A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da informação

The protection of fundamental rights of confidentiality and integrity of information technology systems

Wolfgang Hoffmann-Riem
Catedrático Emérito de Direito Público da Faculdade de Direito da Universidade de Hamburgo (Alemanha). Juiz do Tribunal Constitucional Federal da Alemanha (1999-2008).
wolfgang.hoffmann-riem(@law-school.de

Tradução de
Pedro Henrique Ribeiro
Doutorando em Teoria do Direito – Faculdade de Direito da Universidade de Frankfurt (Alemanha).
ribeiroph@gmail.com

Recebido em: 27.08.2019
Aprovado em: 17.03.2020

Áreas do Direito: Constitucional; Digital

Resumo: O presente estudo trata do panorama da proteção dos direitos fundamentais na Alemanha em face dos avanços tecnológicos que se revelam no desenvolvimento dos sistemas próprios de tecnologia da informação. Partindo da análise do famoso julgado pelo Tribunal Constitucional Federal Alemão em 1983 acerca da coleta de dados da população para fins censitários, que reconheceu um direito fundamental à autodeterminação informativa, são analisadas necessidades e oportunidades de proteção de direitos fundamentais, incluindo a proteção da confiança em sistemas informáticos, desde que relevantes à personalidade, bem como as diversas normas presentes na Lei Fundamental Alemã pertinentes à proteção de direitos fundamentais.

Abstract: The present analyzes the panorama of protection of fundamental rights in Germany in light of the technology advancement revealed by the recent development of information technology systems. Initially, the paper analyzes the famous trial held in 1983 ruled by the German Federal Constitutional Court, regarding the gathering of population data for census purposes, by which it was recognized a fundamental right to informational self-determination. Then, the paper analyses some necessities and possibilities for the protection of fundamental rights in connection with the subject of the paper, including the protection of confidence in systems information technology, as long as such necessities and possibilities are relevant to the

Hoffmann-Riem, Wolfgang. A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da informação. Ribeiro, Pedro Henrique (trad.). *Revista de Direito Civil Contemporâneo.* vol. 23. ano 7. p. 329-365. São Paulo: Ed. RT, abr.-jun./2020.

Por fim, são analisados limites a essa proteção e a concorrência entre normas distintas de proteção de direitos fundamentais.

Palavras-chave: Direitos fundamentais – Sistemas de tecnologia da informação – Autodeterminação informativa – Direitos da personalidade – Direito alemão.

personality right spectrum. In sequence, the paper analyzes certain provisions relevant to the protection of fundamental rights that are within the German Constitution, and ultimately, limits to such protection as well as conflicts between different provisions for the protection of fundamental rights on German Constitution.

Keywords: Fundamental rights – Information technology systems – Informational self-determination – Personality rights – German law.

I. Os primórdios da decisão sobre o recenseamento populacional e sua relevância contínua

O dia 15 de dezembro de 1983 – já passado um quarto de século – foi um grande dia para a expansão da proteção de direitos fundamentais na Alemanha: A decisão sobre o recenseamento da população do Tribunal Constitucional Alemão (*Volkszählungsurteil*

des BVerfG.)[1] foi proferida nessa data. Nela foi reconhecido o "direito fundamental à autodeterminação informativa" como um subcaso da proteção constitucional ao direito de personalidade. Aqueles que lerem a referida decisão nos dias de hoje poderão se surpreender com o fato de que um censo (*Volkszählung),* ou seja, uma coleta estatística de informações, tais como nome, endereço, meios de sustento, profissão e outros "dados"[2] semelhantes, tenha causado tamanha comoção e, ao mesmo tempo, estimulado uma decisão tão paradigmática como essa.

Pode ser que o ano de 1984, que estava então para chegar e que tinha sido escolhido por *Orwell* como título de seu livro futurista sobre um Estado de controle e vigilância total por meio do "Big Brother", tenha dado asas às fantasias de então e desempenhado um papel relevante nas consequências da decisão em pauta. Naquele tempo, a tecnologia computacional se encontrava ainda em seus estágios mais iniciais. A difusão de dados ocorria em grande medida por grandes computadores centrais que, a partir da perspectiva atual, eram pesados, volumosos, lentos e, sobretudo, com baixíssima capacidade de armazenamento de dados. O computador de bom desempenho e com bom custo-benefício que estivesse à disposição do homem médio – como agora é o caso do PC – estava ainda no início de seu desenvolvimento, algo que, tal qual ocorre atualmente com os *smartphones*, incentivava o crescimento de fantasias. Para se chegar à capacidade de armazenamento de um pequeno *pen-drive* USB atual eram necessárias, nessa época, grandes máquinas imóveis. Como resultado, a consciência ainda não tinha se ajustado à enorme expansão das oportunidades comunicativas de ação que o computador possibilitaria nos anos seguintes, especialmente graças à rede internacional de computadores privados e ao desenvolvimento da Internet. O que estava no centro das discussões públicas,

1. Ver BVerfGE 65, 1. [Nota do Tradutor - N.T.: BVerfGE = Decisão (Acórdão) do BVerfG; BVerfG = Bundesverfassungsgericht = Tribunal Constitucional Alemão]. Nota do Editor (N.E): Manteve-se a notação bibliográfica original. N.T.: Esta contribuição trata de uma versão expandida e melhorada de uma palestra realizada em um evento sobre proteção de dados organizado pela Friedrich-Ebert-Stiftung, que ocorreu em Berlim em 1º de julho de 2008. Agradecimentos, por auxílios e estímulos, são devidos a Marion Albers, Matthias Bäcker e Ulf Buermeyer. A contribuição foi publicada in: *Juristenzeitung* 2008, S. 1009-1022.

2. Em sua decisão sobre o recenseamento popular, o Tribunal Constitucional Alemão *(BVerfG)* valeu-se do conceito de "dados" em um contexto no qual parte da literatura informacional-técnica, na verdade, utiliza o conceito de "informação". Sobre o assunto, entre muitos, ver *Albers*, Informationelle Selbstbestimmung, 2005. p. 87 s.; *Vesting*. In: Hoffmann-Riem/Schmidt-Aßmann/ Vosskuhle (Org.) Grundlagen des Verwaltungsrechts. 2008. v. 2. § 20. nota marginal n. 11 s. A seguir, de acordo com a práxis da literatura jurídica, utilizar-se-á o conceito de dados; mantendo-se, contudo, também o uso do conceito de informação quando se trata de literatura científica ou técnico-informacional. Dados são símbolos objetificados; informações dotadas de sentido formadas nos receptores ou em sistemas de comunicação (Ver Albers, op. cit., p. 141 s.). A proteção de dados é uma dimensão protetiva dos direitos fundamentais à autodeterminação informativa, bem como ao direito fundamental da confiabilidade e integridade de sistemas de tecnologia da informação próprios. Ademais, os dados também são protegidos, na medida em que eles transportam informações que contêm uma expressão de vontade implícita.

contudo, não eram tais oportunidades e novidades, mas sim as ameaças à liberdade por parte do Estado na coleta e no processamento de dados. Embora os dados coletados pelo recenseamento devessem permanecer anônimos, reconheceu-se então o risco de sua individualização e o risco de abusos possíveis e decorrentes, daí se pautaram as discussões.

Em termos da dogmática dos direitos fundamentais, o objetivo era ativar a proteção da defesa de um direito fundamental que tinha, primeiro, de ganhar forma e contornos. O Tribunal Constitucional Alemão (*BVerfG*) conseguiu cunhar a ideia básica em poucas palavras, que até hoje não perderam quase nada de sua expressividade.[3] O direito geral de personalidade garantido nas disposições do Artigo 2, parágrafo 1, em conjunto com o Artigo 1, parágrafo 1, da Lei Fundamental[4] poderia

> "também ganhar em importância face aos desenvolvimentos modernos e aos novos perigos à personalidade humana a eles associados. As concretizações anteriores pela jurisprudência não descreviam de forma suficiente conclusiva o conteúdo do direito de personalidade. O direito de personalidade inclui também a faculdade do indivíduo, derivada da ideia de autodeterminação, de decidir por si mesmo, em princípio, quando e dentro de que limites as circunstâncias pessoais de sua vida podem ser reveladas ou abertas. Tal direito à 'autodeterminação informativa' não é garantido de forma ilimitada. O indivíduo não tem um direito no sentido de um domínio absoluto e irrestrito sobre 'seus' dados; ele é uma personalidade que se desenvolve no seio da comunidade social e depende da comunicação."

A dogmática de direitos fundamentais baseada no direito de defesa (*abwehrrechtlich fundierte Dogmatik)* classificava a atividade do Estado como uma intervenção na posição de direito individual, que, em última análise, agia como um direito aos seus próprios dados,[5] cuja divulgação e utilização deveria ser deixada livre para o indivíduo decidir – em-

3. As citações seguintes provêm de BVerfGE 65, 1, 41-44 (omissões não foram marcadas).

4. *Britz* (Freie Entfaltung durch Selbstdarstellung, 2007, esp. p. 25, s), partindo de argumentos consideravelmente convincentes, é cética nesse ponto e duvida de que seja necessário ou relevante fazer uso também do artigo 1º da GG [N.T.: Grundgesetzt; Lei Fundamental ou Constituição Alemã] como fundamentação do direito geral de personalidade. Em todo caso, pode ser necessário derivar a proteção de dados do artigo 2.1 da Lei Fundamental – na medida em que se trataria de uma proteção da personalidade relacionada com a dignidade humana, desde que outros direitos fundamentais – como os artigos 12.º e 14.º da Lei Fundamental – não sejam afetados.

