenas para citar um exemplo – consequências para a relevância da exigência do consentimento[43]. Para aquele que não pode ver sobre o que está consentindo – que não pode saber quem, o quê[44], quando e em que ocasião sobre quem sabe –, não pode autorizar outros a processar dados de maneira "informada"[45] e, portanto, autodeterminada; sem um fundamento suficiente de informação, o consentimento é reduzido a uma fórmula sem força de legitimação material ou se torna até mesmo uma ficção. Uma proteção de dados eficaz só pode se basear na possibilidade de proteção da liberdade pelos próprios titulares dos dados na medida em que estes possam exercer efetivamente esta possibilidade. Além disso, há a necessidade de mecanismos de proteção suplementares. Muitos esforços foram feitos no passado para estabelecer

40 De modo resumido, in: Sokol (Org.), Persönlichkeit im Netz: Sicherheit – Kontrolle – Transparenz, 2007, p. 4 e ss.

41 Sobre ele, v. BVerfGE 65, 1, 42 e ss.

42 Que essa competência não pode ser (mal)entendida como quase direito à propriedade, já foi acentuado (nota de rodapé 7).

43 Sobre ele, cf., por todos, Holznagel/Sonntag, in: Rossnagel (Org.), Handbuch Datenschutzrecht, 2003, p. 678 e ss., com outras indicações.

44 Neste sentido, BVerfGE 65, 1, 43.

45 Sobre o princípio do consentimento informado, v. § 4 § 1, inciso 1 BDSG, assim como art. 2 Lithdsrl.

tais mecanismos, como aqueles para a proteção da personalidade através da configuração do sistema e da tecnologia[46]. Uma vez que a pessoa envolvida é apenas, de forma limitada, o senhor do sistema e do projeto tecnológico, a proteção efetiva da privacidade pressupõe que a pessoa em questão possa geralmente confiar que tais mecanismos de proteção, na medida em que existam, serão realmente eficazes. Proteção dos direitos fundamentais da personalidade como proteção da liberdade então também exige a proteção da confiança, que vai além da proteção da confiança na possibilidade de autodeterminação decisão sobre a medida em que os dados podem ser acessados. Também deve ser assegurada a própria proteção da confiança na confidencialidade e na integridade do sistema técnico de informação ao qual o titular do direito fundamental se dirige, sem que se espere que ele possa controlá-lo.

IV – ABORDAGENS PARA A PROTEÇÃO DE DIREITOS FUNDAMENTAIS

O direito fundamental à personalidade – complementado igualmente por meio de outras normas de proteção, como na Convenção Europeia de Direitos Humanos (por exemplo, art. 8º da EMRK) –, possibilita que a comunicação baseada em técnicas de informação seja protegida como exercício da liberdade baseada na confiança.

IV.1 Defesa e proteção

A proteção dos direitos fundamentais inclui a defesa contra intervenções (injustificadas) do Estado. No entanto, também se trata da garantia de proteção, seja por meio do cumprimento dos direitos subjetivos inerentes aos direitos fundamentais, e eventualmente pelos respectivos deveres de proteção[47], seja pela configuração das prescrições jurídico-objetivas dos direitos fundamentais[48]. As dimensões de proteção fora da proteção puramente defensiva dos direitos fundamentais[49] tornam-se mais centrais para as garantias dos direitos fundamentais, quanto mais as reais condições prévias para o exercício da liberdade pelos cidadãos têm que ser criadas e mantidas

46 Sobre a proteção do sistema e suas distintas facetas, v. Albers, in: Hoffmann-Riem/Schmidt-Aßmann/Vosskuhle (nota de rodapé 2), § 22 número de margem 102 e ss.

47 Sobre deveres de proteção em geral, v., por exemplo, BVerfGE 39, 1, 42; 46, 160, 164; 56, 54, 73; 115, 118, 152.

48 Neste sentido, por exemplo, Stögmüller CR 2008, 435 e ss. Cf., também, Hornung CR 2008, 299, 305; Kutscha NJW 2008, 1042, 1044; Sachs/Krings JuS 2008, 486. 45.

49 Ver as indicações nas notas 43 e 45.

de um lado pelo Estado, e, por outro lado, também por privados, ou mesmo no curso de atos cooperativos entre Estado e privados, e que eventualmente podem ser questionadas por eles[50]. Portanto, está se tornando cada vez mais significativo o fato de que o Tribunal Constitucional Federal da Alemanha tem se reportado há tempo e por diversas vezes à dimensão jurídico-objetiva da proteção dos direitos fundamentais[51]. No entanto, nas mais recentes decisões do Senado da Corte sobre a proteção contra intervenções em comunicação estruturada tecnologicamente e contra o acesso às informações correspondentes, as intervenções ou autorizações de intervenções por parte do Estado[52] têm permanecido em primeiro plano, uma vez que só elas foram objeto nos respectivos processos. No que diz respeito à ativação de outros, ou seja, também a partir das funções jurídico-objetivas dos direitos fundamentais, ela exige – na medida em que não se tornem significativas no curso da interpretação e aplicação das normas válidas – como regra formulações correspondentes por parte do legislador. Para este fim, não estão abertas apenas proibições e imposições, mas também outras formas de configuração, como regulamentos em relação à organização e ao procedimento, ou sobre configuração técnica.

IV.2 Normas relevantes de direitos fundamentais

Distintas normas já estão à disposição para a proteção dos direitos fundamentais, como a proteção do sigilo das comunicações (art. 10 da LF), a inviolabilidade do domicílio (art. 13 da LF), assim como as diversas dimensões complementares e muitas vezes centrais do direito fundamental à proteção da personalidade a partir do art. 2º, § 1º, c/c art. 1º, § 1º, da LF[53], complementado eventualmente também pelos arts. 12 e 14 da LF, e subsidiariamente a liberdade geral de ação do art. 2º, § 1º, da LF.

50 Cf., por todos, Schulze-Fielitz, in: Hoffmann-Riem/Schmidt-Aßmann/Vosskuhle, Grundlagen des Verwaltungsrechts, vol. 1, 2006, § 23, especialmente número de margem 64 e ss., 91 e ss.

51 Cf., por exemplo – em relação ao art. 5 § 1º, inciso 1 da LF – BVerfGE 7, 198, 205 e ss.; ao art. 10 da LF BVerfGE 106, 28, 37; ao art. 2 § 1º em sentido amplo 1 § 1º da LF BVerfGE 96, 56, 64; ao art. 2 § 1º e 14 § 1º da LF BVerfGE 84, 192, 194 f. 114, 73, 89 e ss. Cf. também a argumentação para a abertura de uma fonte de informação no âmbito da liberdade informacional (art. 5 § 1º da LF): BVerfGE 103, 44, 61. Ver, além disso, BVerfGE 49, 89, 140 e ss., ou por exemplo BVerfG JZ 2007, 576.

52 BVerfGE 107, 299, 313 e ss. Afirma que as medidas das empresas privadas – aqui uma empresa de telecomunicações – devem ser imputadas ao Estado se tiverem sido ordenadas pelo Estado e a empresa em causa não tiver margem para alternativas.

53 BVerfG (nota de rodapé 17), número de margem 166 e ss.

IV.2.a Sigilo das telecomunicações

O art. 10 da Lei Fundamental protege a transmissão incorpórea de informações por meio do tráfego das telecomunicações[54]. O ponto de partida da garantia constitucional é a ideia de proteger os direitos e liberdades do indivíduo decorrentes do processo de transmissão técnica e do envolvimento de um intermediário de comunicação – em regra, devido aos perigos que surgem como resultado do distanciamento físico[55]. Com esse objetivo determinado, o direito fundamental contém, em especial, um direito de defesa contra a divulgação do conteúdo e das circunstâncias detalhadas das telecomunicações pelo Estado; mas também inclui a tarefa ao Estado de fornecer proteção contra o acesso de terceiros privados ao conteúdo e às circunstâncias da comunicação. Além disso, existe proteção contra o Estado tornar acessível a si mesmo o conhecimento relevante relacionado à comunicação de pessoas privadas, por exemplo, autorizando o acesso aos dados de tráfego (anteriormente: "dados de conexão")[56] detidos por empresas de telecomunicações em processos de comunicação específicos, ou por meio da padronização de uma obrigação de retenção de dados, juntamente com direitos de acesso aos dados armazenados[57].

IV.2.b Proteção do domicílio

A proteção também pode ser garantida pelo direito fundamental especial previsto no art. 13 da Lei Fundamental[58], que protege a esfera espacial em que se desenvolve a vida privada, especialmente contra intromissões, isto é, incluindo a utilização de meios para a aquisição de imagens e impressões sobre eventos no domicílio[59]. A proteção assim garantida estende-se à coleta de informações tornada possível pela intromissão, bem como ao uso dos dados obtidos desta forma.

54 Cf. BVerfGE 67, 157, 172; 106. 28, 35 e ss.; 115, 166, 182. Acerca da amplitude desta proteção, ver em especial Bäcker, in: Brink/Rensen (nota de rodapé 32), sob o título II.

55 Em todo caso, a distância espacial não pode ser um elemento essencial na medida em que a possibilidade de acesso não se baseia nela, mas sim no uso das telecomunicações – independentemente da distância que os computadores utilizados para eles estão "localizados" uns dos outros.

56 Cf. BVerfGE 107, 299, 312 f.; 113, 348, 365.

57 Sobre o tema, cf. §§ 113a, b TKG e a decisão do BVerfG NVwZ 2008, 543.

58 Cf. BVerfGE 89, 1, 12; 103, 142, 105 e ss.

59 BVerfG (nota de rodapé 17), número de margem 193.

IV.2.c Direito fundamental à proteção da personalidade

Particularmente importante é o direito fundamental à proteção da personalidade nos termos do art. 2º, § 1º, combinado com o art. 1º, § 1º, da Lei Fundamental[60], sobre o qual o Tribunal Constitucional já decidiu no julgamento do censo no sentido de que as concretizações realizadas até agora não são conclusivas. A complementação do direito à autodeterminação informativa não estava associada à declaração segundo a qual uma concretização conclusiva tivesse sido realizada.