5. Crítico a esse ponto: *Hoffmann-Riem*, AöR 123, 1998 513, 520, com maiores referências. Para uma crítica mais detalhada e fundamental à construção desenvolvida pelo Tribunal Constitucional Alemão, ver: *Albers* (nota de rodapé n. 2), p. 238 e passim. A noção de direito aos próprios dados é de fato inadequada quando se trata de dados sobre informações que fornecem exposição sobre a conduta de várias pessoas, sem que o interesse de uma das pessoas afetadas, por si só, mereça proteção jurídica. Isso é ainda mais difícil com a atribuição de um dado a uma pessoa, quando seu valor informacional é obtido a partir da combinação com outros dados que são ou foram gerados por outras pessoas.

bora reconhecendo o seu envolvimento em contextos sociais. Tratando-se de uma questão de defesa contra a intervenção do Estado, a decisão se estabeleceu enfocada na relação entre Estado e cidadão.

O fato de que ainda exista necessidade de proteção nesse âmbito é algo ilustrado pelas numerosas autorizações de acesso a dados com vistas a garantir a segurança pública e a repressão de infrações penais, algo que se encontra cada vez mais presente nas leis policiais e de proteção constitucional, bem como nas normas penais, muitas delas criadas (também) como meio de defesa contra o terrorismo, principalmente após o 11 de Setembro de 2001. O fato de algumas dessas autorizações, ou pelo menos sua aplicação no caso específico, terem sido consideradas inconstitucionais pelo Tribunal Constitucional Alemão nos últimos anos – e, em particular, também como uma violação do direito fundamental à autodeterminação informativa[6] – sinaliza a importância contínua da proteção de defesa contra intervenção estatal (*des abwehrrechtlichen Schutzes)*.

II. Mudanças dos perigos e das oportunidades trazidas pelas tecnologias da comunicação

1. Oportunidades e riscos

Em comparação com o momento da decisão sobre o recenseamento populacional (*Volkszählungsurteils)*, a constelação dos perigos potenciais alterou-se fundamentalmente, assim como as oportunidades abertas pelo uso comunicativo da eletrônica para o desenvolvimento individual e coletivo aumentaram enormemente. Hoje, praticamente todos têm acesso a computadores poderosos; cerca de 35 milhões de alemães usam a rede global da Internet. Em julho de 2008, havia mais de 860 milhões de usuários de Internet em todo o mundo. O que é mais marcante, agora, não é mais o armazenamento central de dados, mas sim o uso descentralizado e a rede de sistemas de computador descentralizados, acessíveis global e repetidamente, além de serem de alto desempenho. Juntamente com a tecnologia informática, a digitalização trouxe – também relacionada com a globalização – uma evolução comunicativa que não é em nada inferior, em seu significado para o desenvolvimento social, ao significado que teve a revolução industrial do século XIX.

Grandes e pequenos computadores e as correspondentes infraestruturas de comunicação de tecnologia da informação tornaram-se forças produtivas centrais em praticamente todos os âmbitos da vida, seja para a formação do mundo privado, seja para o cumprimento de tarefas pelo Estado e pelas empresas de negócios na economia. As tecnologias da comunicação moldam o exercício real dos direitos fundamentais em

6. Ver, com especial atenção, BVerfGE 115, 320 s. (decisão *Rasterfahndung*), bem como BVerfGE, Acórdão de 11. 5. 2008 – 1 BvR 2074/05, 1 BvR 1254/07 = NJW 2008, 1505 s.

praticamente todos os âmbitos da vida.[7] Grande parte dessas tecnologias e serviços eram desconhecidos ao tempo do acórdão sobre o recenciamento populacional (*Volkszählungsurteils*); por exemplo, ISDN, RFID, WLAN, UMTS; serviços como o comércio eletrônico (*e-commerce)*, o governo eletrônico (*e-government*), os sistemas de navegação; redes sociais, como o StudiVZ; e métodos de investigação, como o *scanning* automático de placas automóveis ou as investigações *on-line*.

O Estado tem apenas uma capacidade limitada para fornecer e garantir o funcionamento das infraestruturas de tecnologia da informação. Além disso, são sobretudo as empresas privadas, incluindo as que têm poder global – como a Google, a Microsoft ou as grandes empresas de telecomunicações – que são os garantes e portadores dessa infraestrutura de tecnologia da informação. Existem assimetrias de poder consideráveis entre as várias empresas e entre estas e seus cidadãos, mas também entre essas empresas e o Estado. O fato de a utilização do poder e os riscos associados de abuso de poder não estarem de modo algum apenas limitados ao Estado se torna cada vez mais evidente na consciência pública, por exemplo, quando se discute a enorme capacidade de armazenamento de dados e as opções de seleção disponíveis no Google,[8] ou quando se descobrem escândalos, tais como a utilização dos dados de ligação dos clientes da Deutsche Telekom para controlar seus próprios empregados,[9] ou para a venda ilegal de dados bancários.[10] Ao mesmo tempo, porém, o Estado acede aos dados, principalmente no domínio da prevenção de riscos e da defesa, bem como da ação penal, pelo que a proteção contra tais intervenções também deve ser concedida.

2. Necessidades e oportunidades de proteção

Os direitos fundamentais de proteção da personalidade, de liberdade de comunicação e de proteção do domicílio, que são decisivos no caso vertente, visam a proteção contra a intervenção do Estado, mas também contra as violações da liberdade por parte dos particulares.

---

7. Sobre a noção de *ubiquitous Computing* (computação ubíqua ou processamento de dados omnipresente), ver, entre muitos, *Kühling*, Die Verwaltung 40, 2007, 153 s., bem como as contribuições diversas na seguinte obra coletiva: *Roßnagel/Sommerlatte/Wienand* (Org.). Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien, 2008; ver, também, aqueloutras in: *Mattern* (Org.). Die Informatisierung des Alltags – Leben in smarten Umgebungen, 2007.

8. Sobre o assunto, entre muitas, ver *Maurer*, Informatik Spektrum 30, 2007, 273 s.

9. Sobre esse assim chamado escândalo da Telekom, ver *Süddeutsche Zeitung* de 29.05.2008. p. 2, bem como de 30.05.2008. p. 1 e *Scherer*, MMR, 2008, 433 s.

10. Ver, entre muitos, *Dams*, *Die Welt* vom 18.08.2008.

A liberdade de desenvolvimento comunicativo é particularmente afetada aqui. A liberdade de comunicação é uma liberdade usada na interação com as outras.[11] A esse respeito, a posição individual só pode ser descrita a partir da relação social. Um pensamento de dogmática de direitos fundamentais focado no indivíduo "solitário" não poderia compreender adequadamente as dimensões sociais da liberdade de comunicação e, portanto, os requisitos de proteção relacionados a ela. Na medida em que a comunicação pessoal é apoiada tecnologicamente, a proteção eficaz dos direitos fundamentais exige também a proteção da infraestrutura tecnológica de comunicação e a sua utilização concreta, na medida em que essa infraestrutura possa estar relacionada à liberdade do indivíduo. A funcionalidade não tem apenas um lado técnico, mas também um lado social, e pode ser influenciada normativamente, por exemplo, através da salvaguarda da liberdade de acesso, da liberdade de manipulação e, em geral, da proteção contra o uso unilateral do poder ou mesmo do abuso. As diferentes dimensões da capacidade funcional referem-se a diferentes potenciais de perigo e pessoas em perigo, bem como a diferentes atores que asseguram ou põem em perigo a capacidade funcional. Portanto, são necessários conceitos multipolares e multidimensionais de proteção da liberdade.

O Estado só pode assegurar o funcionamento das infraestruturas de comunicação em medida limitada – tanto devido ao alcance global das redes quanto também, principalmente, devido à predominância dos atores privados na criação e manutenção de redes com a prestação de serviços. Também estão envolvidos atores que estabelecem o seu próprio direito (como a ICANN).[12] No entanto, o Estado pode utilizar o seu poder legislativo no âmbito das normas que estabeleceu, eventualmente expandido de modo a incluir atos jurídicos intergovernamentais.

A salvaguarda dos verdadeiros pressupostos da liberdade de conduta – em particular da liberdade de comunicação – nas relações estabelecidas tecnologicamente em rede, pode ser conseguida não só estabelecendo normas estatais (ou privadas) de comportamento e controle, mas também de outras formas,[13] como através de disposições jurídicas que afetam o tipo de configuração do sistema de comunicação ou permitem a proteção tecnológica dos dados e a autoproteção, como a criptografia. A esse respeito, o Estado pode estabelecer incentivos, se necessário também por meio de proibições e ordens, para

11. De maneira geral, sobre esse conceito, ver, em especial, *Suhr*, Entfaltung des Menschen durch die Menschen, 1976; idem, EuGRZ 1984, 529, 537. Ver também – em continuação – *Albers* (Nota de rodapé n. 2) e *Britz* (Nota de rodapé n. 4). p. 45 s.

12. A Internet Corporation for Assigned Names and Numbers, com sede em Marina del Rey (Califórnia – EUA) administra as estruturas-chave da internet, ou seja, entre outros, a atribuição de blocos de endereços de IP (os assim chamados espaços de endereço) e os servidores DNS centrais que asseguram, funcionando tal qual uma "lista telefônica" da internet, a realização e concreção das entradas textuais de endereço (p. ex., [www.bundesverfassungsgericht.de]) para endereços de IP (no mesmo exemplo: 134.96.83.81).