O direito fundamental[61] à proteção da própria imagem, o direito fundamental à proteção da própria palavra, o direito fundamental à proteção dos dados pessoais e o direito fundamental à proteção da esfera privada em perspectiva espacial e temática, bem como o direito fundamental à autodeterminação informativa, há muito foram reconhecidos como manifestações parciais deste direito fundamental (não explicitamente contidos no texto constitucional).

Em sua decisão sobre as buscas on-line[62], o Tribunal Constitucional Federal a eles adicionou, como outra expressão parcial do direito fundamental, a garantia da confidencialidade e da integridade dos sistemas próprios de tecnologia da informação[63], por vezes designado direito fundamental da TI[64].

A relação destas manifestações parciais do direito fundamental à proteção da personalidade nem sempre é fácil de esclarecer. Os direitos fundamentais à sua própria imagem e à sua palavra são destinados a elementos da proteção da personalidade que também são cobertos pelo direito fundamental à autodeterminação informativa, mas que também são

60 Cf. também a nota de rodapé 4.

61 A designação como "direito fundamental" (ver, por exemplo, BVerfG NJW 2008, 1793, 1794) deve ser preferida à anteriormente "lei" consuetudinária, uma vez que enfatiza o fundamento constitucional e permite uma distinção à "lei" do direito civil correspondente. Quaisquer outras consequências legais não estão associadas a isso, conforme indicado em Böckenförde JZ 2008, 925, 927 nota de rodapé 25.

62 BVerfG (nota de rodapé 17): Especificamente, a sentença se refere a pesquisas online; mas seu alcance constitucional vai muito além disso.

63 A redução do direito fundamental como "direito fundamental do computador" proposta na mídia é enganosa. Melhor – mas inadequado como termo jurídico – é o direito fundamental de TI, que Bäcker, por exemplo, usa em: Brink/Rensen (nota 32).

64 Bäcker, in: Brink/Rensen (nota de rodapé 32).

cobertos por outros direitos fundamentais (como no caso do art. 5º da Lei Fundamental). A proteção da privacidade inclui dados pessoais[65], mas claramente vai além da sua proteção, por exemplo, quando se refere à proteção do comportamento em uma situação protegida como esfera privada, ou como proteção contra exigências comportamentais nos respectivos espaços. A garantia de confidencialidade e integridade dos próprios sistemas de tecnologia da informação, que agora foi reconhecida pelo Tribunal Constitucional, sobrepõe-se às outras subcategorias, mas ganha seu significado especial através do foco na proteção do uso dos sistemas de tecnologia da informação para fins próprios relacionados à personalidade contra ameaças associadas.

A proteção da confidencialidade e da integridade dos próprios sistemas de informática pelos direitos fundamentais não foi concebida pelo Tribunal Constitucional como um novo direito fundamental[66], mas como uma manifestação do direito fundamental à proteção da personalidade. Isto é, como os outros direitos mencionados da proteção da personalidade, não é explicitamente abordada na parte dos direitos fundamentais da Lei Fundamental, mas é fundada nela. O direito à proteção se baseia nas mesmas premissas normativas que são o fundamento das concretizações das outras dimensões protetivas do direito de personalidade.

V – EM ESPECIAL: A GARANTIA JURÍDICO-FUNDAMENTAL DA CONFIDENCIALIDADE E DA INTEGRIDADE DOS SISTEMAS TÉCNICOS DE INFORMAÇÃO DE USO PRÓPRIO

A nova forma de proteção da personalidade encontrou ampla aprovação na mídia[67], e tem recebido críticas na literatura especializada, mas

65 Isso parece ser o discurso da "privacidade eletrônica" de Böckenförde JZ 2008, 925. A objeção a isso, no entanto, é que a proteção da privacidade sob os direitos fundamentais – espacial/temática – não é definida com base no meio com o qual a privacidade é configurada.

66 Uma parte da literatura ignora isso, por exemplo Lepsius, em: Roggan (nota 34), p. 21 e ss. Este artigo também empreende uma reconstrução da decisão, que é tão destacada de suas declarações e premissas que a classificação dogmática constitucional de Lepsius não pode sequer começar a convencer. Portanto, Böckenförde JZ 2008, 925, 928 nota 38 também rejeita este ponto com razão.

67 Cf., por todos, Prantl Süddeutsche Zeitung aos 28.02.2008, p. 4.

também concordâncias[68]. Os críticos[69] consideram que a nova concretização é dispensável, especialmente porque a proteção pretendida já é concedida pelo direito fundamental à autodeterminação informativa; eles também veem o risco de que a proteção da autodeterminação informativa seja minimizada[70]. A falta de uma estrutura dogmática e os riscos associados na delimitação do direito à autodeterminação informativa são também criticados[71]. Há receios igualmente acerca de um "direito fundamental a-pessoal orientado para a tecnologia"[72]. A seguir, será feita uma tentativa de reconstruir as importantes premissas para o novo do direito fundamental e, em particular, de mostrar que a necessidade de proteção vai além do que aquela até agora desenvolvida segundo a jurisprudência com o direito fundamental à autodeterminação informativa.

V.1 O ponto de partida

Nas manifestações feitas até o momento pelo Tribunal Constitucional sobre a proteção do direito fundamental à autodeterminação informativa, foi afirmado, em particular, que tal direito oferece a seus titulares proteção contra coleta, armazenamento, uso e divulgação ilimitados de dados individualizados ou individualizáveis relacionados a eles[73]. Em parte, também

68 Em particular, a construção e a forma de raciocínio são atacadas em detalhes, mas não a dimensão de proteção pretendida. Da literatura bastante crítica, ver, por exemplo, Britz DÖV 2008, 411 e ss.; Sachs/Krings JuS 2008, 482 e ss.; Eifert NVwZ 2008, 521 e ss.; Lepsius, em: Roggan (nota 60), p. 21 e ss.; Bull, em: Anuário de Segurança Pública 2008/2009, p. 317 e ss.; V. MMR 2008, 365 e ss. Cf. também o acompanhamento nos nºs 16 e 25, bem como as contribuições em Roggan (nota 34). Em princípio e de acordo com muitos detalhes, por exemplo Hornung CR 2008, 299 e ss.; Hirsch NJW 2008 com referência a NJOZ 2008, 2902; Lorenz StRR 2008, 140 e ss.; Stögmüller CR 2008, 435 e ss.; Jäger Juris-itr 12/2008; Petri DUD 2008, 443; Bäcker, em: Brink/Rensen (nota 32); Böckenförde JZ 2008, 925 e segs.; Michael/Morlok, Grundrechte, 2008, número de margem 427 e ss.

69 Em particular, a visão subordinada do tribunal é criticada de que o direito à autodeterminação informacional só se aplica a "requisitos de comunicação individual ou dados armazenados" ou dados com "referência seletiva a uma determinada área da vida" (a este respeito, a referência é feita em particular para as formulações do Tribunal Constitucional [nota 17], número de margem 201 e ss.). No entanto, as declarações do Tribunal Constitucional são mal interpretadas se forem entendidas como as declarações finais sobre o âmbito da proteção do direito fundamental à autodeterminação informativa. Como o contexto das explicações mostra, deve, antes de tudo, ficar claro que a complexidade da necessidade de proteção no que diz respeito aos sistemas de tecnologia da informação ainda não foi adequadamente acolhida pela jurisprudência anterior. A jurisprudência e, em grande parte, também a literatura tratam de precauções contra medidas concretas de coleta e uso de dados, mesmo quando fornecem instrumentos – tais como precauções para autoproteção, proteção por meio de tecnologia e configuração de sistemas – em um nível anterior. A dimensão da proteção independente da confiança no sistema de tecnologia da informação utilizado pelo próprio Tribunal Constitucional não entra em foco.

70 Assim, por exemplo: Britz DÖV 2008, 411, 413; Sachs/Krings JuS 2008, 481, 484; Volkmann DVBl. 2008, 591; Eifert NVwZ 2008, 521 e ss.

71 Cf. Kutscha NJW 2008, 1043; Lepsius, in: Roggan (nota de rodapé 34); v. também nota de rodapé 60.

72 V., sobre o tema, acima nota de rodapé 36.

73 Cf. BVerfGE 65, 1, 43; 67, 100, 143; 84, 239, 279; 103, 21, 33; 115, 166, 190; 115, 320, 341 e ss.

foi afirmado (de forma transversal e, portanto, sem mais especificações e sem poder de delimitação jurídico-dogmática) no sentido de que devem ser levadas em conta as ameaças e violações da personalidade que surgem para o indivíduo, especialmente sob as condições do moderno processamento de dados, "a partir de medidas relacionadas à informação"[74]. As decisões sobre este direito fundamental tomadas pelo Tribunal Constitucional até o momento referem-se a ameaças causadas por coleta de dados, independentemente de ser seletiva ou contínua, ou se são realizadas em casos individuais ou em escala de massa.

As proteções que são possíveis, ou mesmo requeridas, não se limitam, no entanto, a medidas diretamente relacionadas ao processo de coleta de dados e subsequente armazenagem, uso, processamento ou divulgação, mas também se estendem aos pressupostos (organizacionais, procedimentais, sistêmicos, dentre outros) para garantir que tal coleta e subsequentes medidas atendam às exigências ou, conforme o caso, para que sejam encerradas. Aqui se torna claro que a proteção da autodeterminação informativa já começa no nível da ameaça aos direitos fundamentais e pode, portanto, ser alcançada por meio de medidas para reduzir tais ameaças. Mesmo quando as medidas de proteção – tais como medidas de proteção de dados do sistema[75] – estão previstas na coleta de dados, elas são medidas para evitar prejuízos aos dados – elas ocorrem especialmente na forma de controle e design do contexto, mas não na proteção da confiança no funcionamento do sistema de tecnologia da informação em si. Em outras palavras: a proteção de dados por meio do design do sistema não é idêntica à proteção do sistema de tecnologia da informação (independentemente de as disposições jurídicas para design do sistema serem implementadas nele) contra o acesso ao próprio sistema e o acesso subsequente aos dados.