13. Ver *Albers* (Nota de rodapé n. 2), esp. p. 466 s., 544 s.

trabalhar em estruturas que possam conduzir à ativação de distintas funções de proteção. Uma proteção de dados que não é apenas orientada pelo paradigma da autodeterminação na determinação do objetivo de proteção, mas também nas precauções de proteção, na medida do possível, esbarra nos seus limites factuais – e normativos – em que o indivíduo não tem possibilidades de proteção ou consciência da necessidade de proteger os seus dados pessoais.[14]

III. Em particular: proteção da confiança nos sistemas informáticos utilizados pelo próprio usuário

Atualmente, pode-se observar que as infraestruturas de comunicação das tecnologias da informação[15] estão recolhendo e tratando cada vez mais dados pessoais[16], por exemplo, em computadores de uso próprio: como um arquivo de informações a armazenar, para ajudar a realizar as próprias tarefas (escrita, contas, administração geral), como um meio de entretenimento (jogos de computador, biblioteca digital, biblioteca de áudio, biblioteca de vídeo) ou para controle (remoto) de sistemas de controle doméstico em "agregados familiares inteligentes"[17], e para a criação dos chamados veículos inteligentes[18]

14. A diferença entre a motivação das massas que se voltam contra o censo popular nos anos 1980, por um lado, e a prontidão atualmente muito difundida em redes sociais de se publicar e expor – até no mais privado dos detalhes – sua vida em redes sociais (como as plataformas SchülerVZ e StudiVZ); em programas de fidelização de clientes (p. ex., Payback) e em portais de internet, por outro, é uma diferença que limita adicionalmente as chances de realização de ajuda estatal para autoproteção; ainda que não a torne uma oferta indispensável. Veja, adiante, o item V 2 d.

15. Sobre as perspectivas de desenvolvimento, entre muitos, ver *Roßnagel*, Datenschutz im informatisierten Alltag, 2007. esp. p. 26 s. Sobre a necessidade de um quadro referencial transdisciplinar, ver *Rolf*, Mikropolis, 2010, 2008. p. 95 s.

16. Ver, entre muitos, *Kutscha*, NJW 2008, 1042, 1044.

17. O BVerfG já se referiu ao problema da vinculação *on-line* des aparelhos eletrodomésticos (incluído aí o controle remoto) na sua decisão sobre as pesquisas *on-line* (Acórdão de 27 de fevereiro de 2008 – 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822. Disponível em: [www.bundesverfassungsgericht.de]). Para uma ilustração prática disso, ver: *Bayerlein-Hoppe*, Elektrobörse Handel 02/2004, 12 s. Certamente, não é por acaso que a Feira Internacional de Eletrônica de Consumo de Berlim, em 2008, reorientou o seu conceito de tal forma que as precauções suportadas eletronicamente para "casas inteligentes" foram agora também integradas numa feira de comunicações.

18. Ver, especialmente, a iniciativa da União Europeia apresentada na Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões – Para uma mobilidade mais segura, mais ecológica e mais eficiente na Europa – Primeiro relatório sobre a Iniciativa "Veículo Inteligente" COM/2007/0541, final. Os sistemas de transporte inteligentes buscam, em especial, aumentar a segurança rodoviária e a eficiência energética e permitir uma maior utilização das tecnologias da informação e da comunicação que, ao mesmo

("Internet das Coisas").[19] Na aplicação *on-line*, o computador é ligado em rede com outros computadores e os dados nele contidos e gerados por ele também podem ser usados em outros computadores, se necessário. A integração em redes, principalmente na internet global, permite igualmente o acesso aos dados aí disponíveis, mas também aos serviços aí oferecidos quando se trabalha com o próprio computador, pelo que o utilizador muitas vezes não sabe que *software* está ainda "a seu serviço" ou que é utilizado para aceder à sua informação. Se, no futuro – como é de esperar –, as aplicações disponibilizadas através da Internet crescerem cada vez mais em conjunto com o crescimento dos *softwares* do computador utilizado (a chamada "computação em nuvem" – *cloud computing*[20] – ou "serviços em nuvem" – *services in the cloud*), a sua distribuição e diversidade e, consequentemente, também a complexidade e obscuridade para o utilizador continuarão a aumentar. A perda de controle é inevitável. Princípios normativos como a economia de dados e a prevenção de dados (§ 3a par. 1 BDSG)[NT] não se tornarão supérfluos, mas perderão a sua eficácia se a infraestrutura de rede for acedida – o que é praticamente inevitável para a utilização *on-line*.

O disco rígido de muitos PCs já fornece uma imagem que reflete de maneira precisa os interesses e inclinações pessoais, a situação econômica, bem como o estado e comportamento físico e psicológico de seus usuários.[21] No entanto, as informações sensíveis não são apenas "armazenadas" no seu próprio computador, mas também estão localizadas na própria rede. Aqueles que ganham acesso ao sistema de tecnologia da informação podem, de certa forma, ter acesso ao "cérebro externalizado"[22] ou mesmo à "psique externalizada", mas também obter acesso a muitas outras informações importantes sobre a personalidade afetada.

---

tempo, deverão permitir a transmissão de informações de veículo para veículo; entre veículo e infraestrutura; de veículo para sistemas de chamadas de emergência (incluindo disposições com monitoramento da localização precisa) etc., através de interfaces normalizadas dos sistemas de informação e comunicação a bordo. Ver, também, *Dencker*, zfs 2008, 423 s.; *Vieweg,* in: 45. VGT, 2007. p. 292 s.

19. *Ullinger/ten Hompel* (Org.), Internet der Dinge, 2007; *Fleisch/Mattern* (Org.), Das Internet der Dinge –Ubiquitous Computing und RFID in der Praxis, 2005. Ver, também, a nota de rodapé n. 7, *supra*.

20. Ver *David Chappell*, A Short Introduction to Cloud Platforms. An enterprise-oriented view, 2008. Disponível em: [www.davidchappell.com]. A "nuvem" (*cloud*) figura como metáfora para uma infraestrutura complexa, obscura e que se encontra em constante movimento. A comunicação baseada em rede pode aceder a essa infraestrutura sem que os usuários precisem se conhecer ou sequer controlar.

NT. Lei Federal Alemã de Proteção de Dados (*Bundesdatenschutzgesetz*).

21. Ver *Kutscha*, NJW 2008, 1043.

22. *Hassemer*, Süddeutsche Zeitung v. 11.06.2008, afirma: "o computador é uma parte do corpo externalizada".

Essa "vulnerabilidade" do direito de personalidade leva a exigências de proteção em dois âmbitos: tanto, por um lado (ainda e de forma continuada), no que diz respeito aos dados e à coleta de dados conhecidos pelo usuário; quanto, por outro lado, proteção daqueles dados resultantes de conteúdo gerados durante o processo de utilização juntamente com os dados (os dados funcionais) e possíveis utilizações que são frequentemente desconhecidos pelo usuário e que são gerados, seja de forma fugaz, seja de forma permanente. Tais salvaguardas adquirem relevância ao abrigo de cunho de direito fundamental, em especial na medida em que sejam necessárias para garantir a proteção da personalidade (relevância para a personalidade – *Persönlichkeitsrelevanz*).

1. Proteção da confiança

A proteção eficaz desses dados e da comunicação que os divulga deve abarcar não só a proteção contra o acesso a eles, mas também a proteção da confiança[23] de que os *hardware* e *software* utilizados e as infraestruturas de comunicação das tecnologias da informação utilizadas pelo usuário funcionam no seu conjunto,[24] ou seja, que funcionem não apenas tecnicamente, mas também nos contextos de aplicação; e que funcionem de tal forma que o usuário possa esperar tal funcionamento e o supor[25] e que, portanto, ele possa confiar na proteção dos dados armazenados ou comunicados pelas tecnologias da informação (confiança relacionada com o sistema).

As expectativas normativamente protegidas associadas à confiança incluem a confidencialidade fundamental do seu próprio sistema técnico-informático,[26] que é a base da confidencialidade da própria comunicação, ou seja, a proteção contra o acesso por parte

23. Para uma análise compreendente da confiança e suas dimensões, ver as contribuições em da obra coletiva *Klumpp* et al. (Org.), Informationelles Vertrauen für die Informationsgesellschaft, 2008. Não é possível adentrar, aqui, às diversas facetas do conceito de confiança, tampouco às teorias acerca da construção de confiabilidade. Para os modos de vista disciplinares diversos, ver: *Möllering*, in: Max-Planck-Institut für Gesellschaftsforschung, Jahrbuch 2007/2008. p. 73 s.

24. Trata-se, nesse sentido, de uma proteção à função. Ver *Hornung*, CR 2008, 299, 302. A proteção da função, do ponto de vista dos direitos fundamentais, deve ser compreendida como um meio para a proteção da personalidade.

25. Ver *Volkmann*, DVBl. 2008, 590, 592.

26. O conceito de sistemas de tecnologias da informação ainda não foi definido legalmente, O Tribunal Constitucional Alemao, *BVerfG,* (ver nota de rodapé n. 17) tomou esse conceito da literatura sobre sistemas de tecnologias da informação, cuja terminologia constava da legislação impugnada na decisão em causa. Uma das futuras tarefas jurídico-dogmáticas consistirá em descrever em mais pormenor as estruturas juridicamente relevantes dos "seus próprios sistemas informáticos" de uma forma que seja orientada para a relevância da proteção sistêmica da personalidade. Mesmo quando o BVerfG nem sempre fala de sistemas de tecnologia da informação "próprios" (melhor: autoutilizados), o contexto deixa claro que a proteção da personalidade é o ponto de referência decisivo para a proteção dos direitos fundamentais.

do Estado ou de terceiros.[27] No entanto, as expectativas de proteção abarcam também a integridade do sistema de tecnologia da informação, ou seja, a proteção contra a superação de obstáculos que protegem contra intrusões, bem como contra erros e manipulações,[28] tais como falsificações, adições por meio de dados adicionais ou de *software* que possa manipular o tratamento dos dados.[29] Há também necessidade de proteção contra a manipulação do *hardware* utilizado, bem como contra infiltração e manipulação dos programas que (como o sistema operativo ou o *software* do usuário) permitem acesso de terceiros a esse sistema ou às funcionalidades dele.

O *BVerfG* se vale do conceito "sistema de tecnologia da informação" como um termo constitucional, cujos contornos ainda precisam ser definidos e não podem, de forma alguma, ser retirados apenas da literatura de tecnologia da informação. Ele deixa claro que a necessidade especial de proteção apenas existe para sistemas informáticos complexos, e não para sistemas tais como de controle eletrônico não ligados em rede para a tecnologia doméstica.[30] Tal necessidade de proteção, portanto, compreende, sim, os computadores pessoais ligados em rede, os telefones celulares mais complexos e assistentes digitais pessoais (PDA).[31] Um *pen-drive* USB conectado ao computador ou um disco rígido externo conectado também pode satisfazer aos requisitos de alta complexidade de forma suficiente.[32]

2. Relevância para a personalidade

No entanto, o sistema informático não está protegido por direitos fundamentais por si só,[33] mas apenas na medida em que a sua confidencialidade e integridade impliquem relevância para a personalidade.[34] Tal relevância, por sua vez, resulta do tipo de dados que

27. Ver, também, Britz (nota de rodapé n. 4), p. 77.

28. A esse respeito, a terminologia de sistemas de informação também se refere à "segurança" no sentido de segurança de T.I. Sobre o assunto, ver *Kubicek*, in: *Klumpp* u.a. (nota de rodapé n. 23). p. 17, 25 s.

29. Sobre a proteção da "exatidão das informações", ver Albers (nota de rodapé n. 2), p. 119 s.; Britz (Nota de rodapé n. 4), p. 52 s.

30. Ver BVerfGE (nota de rodapé n. 17), nota marginal n. 202.

31. Ver BVerfGE (nota de rodapé n. 17), nota marginal n. 194.

32. De maneira mais detida sobre o assunto, *Bäcker*, in: *Brink/Rensen* (Org.), Aktuelle Rechtsprechung des Bundesverfassungsgerichts, 2009, ver, adiante, III, 2a; *Böckenförde*, JZ 2008, 925, 929. Nota de rodapé n. 41.

33. A esse respeito, porém, existe uma proteção suplementar por parte de outros direitos fundamentais, como os artigos 12. e 14. da Lei Fundamental. No entanto, é ainda necessário elaborar um conceito de proteção da propriedade baseado em sistemas de tecnologias da informação.

34. É esse o risco que *Eifert* (NVwZ 2008, 521, 522) teme: que a proteção da integridade fizesse da proteção de direitos fundamentais um direito fundamental a-pessoal e orientado pela técnica. Esse risco não se concretiza se o Tribunal Constitucional Alemão mantém garantido a relação da proteção de integridade como direito fundamental da proteção da personalidade do Art. 2,

é transportado com a ajuda do sistema ou que está ou pode ser armazenado nele. A proteção de dados visada pela proteção do sistema informático estende-se também aos dados pessoais (dotados de relevância para a personalidade) armazenados na memória de trabalho e armazenados temporária ou permanentemente nos suportes de armazenamento do sistema (possivelmente apenas indiretamente).[35]

No entanto, uma vez que o usuário dos complexos sistemas informáticos atuais normalmente não sabe e não pode saber que dados pessoais ou dados relativos à sua personalidade são gerados para além dos dados que introduziu durante o processo de utilização, muito menos onde e durante quanto tempo são mantidos disponíveis (armazenados) nem em que contextos de utilização são utilizados ou por quem, esse usuário praticamente não pode exercer o seu direito de autodeterminação relativo à divulgação e utilização desses dados – direito com o qual ele decidiu anteriormente em que medida podia depositar a sua confiança na confidencialidade de tais dados. A possibilidade de disposição autônoma também não ocorre no caso em que, anda que o tipo de dado for conhecido pelo usuário, ele se encontre sobrecarregado pela autoproteção ou a autoproteção, ou a autoproteção levaria a perdas funcionais irrazoáveis. O ganho em possibilidades técnicas de intercâmbio de informações corresponde a uma perda estrutural de autonomia informacional.[36] No entanto, a proteção funcional do sistema permite – pelo menos de forma limitada – tomar precauções para compensar as consequências dessa perda de autonomia, mas dificilmente restabelece a possibilidade de tomar decisões importantes e autodeterminadas sobre o tratamento dos próprios dados.

O paradigma de garantia da liberdade baseado no direito à autodeterminação informativa[37] através da possibilidade fundamental de decisões autônomas sobre acesso e uso de dados[38] encabeçado pelo *BVerfG* indica, inicialmente, um objetivo de proteção da liberdade, mas também se refere a possíveis formas de alcançar o objetivo através da autodeterminação. O direito da proteção de dados retomou tal objetivo através de instrumentos determinados, tais como a função de consentimento (§ 4, par. 1, § 4a, BDSG) ou o pedido de utilização das possibilidades de anonimização e pseudonimização (§ 3a,

parágrafo 1, em conjunto com o Art. 1, parágrafo 1, da Lei Fundamental, mesmo que ele se estenda ao nível de perigo à personalidade. Esse componente vinculado à personalidade também passa despercebido por *Lepsius*, in: *Roggan* (Org.), *On-line*- Durchsuchungen, 2008. p. 21, 32 s., quando ele descreve a nova dimensão da proteção como "proteção desindividualizada da funcionalidade" desses sistemas e descreve a referência de personalidade exigida pelo tribunal apenas como "contornando o âmbito da proteção, mas não a individualizando" (op. cit., p. 35).

35. *Buermeyer* (HRRS 2007, 154 p.) oferece uma visão ilustrativa sobre os perigos potenciais e as possibilidades de um acesso soberano encoberto a sistemas de computador.

36. De forma instrutiva, ver *Kurz*, in: *Sokol* (Org.) Persönlichkeit im Netz: Sicherheit – Kontrolle – Transparenz, 2007. p. 4 s.

37. ver. BVerfGE 65, 1, 42 f.

38. Já foi ressaltado aqui que tal competência não deve ser (mal)compreendida como sendo quase de direito de propriedade (ver a nota de rodapé n. 5).

BDSG). No entanto, ao referir-se a esses instrumentos, a proteção da personalidade baseia-se em premissas empíricas que sofrem uma erosão crescente devido ao desenvolvimento da tecnologia informática, das constelações de redes e de muitos novos serviços. Para citar apenas um exemplo, isso tem consequências para a relevância do requisito de se obter o consentimento (*Relevanz des Einwilligungserfordernisses*).[39] Aquele que não pode sequer negligenciar aquilo com o que ele concorda – aquele que não pode saber quem, o quê, quando, em que ocasião e sobre quem[40] – não pode "informar"[41] os outros e, portanto, autodeterminadamente autorizá-los a processar dados; sem uma base suficiente de informação, o consentimento é então reduzido a uma formalidade sem legitimação material ou se torna mesmo mera ficção. Uma proteção de dados eficaz só pode ser baseada na possibilidade de proteção da liberdade pelo próprio titular dos dados na medida em que este possa perceber e utilizar eficazmente essas possibilidades. Além disso, são necessários mecanismos de proteção suplementares. Muitos esforços já foram feitos no passado para criá-los, tais como aqueles para a proteção da personalidade através do design de tecnologia e de sistemas.[42] Uma vez que o titular de dados ou a pessoa afetada é apenas numa medida muito limitada o mestre do desenho ou modelo de sistema e de tecnologia, a proteção efetiva da personalidade pressupõe que a pessoa afetada possa, em princípio, invocar o fato de esses mecanismos de proteção, na medida em que existam, serem efetivamente aplicáveis. A proteção dos direitos de personalidade em âmbito dos direitos fundamentais, tomada enquanto proteção da liberdade, exige também – e em decorrência disso – a proteção da confiança, uma proteção que vai além da proteção da confiança na possibilidade de decisões autodeterminadas no que toca à extensão da acessibilidade dos dados. A proteção da confiança na confidencialidade e na integridade do próprio sistema informático, a que o titular dos direitos fundamentais se confia sem que se possa esperar que ele próprio o possa controlar, deve, igualmente, ser assegurada.

IV. Abordagens da proteção dos direitos fundamentais

O direito fundamental da personalidade – complementado também pela proteção proporcionada por outras normas, como a CEDH (por exemplo, o artigo 8.º da CEDH) – permite proteger a comunicação baseada na tecnologia da informação enquanto um exercício de liberdade baseado na confiança.

39. Entre muitos, ver *Holznagel/Sonntag*, in: *Rossnagel* (Org.). Handbuch Datenschutzrecht, 2003. p. 678, com maiores referências.