Se forem formulados requisitos especiais para esta nova dimensão da proteção relacionada ao sistema, isto não implica, ao mesmo tempo, a crítica de parte da literatura referente à "minimização" do direito à autodeterminação informativa[76]: seu objetivo de proteção e seu nível de proteção permanecem inalterados. No entanto, seu âmbito de aplicação não se estende a outras dimensões de proteção que até o momento não foram suficientemente cobertas pelo direito fundamental à autodeterminação informativa;

74 Desta forma formulado pelo Tribunal Constitucional, NJW 2008, 1505, 1506 (sobre registros de placas).
75 Ver acima na nota de rodapé 44.
76 Ver acima na nota de rodapé 67.

em vez disso, essa proteção está ancorada em um novo direito fundamental (até este ponto especial) e implementada por meio de requisitos regulamentares mais rigorosos. Uma redução na proteção do direito fundamental da personalidade, em geral, de todo modo não se verifica.

V.2 Novas dimensões da necessidade protetiva

Na decisão sobre as buscas on-line, o tribunal partiu da premissa de que a proteção até então concebida para o direito fundamental à autodeterminação informativa não era suficiente para proteger a confiança importante para a proteção da personalidade na funcionalidade dos sistemas utilizados para comunicação. A proteção (somente) contra a coleta e posterior utilização de dados pessoais não é suficiente se não incluir também a proteção contra o acesso ao seu próprio sistema de tecnologia da informação, que é utilizado para o desenvolvimento comunicativo, cujo funcionamento sem perturbações é regularmente confiado, e cuja infiltração ou mesmo manipulação apresenta perigos para a proteção dos direitos de personalidade, que não são evitados pela proteção dos dados coletados[77]. Assim, a infiltração de um sistema complexo de tecnologia da informação com a possibilidade de manipulação de seu funcionamento ou de instalação de software para alterar os dados processados pelo sistema e os processos de comunicação transmitidos pelo sistema resultam em si em fontes de perigo, cujo surgimento também apresenta riscos para os dados disponíveis na tecnologia da informação. A defesa efetiva contra tais ameaças à personalidade requer um (pré)deslocamento da proteção para a infraestrutura utilizada, que deve assegurar a possibilidade de autodeterminação com os dados, bem como a liberdade e a integridade da comunicação transmitida através das infraestruturas. A necessidade de proteção contra tais infiltrações já existe antes

77 Que os perigos associados à violação da confidencialidade e integridade dos sistemas de tecnologia da informação sejam levados em consideração exclusivamente por meio da "proteção dos dados ao mesmo tempo suficientemente" – como B. Eifert NVwZ 2008, 522 assume – não é reconhecível. A proteção da confiança no tipo de desempenho deste sistema de tecnologia da informação não pode ser alcançada desta forma. Por exemplo, violações de integridade – como a manipulação do software com efeitos relacionados à proteção pessoal – podem tornar praticamente impossível a proteção de dados individuais. Além disso, a proteção que é (apenas) implementada como proteção dos dados coletados teria que se basear na qualidade desses dados, sem poder ser influenciada de forma independente em seu tipo e intensidade pela forma como foram obtidos. Deve-se admitir, no entanto, que o Tribunal Constitucional Federal, ao determinar a necessidade de proteção, em particular a determinação do nível de intervenção, também fez uso de circunstâncias que não estão relacionadas com a qualidade dos dados em causa, como a propagação ou o número de intervenções.

que certos dados possam ser acessados[78], e continua quando tal intervenção ocorre.

Diferentes níveis de perigo vêm à tona. Alguns dos perigos podem ser combatidos[79] pelo (já desenvolvido) direito fundamental à autodeterminação informativa, eventualmente após modificações; outros não poderiam, ou pelo menos não de tal forma que as especificidades da situação de risco no uso de seus próprios sistemas de tecnologia da informação são sejam suficientemente levadas em consideração.

V.2.a Amplitude da intervenção relativa à personalidade

O risco de que tais infiltrações possam facilitar mais a coleta de dados do que no passado poderia de fato ser combatido em muitos aspectos pelo direito fundamental à autodeterminação informativa – complementado também pelos arts. 10 e 13 da Lei Fundamental. Se a infiltração não só torna possível o acesso a processos de comunicação específicos ou a dados individuais, mas também a todos os outros dados "arquivados" no sistema de comunicação ou a dados que podem ser acessados através dele (por exemplo, dados do provedor), então podem ser capturadas uma infinidade e uma variedade de circunstâncias da vida e de características pessoais que antes dificilmente poderiam ser previstas em detalhe e possivelmente até tipificadas, o que só é possível em virtude da infiltração do sistema de tecnologia da informação. A amplitude "pessoal" de acesso ao sistema de tecnologia da informação aumenta o potencial de risco de intervenções posteriores em tecnologia da informação e reduz a possibilidade de contra medidas autodeterminadas. De todo modo, isso exigiria novos esforços dogmáticos caso tais riscos fossem combatidos unicamente pela extensão do alcance do direito fundamental à autodeterminação informativa.

V.2.b Sobre dados gerados pelo sistema

Em especial, é duvidoso se o direito fundamental à autodeterminação informativa é suficientemente eficaz contra o acesso aos dados relevantes para a personalidade gerados pelo sistema de tecnologia da informação – geralmente sem o conhecimento da pessoa envolvida. Acessos ao sistema de tecnologia da informação para fins de acesso a tais dados podem ser concebidos como uma intervenção no direito fundamental à autodeterminação

78 Neste sentido, Petri DUD 2008, 446.

79 V. as indicações acima na nota 66: vários autores qualificam este método como suficiente.

informativa e submetido ao seu programa de justificação. Os problemas surgem, no entanto, porque a possibilidade de proteção para a pessoa afetada – incluindo a possibilidade de proteção efetiva ex post – é, de fato, limitada. Não auxilia também, como é defendido em alguns casos, que seja referido à pessoa a possibilidade de autoproteção preventiva. Por exemplo, há certas possibilidades para o usuário de impedir tecnicamente a criação de dados individuais gerados no processo de comunicação – tais como cookies[80] – ou conjuntos de dados – tais como caches[81] –, mas apenas de forma limitada: eles sempre exigem tanto uma consciência especial do perigo quanto uma considerável experiência técnica, e em alguns casos – como no caso dos flash cookies – é extremamente difícil encontrá-los[82]. As qualificações correspondentes não podem ser adquiridas pelos usuários prontamente. Tampouco corresponde ao modelo constitucional de proteção da liberdade concedê-la apenas a uma pequena minoria de pessoas conscientes do perigo e com experiência técnica – tais como freaks, hackers, ou criminosos especializados em tais habilidades[83]. Também é importante observar que os cookies ou caches geralmente só podem ser desativados ao custo de uma perda não desprezível de funcionalidade: em muitos aspectos, eles também são "úteis" para a pessoa envolvida. Ela confia, em última análise, que pode utilizá-los sem preocupação.

Caso o usuário não queira impedir a geração e a coleta de dados, exige-se uma proteção efetiva da personalidade, de modo que o usuário tenha a confiança de que os dados assim obtidos não possam ser utilizados em contextos diferentes e, em particular, por terceiros não autorizados. Porém, por meio da infiltração dos sistemas técnicos de informática, eles podem ser utilizados por quem não está envolvido no processo de comunicação, sem que o interessado possa reconhecer e se proteger.

80 São dados armazenados em um computador usuário para transmitir certas informações a um computador servidor, especialmente no caso de visitas repetidas.

81 Um cache é uma memória de buffer rápida que contém cópias do conteúdo de outra memória (de fundo) e, portanto, acelera o acesso a ela. Portanto, os dados são armazenados em cache para acesso mais rápido a um meio mais rápido. A maioria dos navegadores da web cria esse cache no disco rígido na forma de arquivos temporários.

82 Os cookies em Flash – assim chamados em homenagem ao software flash player com o qual são criados – são consideravelmente mais difíceis de exibir e excluir em comparação com os cookies "normais". Com as configurações padrão do sistema operacional Microsoft Windows XP, por exemplo, eles não são iguais visíveis no disco rígido. Eles não podem ser localizados de forma alguma no navegador, pois são processados e armazenados independentemente do navegador. Pelo mesmo motivo, os dados armazenados podem ser atribuídos de forma clara ao respectivo usuário, mesmo quando usando navegadores diferentes no mesmo sistema e também em qualquer número de sessões do navegador.

83 Cf. BVerfG JZ 2007, 576: Proteção própria informacional precisa ser ao indivíduo possível e razoável.

V.2.c Criação de novas imagens da personalidade de nova profundidade e amplitude

Uma situação de risco especial, que não é coberta pela proteção tradicional dos direitos fundamentais sem extensões consideráveis, é criada pelo fato de que a infiltração supera fundamentalmente – ou seja, não apenas em casos individuais – obstáculos técnicos que, de outra forma, impediriam a espionagem ou vigilância. Se o obstáculo for superado, a barreira de proteção relacionada ao sistema, que de outra forma teria que ser superada repetidamente no caso de intervenções no direito à autodeterminação informativa e contra a qual pode haver opções de proteção legal, não está mais disponível. Mesmo que o ponto de infiltração esteja interessado apenas em determinados dados[84], é praticamente possível para ele também obter outros dados e acessar outros processos de comunicação. Por exemplo, a infiltração possibilita a obtenção de um banco de dados potencialmente grande, altamente informativo sobre várias facetas da personalidade. Percepções sobre partes essenciais do estilo de vida podem ser reveladas, bem como maneiras de criar perfis sociais, de interesse, comportamento e de comunicação diferenciados e, portanto, perfis de personalidade altamente significativos[85].