40. Sobre isso: BVerfGE 65, 1, 43.

41. Sobre o princípio do consentimento esclarecido, ver. § 4 par. 1 N. 1 BDSG, bem como o Art. 2 Lithdsrl.

42. Sobre a proteção do sistema e suas diversas facetas, ver *Albers*, in: *Hoffmann-Riem/Schmidt- Aßmann/Vosskuhle* (Nota de rodapé n. 2), § 22, nota marginal n. 102 s.

1. Defesa e proteção

A proteção dos direitos fundamentais abarca a defesa contra a intervenção estatal (injustificada). No entanto, trata-se também de conceder proteção, seja através do cumprimento das exigências subjetivas de proteção contidas nos direitos fundamentais e, se for caso, das correspondentes obrigações de proteção,[43] seja através da definição dos requisitos dos direitos fundamentais no direito objetivo.[44] As dimensões de proteção que vão além da proteção puramente defensiva dos direitos fundamentais[45] se tornam o centro das garantias fundamentais. Isso ganha tanto mais relevância quanto mais as condições reais para o exercício da liberdade dos cidadãos forem criadas e mantidas pelo Estado, por um lado, mas também pelo setor privado ou no decurso de atos de cooperação entre o Estado e o setor privado, por outro lado – acordos que podem ser, por vezes, questionados[46]. Por isso é importante que o BVerfG tenha se baseado de forma repetida e renovada, desde há algum tempo, na dimensão jurídica objetiva da proteção dos direitos fundamentais.[47] Nas decisões mais recentes da turma (senado) sobre a proteção contra a intervenção em comunicações apoiadas tecnologicamente e contra o acesso às informações nesses meios, no entanto, o foco foi colocado nas intervenções ou autorizações do Estado[48] para intervir, uma vez que só elas foram objeto dos procedimentos correspondentes. No que diz respeito à ativação de outras funções em matéria de direitos fundamentais, ou seja, também as funções dos direitos fundamentais ao abrigo do direito objetivo, o legislador deve tomar regularmente as disposições adequadas – na medida em que não se tornem significativas no decurso da interpretação e aplicação das normas aplicáveis. À sua disposição não existem apenas ordens e proibições, mas sim também outras disposições, tais como regulamentos relativos à organização e aos procedimentos ou à concepção da tecnologia.

---

43. Para deveres de proteção em sentido amplo, ver BVerfGE 39, 1, 42; 46, 160, 164; 56, 54, 73; 115, 118, 152.

44. De maneira pertinente, ver *Stögmüller*, CR 2008, 435 s. S. auch *Hornung,* CR 2008, 299, 305; *Kutscha,* NJW 2008, 1042, 1044; *Sachs/Krings*, JuS 2008, 486.

45. Ver as referências na nota de rodapé n. 43.

46. Para uma abordagem em sentido amplo ver, entre muitos, *Schulze-Fielitz*, in: *Hoffmann-Riem/Schmidt-Aßmann/Vosskuhle*, Grundlagen des Verwaltungsrechts. v. 1, 2006, § 23, especialmente a nota marginal n. 64 s. p. 91 s.

47. Sobre o Art. 5 par. 1 n. 1 GG ver BVerfGE 7, 198, 205 s.; para o Art. 10 GG: BVerfGE 106, 28, 37 para o Art. 2 par. 1 em conjunto com I Arbs. 1 GG: BVerfGE 96, 56, 64; para o Art. 2 par. 1 e 14 par. 1 GG: BVerfGE 84, 192, 194 f; 114, 73, 89 s. Ver também a Argumentação a favor da abertura de uma fonte de informação no âmbito da liberdade de informação (Art. 5 par. 1 GG): BVerfGE 103, 44, 61. Ver, ademais, BVerfGE 49, 89, 140 s. eBVerfG, JZ 2007, 576.

48. A decisão BVerfGE 107, 299, 313 s. estipula que medidas de empresas privadas – aqui se trata de uma medida de uma empresa de comunicação – devem ser imputadas ao Estado, caso tiverem sido ordenados por uma autoridade pública e a empresa em causa não tiver margem de manobra.

2. *Normas pertinentes em matéria de direitos fundamentais*

Diferentes normas estão disponíveis para a proteção dos direitos fundamentais, tais como a proteção do segredo das telecomunicações (Art. 10 GG), a proteção da inviolabilidade do domicílio (Art. 13 GG) bem como, além disso e muitas vezes centralmente, as várias dimensões do direito fundamental à proteção da personalidade do Art. 2 (1) em conjunto com o Art. 1 (1). Artigo 1 (2) da Lei Fundamental,[49] complementado, se necessário, pelos artigos 12, 14 da Lei Fundamental e, subsidiariamente, pela liberdade geral de ação do artigo 2º, n. 1, da Lei Fundamental.

a) O sigilo das telecomunicações

O artigo 10. da GG (Lei Fundamental) protege a transmissão incorpórea de informações através das telecomunicações.[50] O ponto de partida da garantia constitucional é a ideia de evitar os perigos decorrentes do processo técnico de transmissão e o envolvimento de um mediador de comunicação – normalmente condicionado pela distância espacial.[51] Com tal objetivo em mente, o direito fundamental contém, em particular, um direito de defesa contra o conhecimento do Estado sobre o conteúdo detalhado e as circunstâncias das telecomunicações; contudo, inclui também o mandato para que o Estado conceda proteção contra o acesso de terceiros privados ao conteúdo e às circunstâncias das comunicações. Além disso, existe proteção contra que o Estado ponha à disposição de si mesmo os conhecimentos correspondentes relacionados à comunicação produzidos pelos entes privados, por exemplo, autorizando o acesso a dados de tráfego relativos a processos de comunicação específicos (anteriormente: "dados de conexão")[52] à disposição das empresas de telecomunicações ou normalizando uma obrigação estruturada em conformidade de armazenar dados, juntamente com direitos de acesso aos dados armazenados. [53]

b) Proteção ao domicílio

A proteção pode também ser concedida pelo direito fundamental especial previsto no artigo 13.º da Lei Fundamental,[54] que protege a esfera espacial em que a vida privada

49. BVerfG, (Nota de rodapé n. 17), nota marginal 166 s.

50. Ver BVerfGE 67, 157, 172; 106. 28, 35 f.; 115, 166, 182. Para o alcance dessa proteção, ver *Bäcker*, in: *Brink/Rensen* (nota de rodapé n. 32), *infra*, II.

51. De qualquer maneira, a distância espacial não pode, entretanto, ser um elemento fundamental, uma vez que as possibilidades de acesso não tratam dela, mas sim da utilização da telecomunicação – independentemente de quão distante os computadores estejam do ponto de vista físico.

52. Ver BVerfGE 107, 299, 312 s.; 113, 348, 365.

53. Sobre o assunto s. §§ 113a, b TKG e BVerfG, NVwZ 2008, 543.

54. Ver BVerfGE 89, 1, 12; 103, 142, 105 s.

se desenvolve, em especial contra a intrusão, mesmo quando se utilizam ajudas para fornecer informações ou impressões sobre os processos no domicílio.[55] A proteção assim concedida estende-se à coletada de informações possibilitada pela intrusão e à utilização dos dados assim obtidos.

c) Direito fundamental à proteção da personalidade

O direito fundamental à proteção da personalidade nos termos do artigo 2.1 em conexão com o Art. 1.1 da Lei Fundamental,[56] sobre o qual o Tribunal Constitucional Alemão (*BVerfG)* já declarou no acórdão do censo (*Volkszählungsurteil)* que as concretizações até a data ainda não esgotaram a extensão da matéria é, pois, de fundamental importância. Mesmo a adição ao direito à autodeterminação informativa não foi acompanhada da declaração de que, a partir de então, uma concretização final tinha ocorrido.

Já há algum tempo que o direito fundamental à proteção da própria imagem, o direito fundamental à proteção da própria palavra, o direito fundamental à proteção da privacidade em termos espaciais e temáticos, bem como o direito fundamental à autodeterminação informativa são reconhecidos como manifestações parciais desse direito fundamental[57] (ainda que não expressamente contido no texto constitucional). O BVerfG acrescentou, em seu julgamento sobre investigações policiais *on-line*,[58] um direito fundamental de garantir a confidencialidade e integridade de sistemas de tecnologia da informação[59] como expressão parcial de direito fundamental, o que é ocasionalmente referido como um direito fundamental de TI.[60]

A relação entre essas expressões parciais do direito fundamental à proteção da personalidade nem sempre é fácil de clarificar. Assim, o direito fundamental à própria imagem e palavra visa elementos de proteção da personalidade que são também abrangidos pelo direito fundamental à autodeterminação informativa, mas que também podem ser importantes em outras relações de direitos fundamentais (como o artigo 5º da Lei

55. Ver BVerfG (nota de rodapé n. 17), nota marginal n. 193.

56. Ver, também, nota de rodapé n. 4.

57. O termo "direito fundamental" (ver, por exemplo, *BVerfG*, NJW 2008, 1793, 1794) é preferível ao termo anterior "direito", uma vez que enfatiza a base constitucional e permite uma distinção do "direito" civil correspondente. Consequências jurídicas que vão além disso, contudo, não se retiram daí. Ver, nesse sentido, de forma convincente, *Böckenförde*, JZ 2008, 925, 927, nota de rodapé n. 25.

58. *BVerfG* (nota de rodapé n. 17): o acórdão concerne concretamente à investigação *on-line*. Seu alcance no âmbito do direito constitucional, contudo, vai muito além disso.

59. A redução do direito fundamental para um "direito fundamental computacional" – proposta pelos meios de comunicação – induz ao erro. Melhor – mas inadequado como termo jurídico – é o direito fundamental das TI (tecnologias da informação), ver *Bäcker*, in: *Brenk/Rensen* (nota de rodapé n. 32).

60. *Bäcker*, in: *Brenk/Rensen* (nota de rodapé n. 32).

Fundamental). A proteção da privacidade inclui dados pessoais,[61] mas vai muito além da proteção desses dados, por exemplo, quando se destina a proteger comportamentos numa situação protegida como a privacidade, por exemplo, como a proteção contra comportamentos em ambientes específicos. A garantia da confidencialidade e integridade dos próprios sistemas informáticos, agora reconhecidos pelo *BVerfG*, contém também sobreposições com os outros subtipos ou expressões parciais, mas adquire uma importância especial através da concentração objetiva na proteção da utilização de sistemas informáticos para fins pessoais contra os perigos associados. O *BVerfG* não concebeu a proteção da confidencialidade e integridade dos seus próprios sistemas informáticos como um novo direito fundamental,[62] mas como uma manifestação do direito fundamental à proteção da personalidade. Isso, assim como as outras formas de proteção da personalidade mencionadas anteriormente, não é expressamente abordado na parte da Lei Fundamental relativa aos direitos fundamentais, mas está bem fundamentado nela. O direito de proteção baseia-se, por conseguinte, nas mesmas premissas normativas que constituem a base para a concretização das outras dimensões protetoras do direito de personalidade.

V. Em particular: o direito fundamental de garantia a confidencialidade e integridade dos sistemas informáticos utilizados pelo usuário

A nova forma de proteção da personalidade recebeu aprovação geral, especialmente nos meios de comunicação,[63] mas, no que toca à literatura especializada, ela foi recebida parcialmente com críticas, ainda que também com aprovação parcial.[64] A crítica consi-

61. Isso parece falar a favor da expressão cunhada por *Böckenförde* (JZ 2008, 925) sobre uma "esfera privada eletrônica". Por outro lado, há que objetar que o direito fundamental à proteção da privacidade não é definido – espacialmente/tematicamente – com base no meio através do qual a privacidade é concebida.

62. Uma parte da literatura ignora isso, como *Lepsius*, in: *Roggan* (nota de rodapé n. 34), S. 21 s. A propósito, esse ensaio empreende uma reconstrução da decisão que se desprende de suas afirmações e premissas a tal ponto que a classificação dogmática dos direitos fundamentais por *Lepsius* não consegue convencer nem mesmo rudimentarmente. Por isso, *Böckenförde* (JZ 2008, 925, 928, nota de rodapé n. 38.), com razão, rejeita tal argumentação.

63. Ver, entre muitos, *Prantl*, Süddeutsche Zeitung v. 28. 2. 2008. p. 4.

64. Em particular, a construção e o método de argumentação são atacados em detalhe, mas não a dimensão de proteção desejada. Como parte da literatura bastante crítica a esse respeito, ver, por exemplo, Britz, DÖV 2008, 411 s.; *Sachs/Krings*, JuS 2008, 482 s.; *Eifert*, NVwZ 2008, 521 s.; *Lepsius*, in: *Roggan* (nota de rodapé n. 62), S. 21 s.; *Bull*, in: Jahrbuch Öffentliche Sicherheit 2008/2009, S. 317 s.; *Hoeren*, MMR 2008, 365 s. Ver também as referências nas notas de rodapé n. 16 e 25, bem como as contribuições em Roggan (nota de rodapé n. 34). Para um texto que, ao contrário, concorda em muitos detalhes e de forma geral, ver *Hornung*, CR 2008, 299 s.; *Hirsch*, NJW 2008 com referência a NJOZ 2008, 2902; *Lorenz*, StRR 2008, 140 s.; *Stögmüller*, CR 2008, 435 s.; *Jäger*, Juris-itr 12/2008;

dera[65] a nova concretização supérflua, em especial porque a proteção pretendida já seria concedida pelo direito fundamental à autodeterminação informativa. Além disso, a crítica vê o risco de uma minimização da proteção à autodeterminação informativa.[66] Critica-se, ademais, a falta de estruturação dogmática da diferenciação ou distinção do direito à autodeterminação informativa, bem como os riscos que daí podem decorrer.[67] Teme-se, portanto, o risco de um "direito fundamental apessoal orientado pela técnica".[68] Em seguida, procurar-se-á reconstruir premissas importantes para a nova expressão do direito fundamental e, em particular, demonstrar que a necessidade de proteção vai além daquilo que, em todo caso, foi satisfeito com o direito fundamental à autodeterminação informativa de acordo com a jurisprudência anterior.

1. O ponto de partida

Nas anteriores declarações do *BVerfG* sobre a proteção do direito fundamental à autodeterminação informativa, afirmava-se, em particular, que o *BVerfG* concede aos titulares proteção contra a coleta, conservação, utilização e divulgação ilimitadas, individualizadas ou individualizáveis dos dados que lhes digam respeito.[69] Em parte, também foi formulado (de forma abrangente e, portanto, sem mais especificações e sem qualquer força para limitação jurídico-dogmática) que seria necessário levar em conta os perigos e violações da personalidade que resultam para o indivíduo, especialmente sob as

Petri, DUD 2008, 443; *Bä- cker*, in: *Brink/Rensen* (nota de rodapé n. 32); *Böckenförde*, JZ 2008, 925 s.; *Michael/Morlok*, Grundrechte, 2008, nota marginal n. 427 s.

65. Uma crítica especial é dirigida à opinião do tribunal de que o direito à autodeterminação informativa diz respeito apenas a "requisitos de comunicação individual ou dados armazenados" ou dados com "referência seletiva a uma área específica da vida" (a esse respeito, é feita uma referência especial à redação do *BVerfG* [nota de rodapé n. 17], nota marginal n. 201 s.). As declarações do BVerfG são, contudo, mal-entendidas se forem entendidas como observações finais sobre o alcance da proteção do direito fundamental à autodeterminação informativa. Como mostra o contexto das observações, deve ficar claro que a complexidade da necessidade de proteção no que se refere aos sistemas informáticos ainda não foi suficientemente coberta pela jurisprudência e dogmática anterior do direito à autodeterminação informativa. A jurisprudência e, em grande medida, a literatura tratam de precauções contra medidas concretas de coleta e utilização de dados, também estabelecendo instrumentos em um nível anterior – tais como precauções para autoproteção, para proteção por meio de tecnologia e *design* de sistemas. A dimensão da proteção independente da confiança no próprio sistema de tecnologia da informação, que agora é enfatizada pelo BVerfG, não é, com isso, considerada ao longo de todo o processo.

66. *Britz,* DÖV 2008, 411, 413; *Sachs/Krings,* JuS 2008, 481, 484; *Volkmann*, DVBl. 2008, 591; *Eifert*, NVwZ 2008, 521 s.

67. Ver *Kutscha,* NJW 2008, 1043; *Lepsius*, in: *Roggan* (nota de rodapé n. 34); ver também a nota de rodapé n. 62.

68. Sobre o assunto, ver, *supra*, nota de rodapé n. 34.

69. Ver BVerfGE 65, 1, 43; 67, 100, 143; 84, 239, 279; 103, 21, 33; 115, 166, 190; 115, 320, 341 s.

condições do processamento de dados moderno, "de medidas relacionadas à informação".[70] As decisões sobre esse direito fundamental tomadas até a data pelo *BVerfG* dizem respeito aos riscos causados pela coleta de dados, independentemente de serem tomadas de forma seletiva ou contínua, em casos individuais ou em grande escala.

No entanto, as medidas de proteção possíveis ou mesmo exigidas ao abrigo dos direitos fundamentais não se limitam às medidas diretamente relacionadas ao processo de coleta e subsequente armazenamento, utilização, tratamento ou transferência de dados, mas abrangem também os requisitos (organizacionais, processuais, sistémicos etc.) para que esses inquéritos e medidas subsequentes respeitem os direitos fundamentais ou, se necessário, abstenham-se de o fazer. Aqui fica claro que a proteção da autodeterminação informativa já começa no nível da ameaça aos direitos fundamentais e, portanto, pode ser implementada por meio de medidas para reduzir tais ameaças.

Mesmo quando as medidas de proteção – como as medidas de proteção dos dados do sistema[71] – se encontram antes da coleta de dados, trata-se de medidas destinadas a prevenir a deterioração dos dados – em especial sob a forma de controle e concepção do contexto – mas não a proteger a confiança no funcionamento do próprio sistema informático. Em outras palavras: a proteção de dados através da concepção de sistema não é idêntica à proteção do sistema informático (independentemente de nele terem sido implementadas precauções legais de concepção do sistema) contra o acesso ao próprio sistema e de os acessos aos dados serem subsequentemente tornados possíveis.

Se forem formulados requisitos especiais para essa nova dimensão da proteção do sistema, isso não constitui uma "minimização" do direito à autodeterminação informativa, tal qual o argumento que tem sido levantado criticamente por parte da literatura[72]: o seu objetivo de proteção e seu nível de proteção permanecem inalterados. No entanto, o seu âmbito de aplicação não é alargado a outras dimensões de proteção que ainda não tenham sido adequadamente abrangidas pelo direito fundamental à autodeterminação informativa; pelo contrário, essa proteção está ancorada numa nova (na medida em que especial) concretização de direitos fundamentais e é aplicada através de requisitos regularmente mais rigorosos. De qualquer modo, não se constitui de maneira alguma uma redução da proteção dos direitos de personalidade no conjunto dos direitos fundamentais.