No entanto, o direito fundamental à autodeterminação informativa já protege contra a construção de imagens da personalidade por meio do uso de levantamentos de dados individuais[86]. No entanto, se a infiltração de sistemas de tecnologia da informação fundamentalmente remove o obstáculo técnico de acesso a todas essas informações, o registro de todos os dados acessíveis no sistema de tecnologia da informação por longos períodos de tempo cria oportunidades para o acúmulo e combinação de muitas informações de diferentes áreas da vida em uma profundidade e amplitude que não eram possíveis anteriormente com as intervenções[87]. Mesmo quando o direito fundamental à autodeterminação informativa em sua proteção contra imagens de personalidade é suficientemente ativado contra coleta de da-

84 Por exemplo, as autoridades de segurança estão regularmente interessadas apenas na transmissão seletiva direcionada de dados específicos que sejam relevantes para elas. Um Trojan instalado por você funciona melhor se apenas transmitir dados individuais, ou seja, precisamente os dados que são importantes para a tarefa oficial (por exemplo, nomes de parceiros de comunicação, conteúdo de e-mail salvo etc.). No entanto, o obstáculo é geralmente superado pela infiltração.

85 A redação em Böckenförde JZ 2008, 925, 928 é plástica: "É o serviço de mediação do sistema de tecnologia da informação que agrega dados pessoais individuais em um todo dinâmico que é acessível uma e outra vez e, portanto, expõe a pessoa em questão em sua vida pessoal em caso de acesso não autorizado".

86 BVerfGE 65, 1, 42 e ss.; 109, 279, 323; 112, 304, 319.

87 Michael/Morlok (nota de rodapé. 64), número de margem 429 falam sobre um "salto qualitativo".

dos específicos, a infiltração de sistemas de tecnologia da informação ainda envolve riscos de que imagens de personalidade de amplitude e densidade anteriormente desconhecidas sejam criadas e de que a pessoa interessada nem mesmo avalie o perigo potencial e, muitas vezes, sequer consiga se defender com eficácia: em qualquer caso, a lacuna de proteção relacionada ao sistema de tecnologia da informação não se deixa ser efetivamente eliminada no nível de proteção contra a coleta de dados específicos. A infiltração do sistema de tecnologia da informação colocou um "pé virtual na porta" da personalidade.

V.2.d Risco de falsificação de dados

A possibilidade de infiltração no sistema também está associada ao risco de falsificação (praticamente irreconhecível) dos dados individuais registrados e sua combinação com outros, o que, neste aspecto, pode levar a um perfil de personalidade falsificado. O afetado praticamente não pode mais se defender contra tais falsificações, uma vez ocorrida uma infiltração associada a tais possibilidades, que, em princípio, também pode ser utilizada por terceiros[88]. Isso não é, de forma alguma, apenas uma intensificação da intervenção contra a qual o direito fundamental à autodeterminação informativa protege em seu conteúdo[89], mas uma qualidade independente de ameaça[90]. As medidas de proteção necessárias devem começar pela proteção do próprio sistema de tecnologia da informação, ainda que essa proteção deva então ser estendida também aos dados coletados em decorrência da infiltração, no interesse de sua eficácia.

V.2.e Neutralização das possibilidades de autoproteção

A infiltração estatal e – se necessário – para espionagem – a manipulação do sistema de tecnologia da informação devem, em particular, levar ao fato de que a autoproteção aplicada e mesmo recomendada ao afetado como uma expressão da ideia de autodeterminação informativa – por exemplo, a criptografia e o uso de senhas – será fundamentalmente (não só no caso concreto) driblada. A proteção proporcionada pelo direito fundamen-

88 O fato de que as autoridades de segurança que executam a infiltração não deveriam estar interessadas em tais falsificações é apenas mencionado para fins de completude.

89 Por exemplo, Eifert NVwZ 2008, 521: "interferência particularmente grave" na área de proteção do direito fundamental à autodeterminação informativa.

90 Se fosse apenas sobre o problema de "violações aditivas aos direitos fundamentais", poderia, no entanto, ser tratado também no nível da justificação. Ver, por exemplo, BVerfGE 112, 304, 319 e seguintes. No entanto, isso é mais do que apenas uma adição.

tal à autodeterminação informativa será comprometida em suas premissas básicas.

Isso porque a possibilidade de autoproteção tem sido considerada até agora um elemento essencial da participação autodeterminada na comunicação, que também é levada em consideração no direito atual da proteção de dados. A possibilidade de autodeterminação sobre os dados disponíveis foi considerada, por exemplo, pelo Segundo Senado do Tribunal Constitucional como ensejo para a tese segundo a qual a proteção conferida pelo art. 10 da LF para dados no âmbito de controle da pessoa em causa não se aplica, uma vez que ela tem possibilidades de autoproteção[91]. Se a referência do Segundo Senado à possibilidade de autoproteção é praticável e, portanto, realmente funciona, pode ser questionada. No entanto, é viável a reflexão de que os dados armazenados após a conclusão do processo de comunicação não diferem mais daqueles contidos nos arquivos criados pelo próprio usuário. Se, após a conclusão de um processo de comunicação, forem acessados dados de comunicação armazenados no domínio do destinatário, então se materializa não um risco específico de comunicação, mas um risco geral de tecnologia da informação[92].

O alto padrão da possibilidade de autoproteção determinado pelo direito básico à autodeterminação informacional não é desvalorizado pelo fato de muitos cidadãos tratarem seus dados de forma descuidada ou desconsiderarem as possibilidades de autoproteção. A necessidade de proteção dos direitos fundamentais não deixa de existir porque os cidadãos individuais não a sentem ou não podem realizá-la; à autodeterminação pertence a capacidade de decidir o quanto alguém deseja se proteger. Quem quiser prescindir da proteção também faz uso do direito à liberdade. Se, no entanto, ele não puder mais estimar a necessidade de proteção ou se a possibilidade de proteção nem mesmo existir, sua disposição para a proteção autodeterminada não importa mais e a recusa fundamental de proteção em nenhuma circunstância pode ser justificada com referência ao descuido de muitos cidadãos no tratamento dos seus dados (específicos). A possibilidade de proteção é, no entanto, negada aos cidadãos pela infiltração dos sistemas de tecnologia da informação. Isto se aplica mesmo que não ocorra em segredo, desde que o afetado não possa avaliar as consequências da

91 BVerfGE 115, 166, 185 e ss.

92 Desta forma elaborado por Bäcker, in: Brink/Rensen (nota de rodapé. 32), sob o título II 2c.

infiltração e da manipulação associada ou seja praticamente incapaz de as contrariar.

V.2.f Possibilidade de acesso de terceiros

Em particular, existe a necessidade (que já foi apontada por vezes aqui) de proteção contra o risco de terceiros (privados) se aproveitarem da infiltração do sistema de tecnologia da informação por parte das autoridades estatais e, por exemplo, se utilizem do software infiltrado para espionar o sistema ou manipulá-lo – isto é, de rededicar a infiltração a fins próprios como uma espécie de ovo do cuco posto pelo Estado, sem que a pessoa afetada suspeite disso e seja capaz de se proteger com eficácia. A proteção dos direitos fundamentais contra intervenções do Estado – aqui a infiltração – é constitucionalmente mais abrangente, mais fácil e, acima de tudo, mais eficazmente executável do que a proteção contra particulares no curso da eficácia horizontal indireta dos direitos fundamentais. No caso de uso estatal do software infiltrado pelo Estado ou do software ou hardware manipulado, há também a perspectiva de que o Estado observe as restrições constitucionais à sua autorização para intervir; no caso de acesso (ilegal) de terceiros viabilizado por "adiantamentos" estatais, essa perspectiva de proteção não se aplica, já que terceiros não se submetem a tais obrigações constitucionais e, dada a ilegalidade de seu comportamento, dificilmente poderiam ser efetivamente submetidos.

V.2.g Grande variação de pessoas envolvidas

A infiltração e o que é tornado possível por ela, se necessária a vigilância de longo prazo que abrange uma ampla variedade de atos de comunicação e os vincula dinamicamente, não se limita aos seus destinatários como afetados, mas inclui um grupo de terceiros que não pode ser esquecido de antemão como parceiros de comunicação da pessoa envolvida. Este também é o caso com outros tipos de acesso à comunicação – por exemplo, por meio de escuta telefônica ou observação policial. Na medida em que todos os tipos de dados relativos a terceiros são armazenados ou gerados no sistema de tecnologia da informação, a propagação pessoal que é possível aqui pode, no entanto, exceder qualitativamente aquela que está associada à intervenção direcionada em atos de comunicação específicos, como espionagem de certas conversas. Como resultado, terceiros podem ser afetados não apenas na medida em que isso seja "inevitável em casos individuais", mas potencialmente em princípio e – presumivelmente com

frequência – sem qualquer limitação prévia e – é claro – sem serem capazes de se defender "autodeterminadamente".

V.3 Esclarecimento da peculiaridade da situação de risco e da respectiva proteção de direitos fundamentais pelo Tribunal Constitucional Federal da Alemanha

V.3.a Diferenciação ao nível do âmbito de proteção

É verdade que uma tentativa poderia ser feita para lidar com algumas das preocupações que acabamos de listar por meio de uma expansão posterior do direito fundamental à autodeterminação informativa. Teria então de ser desenvolvido em um baluarte que pode ser usado de forma abrangente contra a habilitação e implementação do acesso estatal não apenas aos dados e processos de comunicação de todos os tipos, mas também às infraestruturas de comunicação utilizadas (software e hardware) e também contra os correspondentes acessos de particulares. No interesse da capacidade de gestão dogmática, seria necessária uma maior diferenciação do amplo âmbito de proteção com uma dogmática dos limites correspondentemente coordenada, com a elaboração de limites especiais (em regra especialmente mais altos) para a infiltração e manipulação de sistemas de tecnologia da informação que colocam em perigo a proteção pessoal e a coleta e o processamento de dados que isso permite. Em contraste, parecia constitucionalmente preferível para o Tribunal Constitucional diferenciar ainda mais o direito fundamental geral à proteção da personalidade e a proteção da integridade e confidencialidade dos sistemas de tecnologia da informação usados e antes da coleta e uso dos dados obtidos como resultado do infiltração em uma forma "especial", baseada no sistema de tecnologia de informação, do direito fundamental geral, que não depende de ficções de proteção autodeterminada da personalidade, mas antes coloca, em primeiro plano, a necessidade de proteção da confiança. Isso torna mais fácil observar a nova qualidade da ameaça e a necessidade de proteção baseada na confiança do sistema no nível do âmbito de proteção e a necessidade de reconhecer requisitos especiais para limites e de desenvolver medidas de proteção voltadas para a ameaça.