2. Novas dimensões das necessidades de proteção

No acórdão sobre as investigações policiais *on-line*, o tribunal partiu da premissa de que a proteção previamente concebida para o direito fundamental à autodeterminação informativa não era suficiente para proteger a confiança na funcionalidade dos próprios sistemas de tecnologia da informação utilizados para a comunicação; confiança, esta, que também é

70. Segundo a formulação em *BVerfG*, NJW 2008, 1505, 1506 (*Kfz-Kennzeichenerfassung*).

71. Ver, *supra*, nota de rodapé n. 42.

72. Ver, *supra*, nota de rodapé n. 65.

importante para a proteção da personalidade. Uma proteção (apenas) antes da coleta e posterior utilização de dados pessoais é insuficiente se não incluir também a proteção contra o acesso ao próprio sistema informático que é utilizado para o desenvolvimento comunicativo. Confia-se na função contínua, correta, não perturbada e regular desse sistema e, portanto, sua infiltração ou mesmo manipulação fazem surgir comprometimentos e perigos para a proteção da personalidade que não podem ser suficientemente defendidos pela proteção dos próprios dados coletados.[73] Assim, a infiltração de um sistema informático complexo com a possibilidade de manipular o seu funcionamento ou a instalação de *software* para modificar os dados pessoais tratados pelo sistema e os processos de comunicação transmitidos criam fontes independentes de perigo, cuja emergência também cria riscos e comprometimentos para os dados disponíveis no sistema informático. A defesa eficaz contra essas ameaças à personalidade exige uma (pré) transferência da proteção no sentido da infraestrutura, que deverá garantir a possibilidade de tratamento autodeterminado com dados, bem como a liberdade e a integridade da comunicação veiculada através da infraestrutura. Infiltrações abrem tais sistemas para controles e manipulações externas. A proteção contra essas infiltrações já existe antes que certos dados possam ser ou sejam acessados,[74] mas continua se tal intervenção chega a ocorrer.

Chama-se, pois, a atenção para distintos níveis de comprometimento e risco. Alguns dos perigos poderiam ser evitados pelo direito fundamental (já desenvolvido até aqui) à autodeterminação informativa, possivelmente após modificações,[75] mas outros não poderiam, ou pelo menos não poderiam de tal forma que as especificidades das situações de perigo fossem suficientemente levadas em conta na utilização dos seus próprios sistemas informáticos.

a) Escopo da intervenção relacionado com a personalidade

O risco de certos dados poderem ser coletados mais facilmente do que anteriormente em resultado de tais infiltrações poderia efetivamente ser combatido em muitos aspectos

73. O fato de os riscos associados à violação da confidencialidade e integridade dos sistemas informáticos serem tidos em conta – tal como assumido, por exemplo, por Eifert, NVwZ 2008, 522 – apenas pela "proteção de dados sempre suficiente ao mesmo tempo" não é algo discernível. A proteção da confiança no modo de desempenho desse sistema informático não pode ser alcançada dessa forma. Nesse sentido, por exemplo, violações de integridade – como a manipulação do *software* com efeitos relacionados à proteção da personalidade – podem tornar a proteção de dados individuais praticamente impossível. Além disso, a proteção que (apenas) assume a forma de proteção dos dados recolhidos deveria basear-se na qualidade desses dados sem poder ser influenciada pela maneira e intensidade da forma pela qual eles são obtidos. É necessário admitir, entretanto, que, para determinar a necessidade de proteção, em especial para determinar a intensidade da intervenção, o BVerfG também se baseou em circunstâncias que não estavam relacionadas com a qualidade dos dados em causa, tais como a dispersão ou a qualidade de informação de massa das intervenções.

74. De maneira acertada: *Petri,* DUD 2008, 446.

75. Ver referências *supra:* nota de rodapé n. 64. Diversos autores consideram esse procedimento suficiente para todos os casos.

pelo direito fundamental existente à autodeterminação informativa – complementado pelos artigos 10.º e 13.º da Lei Fundamental. Se a infiltração permitir o acesso não só a determinados processos de comunicação ou dados individuais, mas também a todos os outros dados "armazenados" no sistema de comunicação ou acessíveis através dele (por exemplo, disponibilizados pelo fornecedor), é possível registar uma multiplicidade e variedade de circunstâncias de vida e características pessoais dificilmente individualizáveis, imprevisíveis, o que só é possível através da infiltração do sistema de tecnologia da informação. O escopo de acesso ao sistema de tecnologia da informação "relacionado com a personalidade" aumenta o potencial de risco das intervenções informáticas subsequentes e reduz a possibilidade de resistência e defesa através de medidas autodeterminadas. Em todo caso, seriam necessários novos esforços jurídicos e dogmáticos se esses riscos fossem levados em conta unicamente através da extensão do âmbito do direito fundamental à autodeterminação informativa.

b) Dados gerados pelo sistema

Em particular, é duvidoso que o direito fundamental à autodeterminação informativa seja suficientemente eficaz na proteção contra o acesso aos dados gerados pelo sistema informático – principalmente quando sem um conhecimento mais profundo da pessoa em causa, muitas vezes até sem qualquer possibilidade de adquirir conhecimentos. O acesso ao sistema informático para efeitos de acesso a esses dados pode ser classificado como uma violação do direito fundamental à autodeterminação informativa e sujeito ao seu programa de justificação. No entanto, surgem problemas, porque a possibilidade de proteção da pessoa em causa – incluindo a possibilidade de uma proteção efetiva *ex post* – é limitada do ponto de vista fático. Por outro lado, não ajuda quando tal proteção, como é parcialmente defendido, refira-se à possibilidade de autoproteção preventiva. Assim, existem determinadas possibilidades para o utilizador impedir tecnicamente a criação de dados individuais gerados no processo de comunicação – tais como *cookies*[76] – ou recolhas de dados – tais como *caches*, [77] mas apenas de maneira limitada: eles exigem sempre uma consciência especial do perigo, bem como um conhecimento técnico considerável, às vezes – como no caso dos flash cookies – é extremamente difícil encontrá-los. [78] As qualificações apropriadas não podem ser assumidas, sem mais, para

76. Esses são dados armazenados em um computador cliente para fornecer determinadas informações a um computador servidor, especialmente durante visitas repetidas.

77. Um *cache* é uma memória de *buffer* rápida que contém cópias do conteúdo de outra memória (de fundo), e assim acelera o acesso a ele. Os dados são armazenados em *cache* para um 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.

78. Os *Flash cookies* – denominados assim em decorrência do *software flash player* com o qual são criados – são muito mais difíceis de exibir e excluir do que os *cookies* "normais". Com as configurações-padrão do sistema operacional Microsoft Windows XP, por exemplo, eles não são

os usuários. Também não corresponde ao modelo constitucional de proteção da liberdade concedê-la apenas a uma pequena minoria de pessoas, a saber, aquela pequena parcela com consciência de perigo e tecnicamente experientes – tais como *freaks*, *hackers* ou mesmo criminosos especializados em tais competências.[79] Além disso, é importante notar que a prevenção de *cookies* ou *caches*, por exemplo, normalmente só pode ser alcançada à custa de perdas funcionais não negligenciáveis: em muitos aspectos, eles também são "úteis" para a pessoa em questão. Em última análise, ele confia que também ele será capaz de usá-los despreocupadamente.

Se o utilizador não quiser impedir tal geração e coleta de dados, é necessária uma proteção eficaz da sua privacidade e personalidade para que ele possa ter a certeza de que os dados obtidos dessa forma não podem ser utilizados em contextos abertos e, em particular, acessíveis a terceiros sem autorização prévia. Através da infiltração de sistemas de tecnologia da informação, no entanto, eles podem ser usados por pessoas que não estão envolvidas no processo de comunicação, sem que a pessoa em questão, o usuário, seja capaz de reconhecer isso e se proteger.

c) Criação de imagens de personalidade de profundidade e amplitude inéditas

Uma situação de perigo especial não facilmente coberta pela proteção tradicional dos direitos fundamentais é criada pelo fato de a infiltração ultrapassar as barreiras técnicas de forma generalizada – ou seja, não apenas em casos individuais – ainda que haja certa vigilância. Quando as barreiras técnicas são ultrapassadas, a barreira de proteção do sistema cai. Essa barreira ou muro protetor precisaria, caso estivesse ativa, ser superada a cada e toda vez em que se tentasse infiltrar e intervir no direito da autodeterminação informativa e outras medidas jurídicas eventualmente cabíveis. Ainda que o infiltrador[80] esteja interessado apenas em dados determinados, do ponto de vista prático, não há absolutamente nada que o impeça de obter outros dados e acessar outros processos de comunicação. Por exemplo, a infiltração torna possível obter um banco de dados potencialmente grande e altamente significativo e diferenciado – ou seja, com multiplicidade

sequer visíveis no disco rígido. Eles não podem nem sequer ser localizados dentro do *browser*, já que são processados e salvos de forma independente ao *browser*. Pela mesma razão, os dados armazenados podem ser atribuídos exclusivamente ao respectivo usuário, mesmo que ele use diferentes navegadores no mesmo sistema – e de forma independente de qualquer número de sessões de navegação.