A abordagem do tribunal também pode ser interpretada como uma reação ao fato de que as dimensões da ameaça à confiança nas infraestruturas de comunicação e as necessidades de proteção correspondentes até então só foram abordadas em uma extensão limitada – se é que o fizeram – e que não existem conceitos, aprofundadamente discutidos ou reconhecidos na

jurisprudência e na literatura, sobre como a proteção da confidencialidade e da integridade dos sistemas de tecnologia da informação de uso próprio pode ser embutida no direito fundamental à autodeterminação informativa sem inconsistências e lacunas. Tendo em vista a falta de trabalhos anteriores na literatura, é surpreendente que a maioria dos autores que analisam a nova decisão alega, sem maiores diferenciações, que a proteção poderia ter sido realizada unicamente pelo direito fundamental à autodeterminação informativa. Isso é tanto mais surpreendente quanto o fato de que, antes da decisão na literatura e nos escritos submetidos ao tribunal, foram feitas tentativas para satisfazer a necessidade de proteção em particular por meio do art. 13[93] da Lei Fundamental – ou mesmo também do art. 10 da LF.

V.3.b Reação à especial qualidade do risco

Por outro lado, a designação explícita e a ênfase da proteção dos direitos fundamentais de confidencialidade e integridade dos próprios sistemas de TI, defendida pelo Tribunal Constitucional, deixa claro que qualitativamente há uma situação de risco especial e que as precauções de proteção correspondentes devem estar em vigor. Especificar o âmbito de proteção tem a vantagem, dentre outras, de que o teste de proporcionalidade no sentido amplo pode ser orientado de forma mais precisa. O potencial de risco particular é identificado destacando a expressão de direito fundamental particular de uma maneira tipificadora e a demanda por proteção tipificadora é feita. Como resultado, a proteção não depende apenas de ponderações ad hoc no contexto de testes de proporcionalidade. Ponderações relacionadas ao caso, no entanto, ainda podem ser necessárias para o ajuste estrito em casos individuais.

V.3.c Delimitação com relação ao direito à autodeterminação informativa

Um problema, entretanto, é a demarcação entre o direito à autodeterminação informativa e a proteção da integridade e da confidencialidade dos próprios sistemas de TI tratados aqui. O princípio básico é: contra a coleta de dados (e processamento posterior de dados)[94] sem a infiltração de sistemas de tecnologia da informação e contra a criação das autorizações correspondentes, o direito fundamental à autodeterminação informativa

93 Cf. os argumentos em Böckenförde JZ 2008, 925, 926 nota de rodapé 10.

94 No entanto, a utilização por terceiros, ou seja, após o repasse, é, de acordo com princípios gerais, apenas admissível se os pré-requisitos que justificam tal intervenção também forem cumpridos por esses órgãos.

continua a proteger[95-96]. Se, no entanto, um complexo sistema de informática for infiltrado, espionado e possivelmente manipulado para realizar a coleta de dados, entra em vigor a nova dimensão da proteção aos direitos fundamentais[97]. Este direito fundamental de proteger a confidencialidade e integridade do sistema de tecnologia da informação não só afeta a infiltração (e possivelmente a manipulação) como tal, mas também se estende à coleta e uso dos dados e informações que são (apenas) obtidos como resultado da infiltração[98]: os obstáculos respectivamente aumentados da proteção da personalidade estendem-se ao tratamento dos dados relacionados à personalidade acessíveis por meio da infiltração.

V.3.d Necessidade de outras concretizações

Os contornos da nova especificação dos direitos fundamentais não puderam ser trabalhados em todos os aspectos pelo Tribunal Constitucional, que se ocupou de um litígio específico e na medida em que fez referência ao objeto desse litígio. Como resultado, existe ainda uma necessidade considerável de especificações adicionais, também no que diz respeito ao objeto da proteção, em particular o conceito (relacionado com a personalidade) dos próprios (melhor: de uso próprio)[99] "sistemas de tecnologia da informação"[100]. Também não foi ainda definitivamente esclarecido de que forma deve ser salvaguardada a proteção dos sistemas informáticos contra intervenções não encobertas, que o tribunal também mencionou expres-

95 É errado interpretar a sentença introdutória do Tribunal Constitucional Federal (nota de rodapé 2), números de margem 166 e 201, no sentido de que a nova dimensão da proteção é "subsidiária" ao direito à autodeterminação informacional, por exemplo Petri DUD 2008, 444. O Tribunal Constitucional Federal afirma, em vez disso, que a nova forma de direitos fundamentais se aplica quando uma lacuna na proteção for diagnosticada.

96 A propósito, no que diz respeito a qualquer concorrência remanescente, aplica-se o princípio geral de que os limites dos direitos fundamentais devem ser derivados da expressão do direito de personalidade que protege contra o perigo maior e, portanto, impõe requisitos mais rígidos. Para informações gerais sobre tais regras de competição, ver Jarass/Pieroth, GG, 9ª edição 2007, observações preliminares antes do art. 1, número margem 18, com comentários adicionais.

97 Caso a autorização legal permita que outros órgãos se aproveitem da infiltração ou dos dados obtidos por meio dela, os elevados requisitos para interferir em seu próprio sistema de tecnologia da informação também teriam que ser atendidos por eles.

98 Esta extensão da proteção que foi "obtido" através da intervenção dos direitos fundamentais não é incomum. O art. 13 da LF não protege apenas contra a intrusão no domicílio, mas também as informações ou objetos obtidos por meio da intrusão, ver BVerfGE 109, 279, 374 com referência a BVerfGE 100, 313, 360 (este último no art. 10 da LF). Sobre os paralelos entre a nova garantia dos direitos fundamentais e o art. 13 da Lei Fundamental, ver Bäcker, em: Brink/Rensen (nota de rodapé 32), ponto III 1; Pieroth/Schlink, Grundrechte, 24ª edição 2008, número de margem 377c.

99 Essa alternativa linguística apenas evita ecos inadequados do direito das coisas. Ver também Bäcker, em: Brink/Rensen (nota 32), título III 2a. Há também (mesmo que apenas temporário) uso pessoal ao usar o computador no cibercafé.

100 V. também os requisitos acima III.

samente, mas não foi desenvolvida[101]. É também necessário esclarecer o âmbito da proteção contra particulares. A formulação constitucional da dimensão da proteção dos direitos fundamentais como "garantia" deixa claro, no entanto, que o Estado também tem a responsabilidade de garantir que a integridade e a confidencialidade dos sistemas de tecnologia da informação sejam protegidas na medida em que sejam ameaçados de outras formas que não pela intervenção estatal. No entanto, ele tem uma ampla margem de manobra criativa para a execução dos mandatos regulatórios legais e objetivos correspondentes.

A garantia de direito fundamental também protege contra intervenções com fins repressivos. No entanto, são necessários mais esclarecimentos sob quais condições isso pode ser possível[102]. Ao fazê-lo, o peso dos interesses jurídicos, cuja proteção de que efetivamente serve a norma penal eventualmente violada no caso concreto, deverá ser apurado de forma análoga às medidas preventivas.

No entanto, houve uma necessidade de especificações adicionais também ao formular o direito fundamental à autodeterminação informativa há um quarto de século. Lá, também, a nova perspectiva representou um desafio à dogmática jurídica, à legislação e à jurisdição. Então, agora ele está de volta.

VI – LIMITES AOS DIREITOS FUNDAMENTAIS

O direito fundamental à garantia da integridade e confidencialidade dos sistemas de tecnologia da informação de uso próprio não é protegido sem limitações. Tendo em vista o potencial de risco particular, o teste de proporcionalidade especialmente em regra (mas dependendo da intensidade da intervenção[103]) leva a um grande obstáculo para as intervenções. O dever de proteção do Estado, ancorado no direito objetivo, também é acionado para tomar medidas contra os perigos apresentados por particulares[104].

101 Cf., sobre o tema em mais detalhes, Böckenförde JZ 2008, 925, 931; Bäcker, in: Brink/Rensen (nota de rodapé 32), título III.

102 Cf., também die, as ponderações de Kühne, in: Roggan (nota de rodapé 34), p. 85 e ss.

103 O BVerfG não teve que decidir em que medida as intervenções de menor alcance do que as pesquisas online poderiam ser permitidas em condições menos estritas. Ver também Bäcker, em: Brink/Rensen (nota 32), sob III, 3.

104 Ver as notas acima 44, 45. Com o termo "garantia" da confidencialidade e integridade dos sistemas de tecnologia da informação, o tribunal esclarece a existência de um mandato ao estado para proteção em todas as áreas da vida (ver também Petri DUD 2008 446 e ss.), mas sem elaborá-lo com mais detalhes.

VI.1 Requisitos jurídicos materiais e processuais

O Tribunal Constitucional formulou requisitos para autorizações legais formuladas na área da prevenção de perigos, que dizem respeito à infiltração e manipulação do sistema informático utilizado pelo próprio usuário, mas também dizem respeito à coleta e utilização dos dados e informações obtidos nesta base.

Os requisitos constitucionais das restrições incluem, em primeiro lugar, o cumprimento do requisito da especificidade e da clareza das normas de autorização, que desde sempre é derivado do mandamento do Estado de Direito[105].

Os requisitos para a classificação do bem jurídico protegido também são importantes. Um bem jurídico suficientemente (predominante) para justificar uma busca online[106] inclui a vida, a integridade e a liberdade de pessoas ou bens do público em geral, cuja ameaça afeta os fundamentos ou a existência do Estado ou os fundamentos da existência das pessoas[107]. Um exemplo do último são os ataques a instituições públicas de segurança social, como as represas.

Existem também requisitos constitucionais para o tipo e intensidade do risco e, portanto, também para o grau de probabilidade e a base factual do prognóstico do risco[108]. Em particular, a exigência de uma probabilidade suficiente de ocorrência não pode ser dispensada e as suposições e conclusões devem ter um ponto de partida concreto de fato. Os fatos devem, por um lado, permitir concluir que pelo menos o seu tipo se concretize e seja temporalmente previsível e, por outro lado, que estarão envolvidas certas pessoas cuja identidade é conhecida pelo menos o suficiente para que a medida de vigilância possa ser usada especificamente contra elas e em grande parte limitada a elas[109].

Além disso, as garantias processuais são importantes[110], em particular um controle por uma autoridade independente, que é fundamentalmente

105 Cf. BVerfG (nota de rodapé 17), número de margem 208 e ss., com outras indicações.

106 Requisitos mais baixos podem ser suficientes, por exemplo, para a avaliação offline do disco rígido de um computador confiscado.

107 BVerfG (nota de rodapé 17), número de margem 247.

108 BVerfG (nota de rodapé 17), número de margem 242 e ss., 249 e ss.

109 BVerfG (nota de rodapé 17), número de margem 251.

110 BVerfG (nota de rodapé 17), número de margem 257 e ss.

necessário defronte a infiltração. O acesso secreto aos sistemas de tecnologia da informação, que podem ser avaliados como particularmente importantes, deve fundamentalmente estar sujeito a uma reserva de ordem judicial. Exceto em casos urgentes, outro órgão só pode ser considerado neste caso se oferecer a mesma garantia de independência e neutralidade de um juiz – uma garantia difícil de ser estruturada. As razões da legalidade das medidas de vigilância devem ser registradas por escrito.

VI.2 Núcleo da vida privada

Finalmente, precauções para proteger o núcleo essencial da vida privada são indispensáveis. Os sistemas de tecnologia da informação usados exclusivamente para a comunicação relevante para a área central não devem ser infiltrados. No entanto, isso geralmente não é previsível com antecedência. Nesse sentido, a proteção só pode ser totalmente eficaz quando os dados são coletados devido à infiltração do sistema de tecnologia da informação.

A coleta de dados relevantes para a área central deve ser, em princípio, evitada. A proteção só pode ser adiada para o segundo nível, designadamente a avaliação, se a relevância do núcleo central dos dados coletados não puder ser esclarecida antes ou durante a coleta de dados, mas houver indícios de uma suposta ameaça de perigo de um bem protegido de extrema importância. Ao fazê-lo, no entanto, regras procedimentais adequadas devem assegurar que a intensidade da violação do núcleo essencial e seus efeitos sobre a personalidade e o desenvolvimento da pessoa em causa permaneçam tão baixos quanto possível[111].

A proteção pela não coleta continua sendo a prioridade. Assim, o tribunal formula a exigência de abster-se de coletar dados se houver indícios de que o núcleo essencial está "afetado". O núcleo essencial da vida pessoal é protegido como tal. Não se trata (apenas) da proteção de uma determinada declaração que deve ser avaliada isoladamente, a qual, pelo seu conteúdo, não deve ser acessível ao Estado por razões de dignidade humana. Em vez disso, a proteção do núcleo essencial visa proteger aquela parte do desenvolvimento pessoal privado que, em prol da dignidade humana, deve ser mantida livre do conhecimento do Estado. Mesmo no núcleo essencial da vida privada, no entanto, o íntimo e o banal, o pessoal e o menos significati-

111 BVerfG (nota de rodapé 17), número de margem 281 e ss.

vo, normalmente se misturam. Essa situação de confusão comunicativa também é protegida, mesmo antes de se fazer o levantamento da comunicação, não apenas ao nível da avaliação. Lá, a proteção só poderia ser concedida dividindo o processo de comunicação em – visto isoladamente – conteúdo absolutamente protegido e conteúdo apenas relativamente protegido.

Se a proteção fosse oferecida apenas desta forma, o Estado, em princípio, não estaria impedido de se infiltrar no sistema de tecnologia da informação e, em primeiro lugar, registrar todo o conteúdo para depois remover as declarações individuais como absolutamente protegidas. Isso não faria justiça à ideia básica da proteção do núcleo essencial: a dignidade humana exige que o Estado se abstenha de monitorar uma situação em que haja indícios de que bem de proteção da mais alta prioridade seja afetado pela medida. Esse "contato" geralmente ocorre quando o sujeito está ciente dele. Uma renúncia à proteção no nível da coleta deve, portanto, permanecer uma exceção[112], para a qual há um ensejo, por exemplo, se o núcleo essencial for afetado inesperadamente[113] ou se houver indicações de que a comunicação serve para atender ou planejar atos criminosos específicos[114], ou porque conteúdos íntimos ou outros que precisam de proteção servem apenas como uma camuflagem para que as ações que dão origem a perigos sejam acordadas ou discutidas em mais detalhes[115]. Somente se não for suficientemente previsível qual conteúdo os dados coletados terão, ou se as dificuldades de tecnologia da informação ou de técnica de investigação impedirem a análise do conteúdo dos dados – por exemplo, no caso de documentos em língua estrangeira ou conversas –, permite-se, no que diz respeito aos bens extremamente importantes, mesmo após uma infiltração no sistema de tecnologia da informação, primeiro fazer um levantamento e deixar a proteção constitucional para o nível de avaliação (conceito de proteção em duas etapas).

O requisito de proteção do núcleo essencial não é cumprido pelo fato de que a coleta (somente) é evitada se "apenas" as descobertas relevantes ao núcleo central forem afetadas, conforme previsto na Seção 100a (4) do Código de Processo Penal e em outras normas. É extremamente raro que o conteúdo relevante para o núcleo essencial seja comunicado "sozinho" na

112 BVerfG (nota de rodapé 17), número de margem 281.
113 BVerfGE 109, 297, 318.
114 BVerfGE 113, 348, 391.
115 BVerfG (nota de rodapé 17), número de margem 281.

vida prática em algum ponto; o que não ficará aparente de antemão. Limitar a proteção a esse tipo de uso prejudicaria a proteção do núcleo central de dois estágios. Mesmo em uma conversa confidencial entre cônjuges, em que o conteúdo relacionado à área central é o assunto, também haverá outros conteúdos banais, por exemplo, declarações sobre o comportamento de terceiros ou acontecimentos de outro tipo: não atende aos requisitos constitucionais só por esse motivo permitir o monitoramento e a gravação e negar a proteção do núcleo central ao nível da coleta, adiando-a para o nível de aplicação[116].

VII – CONCORRÊNCIA COM OUTRAS NORMAS DE DIREITOS FUNDAMENTAIS

O direito fundamental à garantia da confidencialidade e integridade dos sistemas de tecnologia da informação pode concorrer com outras normas de direitos fundamentais, como os arts. 10 e 13 da Lei Fundamental.

VII.1 Intervenção no âmbito do domicílio

O âmbito de proteção do art. 13 da LF é afetado se houver uma intervenção no domicílio (ver IV 2b acima). Além disso, há obstáculos especiais para as intervenções, em particular as do § 4. No entanto, é duvidoso que o art. 13 da LF possa garantir a proteção de forma abrangente e adequadamente diferenciada, em particular se a proteção espacial do art. 13 da LF possa causar problemas específicos de infiltrações e alterações em sistemas de tecnologia da informação registrados: art. 13 da LF concede proteção espacial e proteção comportamental referente ao espaço, mas não proteção funcional relacionada à infraestrutura de comunicação pessoal. Aliás, a proteção sob o art. 13 da LF só entraria em consideração se o hardware infiltrado estivesse em um domicílio, situação que nem sempre ocorre em especial com notebooks e smartphones, exemplificativamente.

Deve-se acrescentar, no entanto, que o art. 13 da Lei Fundamental assegura aspectos importantes de proteção, como proteção contra a medição de emissões eletromagnéticas para capturar palavras de código, contra

116 Já no BVerfGE 113, 348, 391 e seguintes, diz – porém com relação ao art. 10, § 1, da LF, que basicamente concede uma proteção mais fraca do que o direito fundamental recentemente concretizado – "No caso concreto há indicações reais para a suposição de que uma vigilância de telecomunicações. Se for registrado conteúdo pertencente a esse núcleo essencial, ele não pode ser justificado e deve ser omitido". A palavra "captura" é usada aqui, mas não com base no fato de que a comunicação "sozinha" contém conteúdo na área central da vida privada. Essa afirmação não foi corrigida pela sentença da busca online.

intrusão na residência, por exemplo, para fins de manipulação do dispositivo, ou contra o acionamento de câmeras e microfones em computadores para monitoramento de atividades no domicílio[117]. Tais medidas constituem também uma intervenção independente que carece de justificação no domínio da proteção do art. 13, § 1º, da Lei Fundamental quando servirem à implementação prática da infiltração de sistemas de tecnologia da informação, tal como uma "busca online". O domínio da proteção dos direitos fundamentais da confidencialidade e integridade dos sistemas de tecnologia da informação não deve ser mal interpretado como se fosse suprimir as garantias dos direitos fundamentais que são afetados paralelamente, de modo que as medidas seriam admissíveis em anexo, na medida em que servem para implementar uma intervenção em um sistema de tecnologia da informação e isso seja permissível como tal – em relação ao padrão de garantia de proteção da personalidade de que trata aqui. De um lado, tal "solução do anexo" não faria justiça ao estatuto do direito fundamental de inviolabilidade do domicílio, que é particularmente protegido pela constituição, por exemplo com uma reserva judicial garantida. De outro, ela também não pode convencer sistematicamente, uma vez que a infiltração de sistemas de tecnologia da informação é tecnicamente possível sem entrar no domicílio[118].

VII.2 Concorrência com o sigilo de telecomunicação especialmente com as TKU-fonte

Existe uma situação de concorrência entre o art. 10 da Lei Fundamental e o direito fundamental à garantia da confidencialidade e integridade dos sistemas de tecnologia da informação, particularmente no caso de monitoramento de telecomunicações na fonte (TKÜ-fonte). O monitoramento de telecomunicações na fonte é um processo de monitoramento que registra as telecomunicações de saída antes da criptografia ou as telecomunicações de entrada após a decifragem pelo destinatário. Enquanto o monitoramento de telecomunicações costumava ocorrer e ser bem-sucedido no período de transmissão na rede – especificamente no caminho de transmissão –, isso não é mais possível com a transmissão digitalizada e o uso de criptografia.

117 Ver – embora não para todos os exemplos mencionados acima – BVerfG (nota 17), parágrafo 193.

118 Sobre o lado técnico, consulte Buermeyer HRRS 2007, 154, 163 e ss. Böckenförde JZ 2008, 925, 933 nota de rodapé 95 enfatiza que o acesso online, sujeito aos princípios da proporcionalidade, pode superar a instalação de hardware na residência.

No entanto, ainda falta clareza sobre a segurança contra a escuta de tecnologias individuais de Voice-over-IP[119].

O monitoramento de telecomunicações na fonte pode levar a perigos que vão além do monitoramento das telecomunicações em andamento durante a transmissão da rede[120]. O Tribunal Constitucional assumiu que as situações de ameaça não podem ser combatidas de forma adequada pelo art. 10º, § 1, da Lei Fundamental, porque existem dados que, na sequência de uma infiltração, são coletados sem referência a telecomunicação em curso. Ao mesmo tempo, afirmou que o art. 10 da LF é o único padrão de teste, desde que apenas a telecomunicação em andamento seja abrangida. A ideia básica dessa declaração é que a circunstância técnica de se o monitoramento ocorreu durante a transmissão da rede ou no terminal pode não ter nenhum significado para a atribuição do art. 10 da LF se a intervenção se limitar à captura da comunicação corrente e, portanto, o potencial de risco específico para a confidencialidade e integridade de sistemas complexos de tecnologia da informação não é ativado. No entanto, o Senado acrescentou que essa restrição deve ser resguardada por precauções técnicas e também garantida em termos legais[121].

No entanto, é duvidoso que tais precauções técnicas sejam possíveis atualmente. Na audiência de 10 de outubro de 2007, diversos especialistas ouvidos pelo tribunal negaram; na literatura, existem também vozes afirmativas[122]. No entanto, já há dúvidas se é praticamente possível se infiltrar em um sistema de tecnologia da informação sem obter um mínimo de informações – por exemplo, sobre seus pontos fracos; o conhecimento de tais pontos fracos podem desencadear novas ameaças. Acima de tudo, há dúvidas se as arquiteturas atuais ou previsíveis de computador permitem tal limitação de acesso: uma vez que um software é executado em um sistema, ele pode basicamente ser usado universalmente.

---

119 O software "Skype", por exemplo, há muito é considerado à prova de bugs e um excelente exemplo da necessidade de telecomunicações de origem. Entretanto, há evidências crescentes de que existe uma "chave duplicada" que também pode ser usada pelas autoridades para o processo de criptografia secreta, de modo que a escuta secreta também seria possível sem uma fonte TKÜ; consulte http://www.heise.de/newsticker/meldung/113 281.

120 BVerfG (nota de rodapé 17), número de margem 188 e ss.

121 BVerfG (nota de rodapé 17), número de margem 190.

122 Em sentido afirmativo, por exemplo, Bär MMR 2008, 423, que considera a existência de um software especial que só se abre quando as chamadas são efetivamente feitas e não requer o acesso a quaisquer outros dados do computador. No entanto, esta é a redação do art. 20 l, § 2º, Cláusula 1, nº 2 do Projeto de Lei do BKA, BR-Drs. 404/08 AC 5 de junho de 2008.

Os requisitos para que uma medida afete apenas o âmbito de proteção do art. 10 da LF e, portanto, para que somente esta norma seja a norma de teste não são atendidos em nenhum caso se a vigilância das telecomunicações estiver dependente de uma infiltração no sistema de tecnologia da informação, o que causa e pode causar intervenções relevantes à personalidade. O mesmo se aplica se o risco de uma alteração técnica no sistema for criado por infiltração ou como resultado do seu uso por terceiros. Essas ameaças à proteção da privacidade não podem ser defendidas apenas com o art. 10 da LF.

O teste à luz do direito fundamental à garantia da confidencialidade e integridade dos próprios sistemas informáticos também não é dispensável se a intervenção apenas ocorre quando é "necessária" para permitir o monitoramento e a captura das telecomunicações de forma não criptografada[123]. Em particular, a proteção mais rígida para sistemas de tecnologia da informação não é removida pelo fato de que uma medida de monitoramento de telecomunicações não pode ser realizada com sucesso sem tais intervenções.

A proteção também não é invalidada pelo fato de que a interferência pode ser posteriormente revertida[124]. Se a integridade e a confidencialidade dos sistemas de tecnologia da informação forem ameaçadas ou mesmo afetadas pela interferência, então a proteção dos direitos fundamentais é ativada sem que isso possa ser revertido pela eliminação posterior das consequências da ingerência – para além do fato de que, do ponto de vista técnico, de acordo com as declarações dos peritos ouvidos pelo Tribunal Constitucional, um restabelecimento total do status quo ante não deve ser viável. Portanto, requisitos especiais materiais e procedimentais também são necessários para um monitoramento de telecomunicações na fonte. Normas como o art. 100a do Código de Processo Penal, que foram criadas para a vigilância das telecomunicações tradicionais, também não contêm autorizações para intervenções dessa intensidade particular; eles também não têm uma limitação para um monitoramento na fonte "puro", ou seja, uma salvaguarda legal de que o monitoramento das telecomunicações será limitado à comunicação em curso e que isso será tecnicamente garantido[125]. Com

123 No entanto, esta é a redação do art. 20 l, parágrafo 2, cláusula 1, nº 2 do Projeto de Lei do BKA, BR-Drs. 404/08 AC 5 de junho de 2008.

124 A aceitação por trás da Seção 20 l, § 2º, cláusula 2 c/c a Seção 20k, § 2, cláusula 1, nº 2 do Projeto de Lei BKA parece ser diferente (nota 119).

125 Isto não é referenciado – Bär MMR 2008, 326.

base neles, não são observados os requisitos das limitações que o Tribunal Constitucional Federal formulou sobre o direito fundamental à garantia da confidencialidade e integridade dos próprios sistemas informáticos.

CONCLUSÃO

Em síntese, pode-se afirmar que o Tribunal Constitucional Federal, ao destacar uma necessidade especial de proteção dos sistemas de informática de uso próprio, tem respondido a um potencial de risco particular decorrente do desenvolvimento da informática, de constelações de rede, de muitos novos serviços e das possibilidades de infiltração e manipulação com base neles. O objetivo da proteção continua sendo a proteção da personalidade como base para o desenvolvimento autodeterminado. O tribunal afirmou uma necessidade fundada constitucionalmente de uma salvaguarda especial da confidencialidade e da integridade de sistemas de tecnologia da informação complexos e de uso próprio, que são especialmente importantes para a liberdade de desenvolvimento pessoal nas condições atuais, nas quais a pessoa afetada confia sem esperar poder controlá-los. A proteção oferecida é dirigida contra influências no próprio sistema de tecnologia da informação, mas também abrange a coleta e posterior utilização dos dados por meio de uma infiltração correspondente no sistema de tecnologia da informação. A Constituição não exige uma proibição estrita de tais influências, mas as vincula a requisitos especiais de natureza substantiva e processual.

Em sua decisão sobre buscas online, o Tribunal Constitucional não criou um novo direito fundamental, mas concretizou o direito fundamental há muito reconhecido à proteção da privacidade por meio de uma outra diferenciação. Nesse contexto, o Tribunal, que deve ser cauteloso quanto ao obiter dicta, não pôde se posicionar sobre todas as questões ainda em aberto. A jurisprudência e a ciência do Direito, mas também o legislador, são agora chamados a elaborar os demais contornos da proteção do direito fundamental.

POSFÁCIO

O direito fundamental à garantia da confidencialidade e da integridade dos sistemas de tecnologia da informação formulado pelo Tribunal Constitucional Federal (BVerfG) em 2008, conforme apresentado em meu artigo agora traduzido, já é parte integrante e sedimentado no sistema jurídico alemão. Inicialmente, foram manifestadas críticas a essa construção

elaborada pelo Tribunal[126]. Hoje, existe uma ampla aprovação a este respeito. A jurisprudência dos Tribunais e a literatura científico-acadêmica, bem como a prática e os legisladores têm seguido neste sentido o Tribunal Constitucional alemão. Foram publicadas várias monografias sobre este direito fundamental que tratam exclusivamente sobre ele[127], mas igualmente muitas outras obras que o fazem em relação a outros temas, bem como um grande número de artigos científicos e discussões nos comentários à Lei Fundamental.

Como resultado do desenvolvimento da transformação digital e do uso de sistemas de tecnologia da informação em praticamente todas as áreas da vida, cresceu a consciência de que a interferência nos sistemas de tecnologia da informação pode ter consequências especialmente graves. Seria falta de visão tomar apenas precauções contra intervenções específicas, como medidas concernentes a pesquisas individuais. Essa proteção seletiva deixaria lacunas consideráveis na proteção. A este respeito, faz sentido focar na proteção do sistema, ou seja, em particular na funcionalidade técnica e social dos sistemas de tecnologia da informação, como um pré-requisito para seu uso autônomo para diferentes fins.

Em 2016, o Tribunal Constitucional Federal, além das afirmações de 2008, deixou claro em decisão de revisão da constitucionalidade da lei da Polícia Criminal Federal[128] que os sistemas de informática protegidos não incluem apenas os computadores pessoais dos afetados, mas também aqueles que estão em rede com sistemas de TI de terceiros que funcionam com computadores, por exemplo, na utilização das assim chamadas nuvens[129]. O Tribunal enfatizou expressamente que os dados que são terceirizados para servidores externos com uma confiança legítima na confidencialidade são cobertos pela proteção. Esta é uma reação clara aos perigos associados às possibilidades de aplicação ampliadas e, acima de tudo, à rede de tecnologias digitais.

126 Ver a nota 66 do meu artigo.

127 WEHAGE, Jan-Christoph. O direito fundamental de garantir a confidencialidade e integridade dos sistemas de tecnologia da informação e seus efeitos no direito civil (2013); HEINEMANN, Marcus. Proteção dos sistemas de tecnologia da informação sob direitos fundamentais: com atenção especial ao direito fundamental de garantir a confidencialidade e integridade dos sistemas de tecnologia da informação (2015); HAUSER, Markus. The IT Basic Right: Interfaces and Effects (Duncker & Humblot, 2015); TARAZ, Daniel. O direito fundamental à garantia da confidencialidade e integridade dos sistemas informáticos e à garantia da privacidade digital no âmbito dos direitos fundamentais: preparando o caminho para o digital.

128 BVerfGE 141, 220, 303 e ss.

129 BVerfGE 141, 220, 304.

Uma vez que o novo direito formulado – geralmente denominado direito fundamental computacional – tem a sua base constitucional nos arts. 1º e 2º da Lei Fundamental (proteção da dignidade humana e proteção da personalidade), a garantia dos direitos fundamentais derivados destas normas contém ambas as garantias jurídico-subjetivas e jurídico-objetivas da proteção[130]. O nível jurídico-objetivo da proteção dos direitos fundamentais visa moldar o sistema jurídico de proteção da liberdade e, portanto, é dirigido, em particular, como mandato ao legislador federal e estadual, para tomar medidas de proteção no sistema jurídico. O Tribunal Constitucional Federal enfatiza que a função de proteção jurídico-objetiva não apenas vincula o Estado, mas também afeta a relação entre os particulares. Segundo o entendimento jurídico alemão, isso ocorre no decurso do chamado efeito indireto de terceiros ou efeito horizontal dos direitos fundamentais. Como resultado, a vinculação dos direitos fundamentais também pode entrar em vigor em disputas de direito civil[131].

O Tribunal Constitucional acentua que os efeitos das possibilidades técnicas de processamento de dados estão se tornando cada vez mais importantes para o relacionamento entre particulares. Os serviços básicos para o público em geral com base em extensas coletas de dados pessoais e medidas de processamento de dados seriam fornecidos por empresas privadas, muitas vezes poderosas. Estas tiveram uma influência duradoura na formação da opinião pública, na atribuição e negação de oportunidades, na participação na vida social e nas atividades elementares da vida cotidiana. Tendo em vista a possibilidade de manipulação, reprodução e a possibilidade temporal e espacialmente praticamente ilimitada de disseminação de dados, bem como sua recombinação imprevisível em processos não transparentes, os cidadãos individuais ficaram em dependências de longo alcance. A Constituição alemã oferece proteção contra isso.

O Tribunal vai um passo além e aponta que o impacto do direito fundamental na área de ação privada é particularmente importante se as empresas privadas passarem para uma posição dominante semelhante à do Estado ou se assumirem a provisão do quadro para o setor público de comunicação. Neste contexto, a vinculação dos direitos fundamentais de indivíduos privados seria próxima ou igual a uma vinculação dos direitos funda-

130 BVerfGE 152, 152, número de margem 85 – 88.

131 Aqui e para a sequência BVerfGE 152, 152, número de margem 85.

mentais do Estado em específico[132]. Estas últimas declarações não se referem especificamente à proteção dos sistemas de tecnologia da informação, mas devem ser entendidas de forma que tais empresas também tenham que observar as obrigações de proteção dos direitos fundamentais a esse respeito.

Em outra decisão de 8 de julho de 2021[133], o tribunal especificou a obrigação do Estado de fornecer proteção em mais detalhes, no sentido de que o Estado tem a obrigação de ajudar a garantir que a integridade e confidencialidade dos sistemas de tecnologia da informação sejam protegidos contra ataques de terceiros[134]. Este mandato de proteção é condensado em uma obrigação de proteção concreta sob os direitos fundamentais se o Estado estiver ciente das lacunas de segurança nos sistemas de tecnologia da informação que podem ser usadas por terceiros para se infiltrar nesses sistemas e pesquisar as informações neles encontradas. Ao acessar todo o banco de dados de um sistema de tecnologia da informação, este também pode ser manipulado e os perpetradores podem ameaçar de modo extorsivo a manipulação, em particular mediante a destruição de dados. Voltarei a isso em um momento posterior. Essa aplicação de proteção concentrada é acionada em particular pelo alto risco e potencial de danos das brechas de segurança.

A Corte Constitucional alemã também justifica a necessidade de proteção daqueles que confiam os dados a sistemas de tecnologia da informação com o fato de que os indivíduos são frequentemente dependentes de tais sistemas, e, portanto, a suposição é irreal de que eles poderiam evitar a espionagem, abstendo-se de usar meios digitais de comunicação[135].

Para além deste dever de proteção, o Tribunal destaca ainda que, em casos excepcionais, pode justificar-se que os órgãos do Estado autorizem a existência de lacuna de segurança de que são conhecidos e, por sua vez, o acesso aos sistemas de dados deste sistema. No entanto, isto só é permitido a título de exceção, designadamente com o objetivo de evitar perigos particularmente graves, em especial os perigos do terrorismo internacional. Para fazer uso dessa exceção, é necessária uma autorização legal expressa, na qual são elencados requisitos de justificação adicionais.

132 BVerfGE 152, 152, número de margem 88.

133 BVerfG, decisão de 08.06.2021, Beck RS 2021, 19234, número de margem 26 e ss.

134 Op. cit., número de margem 35.

135 Op. cit., número de margem 33.

Já mencionei que a necessidade de proteção é desencadeada pela expansão dos potenciais de risco associados às tecnologias digitais. A inteligência artificial amplia o potencial de perigos, mas, por outro lado, também contém possibilidades de reconhecer e combater tais ataques. Fala-se, neste contexto, do potencial de uso duplo da IA. O âmbito da proteção do direito fundamental à integridade e à confidencialidade dos sistemas de tecnologia da informação também inclui ameaças que recentemente chamaram particular atenção. Refiro-me ao uso direcionado de spyware, como o software Pegasus. Isso permite, entre outras coisas – como ficou conhecido em 2021[136] –, o monitoramento remoto de smartphones. Para tanto, são utilizadas lacunas de segurança no software, algumas das quais foram criadas por solicitação expressa dos usuários do software ou foram deliberadamente deixadas após serem detectadas. O spyware suportado por IA tem sido usado em grande escala por várias instituições (privadas, mas também estatais estrangeiras) para espionagem ilegal, em particular de políticos de alto escalão, ativistas de direitos humanos e jornalistas. O fabricante israelense da tecnologia de vigilância – o Grupo NSO – confiou no fato de que a empresa proíbe os compradores do software de uso ilegal e sanciona-o caso se torne conhecido. Isso não parece ter sido muito eficaz.

O problema é particularmente sério quando o "sequestro" de sistemas de tecnologia da informação pode ter consequências para grandes partes da sociedade, por exemplo, paralisando o fornecimento de energia ou água, ou mesmo interrompendo cadeias importantes de abastecimento[137]. Os sistemas de tecnologia da informação usados na produção industrial também podem ser afetados. Mais recentemente, foram conhecidos casos em que sistemas de tecnologia da informação foram hackeados para exigir um alto valor de resgate pela "descriptografia" do software malicioso, que também foi pago por um alto valor.

Os militares também dependem de sistemas de tecnologia da informação. A infiltração em seus sistemas de tecnologia da informação pode, por exemplo, bloquear infraestruturas militarmente importantes ou prejudicar a funcionalidade dos sistemas de armas.

136 Cf., por exemplo, as reportagnes no Jornal Süddeutschen de 20.07.2021, nº 164, S. 9 – 11 assim como do dia 21.07.2021, nº 165, p. 1, 8 e ss.

137 Um exemplo é o ataque perpetrado no ano de 2021 Supply-Chain, que foi efetivado no software do servidor Casey, provavelmente pelo grupo Hacker REvil.

São acréscimos que não estão diretamente relacionados às questões tratadas no ensaio monográfico. Mas, mesmo no momento do seu desenvolvimento, é necessário demonstrar – como em 2008 – que os direitos fundamentais devem ser interpretados de forma dinâmica. Isso significa que eles podem ou mesmo devem reagir às mudanças em sua área real – aqui, às mudanças nas tecnologias e às novas ameaças associadas. A proteção do sistema se tornou cada vez mais importante em tempos de transformação digital. O Estado deve proteger esses sistemas, determinar que os particulares o façam, bem como monitorar o cumprimento dessas obrigações pela autoridade pública.

Sobre o autor:

Wolfgang Hoffmann-Riem

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, 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, é Membro alemão da "Comissão Europeia para a Democracia através do Direito" (Comissão de Veneza) do Conselho da Europa.

Sobre o tradutor e a revisora técnica:

Italo Roberto Fuhrmann

Doutorando em Direito pela PUCRS. Advogado.

Jacqueline de Souza Abreu

Doutoranda em Direito na Faculdade de Direito da Universidade de São Paulo. Advogada. Mestra em Direito pela University of California, Berkeley (EUA), com foco em Direito e Tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em Direitos Fundamentais. Graduada em direito pela Universidade de São Paulo. Cocoordenadora do Dossiê "Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal", da *Revista de Direito Público*, do IDP.

Artigo convidado.