79. Ver *BVerfG*, JZ 2007, 576: A autoproteção informativa deve ser de fato possível e razoável para o indivíduo.

80. Tal como é o caso das autoridades de segurança que normalmente só estão interessadas na transmissão seletiva orientada de dados específicos relevantes para elas. Um Trojan instalado por eles funciona melhor se ele apenas transferir dados individuais, ou seja, precisamente os dados que são importantes para a tarefa oficial (por exemplo, nomes de parceiros de comunicação, conteúdos armazenados de e-mails etc.). A barreira foi, no entanto, superada de forma geral pela infiltração.

de facetas – de dados de personalidade. Torna-se, pois, possível abrir vislumbres sobre partes essenciais da vida, bem como perfis diferenciados de interesses, comportamento, comunicação e perfis sociais e, portanto, imagens de personalidade altamente significativas, ou seja, que têm muito a dizer sobre a pessoa em questão[81].

Não obstante, o direito fundamental à autodeterminação informativa já protege contra a construção de imagens da personalidade através da exploração de agregação de dados individuais.[82] Se, no entanto, a infiltração dos sistemas de tecnologia da informação elimina a barreira técnica de impedimento do acesso à totalidade da informação, a coleta de todos os dados acessíveis no sistema informático durante períodos de tempo mais longos pode criar possibilidades para a acumulação e combinação de uma grande quantidade de informação de diferentes áreas da vida numa profundidade e amplitude tamanha que eram impossíveis de serem alcançadas com as intervenções anteriormente.[83]

Ainda que o direito fundamental à autodeterminação informativa na sua proteção contra a formação de imagens de personalidade possa ser suficientemente ativado contra a coleta de dados concretos, a infiltração de sistemas de tecnologia da informação deixaria aberto, em todo caso, o risco de que imagens da personalidade de uma amplitude e densidade até então desconhecidas sejam criadas e que a pessoa afetada não seja sequer capaz de avaliar o perigo potencial e, frequentemente, não seja nem capaz de se defender eficazmente: a lacuna de proteção relativa ao sistema informático não pôde ser fechada eficazmente ao nível da proteção contra a coleta de dados concretos. Através da infiltração do sistema de informático coloca-se um "pé virtual na porta", mantendo-a aberta para livre acesso à personalidade vulnerável.

d) O risco de falsificação de dados

A possibilidade de infiltração no sistema implica também o risco de falsificação (praticamente indetectável de forma virtual) de dados individuais registados e da sua combinação com outros, o que pode levar a um perfil de personalidade falsificado. O usuário já praticamente não pode mais se defender contra tais falsificações, uma vez que já ocorreu uma infiltração associada a tais possibilidades – uma infiltração que, em princípio, também pode ser utilizada por terceiros.[84] Não se trata, de modo algum nesse caso, apenas de uma intensificação da intervenção contra a qual o direito fundamental à

81. Tal como na formulação plástica de *Böckenförde*, JZ 2008, 925, 928: "É a função de mediação do sistema informático que agrega os dados pessoais individuais num todo dinâmico que pode ser acedido repetidas vezes e, por isso, em caso de acesso não autorizado, pode expor o estilo de vida pessoal da pessoa em questão".

82. Ver BVerfGE 65, 1, 42 f.; 109, 279, 323; 112, 304, 319.

83. *Michael/Morlok* (nota de rodapé n. 64, nota marginal n. 429) falam em um "salto qualitativo".

84. Só por uma questão de exaustividade é que as autoridades de segurança que procedem à infiltração não devem estar regularmente interessadas em tais falsificações.

autodeterminação informativa, no seu conteúdo anterior, protege,[85] mas se trata, sim, de uma qualidade de perigo independente.[86] As medidas de garantia que se tem disponíveis devem basear-se na proteção do próprio sistema informático, ainda que, no interesse da sua eficácia, essa proteção deva ser estendida aos dados coletados em decorrência de infiltrações.

e) Enfraquecimento das possibilidades de autoproteção

A infiltração realizada pelo governo e suas agências e – caso seja necessário para a espionagem – a manipulação de sistema informático, em particular, termina por conduzir ao enfraquecimento (não apenas em casos individuais) da autoproteção levada a cabo pelos usuários e que se lhes é recomendada como expressão da ideia de autodeterminação informativa – por exemplo, encriptando ou utilizando senhas. O direito fundamental à autodeterminação informativa é enfraquecido em suas premissas básicas. A possibilidade de autoproteção tem sido até agora considerada um elemento essencial da participação na comunicação autodeterminada, uma comunicação que é igualmente tida em conta nas disposições da legislação atual em matéria de proteção de dados. O Segundo Senado (segunda turma) do Tribunal Constitucional Federal alemão, por exemplo, tomou a possibilidade de autodeterminação dos dados disponíveis como oportunidade para defender a tese de que a proteção prevista no artigo 10 da Lei Fundamental não se aplicaria mais para os dados que se enquadram no âmbito do controle do titular dos mesmos, uma vez que, com domínio, os titulares teriam uma possibilidade.[87] Tal referência do Segundo Senado à possibilidade de autoproteção é, contudo, questionável e passível de críticas e, portanto, duvida-se se ela seria algo realmente viável. Com efeito, viável é aquela consideração de que, após a conclusão do processo de comunicação, os dados salvos não diferem mais daqueles contidos nos dados criados pelo próprio usuário. Se, após a conclusão de um processo de comunicação, ocorrer acesso aos dados de comunicação armazenados no âmbito de domínio do destinatário, mais do que a atualização de um risco específico da comunicação, ocorre antes um risco geral de tecnologia da informação[88].

O elevado grau da possibilidade de autoproteção que caracteriza o direito fundamental à autodeterminação informativa não é, de forma alguma, desvalorizado pelo fato de muitos cidadãos tratarem os seus dados de forma descuidada ou ignorarem as

85. Tal como, por exemplo, *Eifert*, NVwZ 2008, 521: "intervenção especialmente grave" no âmbito de proteção do direito fundamental à autodeterminação informativa.

86. Caso se tratasse apenas do problema de "intervenções aditivas em direitos fundamentais", seria possível superar a questão, entretanto, no nível da justificação. Ver, nesse sentido: BVerfGE 112, 304, 319 s. Não obstante, não se trata aqui de adição.

87. BVerfGE 115, 166, 185 s.

88. Cf. formulação em *Bäcker*, in: *Brink/Rensen* (nota de rodapé n. 32), *infra* II 2 c.

possibilidades de autoproteção. A necessidade de proteção ao abrigo dos direitos fundamentais não deixa de existir porque os cidadãos individuais não a sentem ou são incapazes de realizá-la; a autodeterminação inclui a capacidade de decidir até que ponto alguém quer proteger a si próprio. Aqueles que querem dispensar tal proteção assim o fazem também por meio de uso de um direito de liberdade. No entanto, se já não for possível avaliar a necessidade de proteção ou se a possibilidade de proteção não existir de forma alguma, a sua vontade de proteção autodeterminada deixa de ter importância e a recusa de proteção não pode, em circunstância alguma, ser justificada por referência à negligência de muitos cidadãos no tratamento dos seus dados (concretos). No entanto, a possibilidade de proteção é negada aos cidadãos pela infiltração de sistemas de tecnologia da informação. Isso é aplicável mesmo que não seja feito secretamente – desde que a pessoa afetada não possa avaliar as consequências da infiltração e da manipulação associada a ela ou for praticamente incapaz de se defender ou resistir.

f) Permissão do acesso de terceiros

Em especial, existe uma necessidade (já repetidamente indicada aqui) de proteção contra o risco de terceiros (privados) tirarem partido da infiltração do sistema informático pelas autoridades estatais e, por exemplo, utilizarem o *software* infiltrado para espiar o sistema ou manipulá-lo, ou seja, redirecionarem a infiltração para os seus próprios fins, como uma espécie de "ovo de cuco" lançado pelo governo, sem que a pessoa em causa suspeite disso nem seja capaz de se proteger eficazmente. A proteção dos direitos fundamentais contra a intervenção do Estado – nesse caso, a infiltração – é constitucionalmente mais abrangente, mais fácil e leve e, sobretudo, mais eficaz do que a proteção contra os particulares no âmbito dos efeitos horizontais dos direitos fundamentais. No caso de uso estatal de *software* – ou *software* ou *hardware* manipulados – que tenha sido infiltrado pelo Estado, há pelo menos a perspectiva de que o Estado observe as restrições do Estado de Direito à sua autoridade para intervir; no caso de acesso (ilegal) de terceiros possibilitado pela "execução antecipada" estatal. Essa perspectiva de proteção não se aplica, pois terceiros não se sujeitam a tais obrigações do Estado de Direito e, dada a ilegalidade de sua conduta, dificilmente poderiam ser efetivamente submetidos.

g) Grande dispersão das pessoas afetadas

A infiltração e o monitoramento possibilitado por ela – que pode durar muito tempo, além de compreender os mais diversos atos de comunicação e ligá-los uns aos outros de modo dinâmico – não se restringem aos destinatários primários para os quais a infiltração foi concebida. Mais que isso, ela se espraia para um dantes imprevisível ciclo de terceiros que são parceiros de comunicação do afetado. Isso também é assim em outras interferências na comunicação – tal qual em escutas telefônicas realizadas pela polícia. No entanto, enquanto sejam armazenados ou gerados dados que se referem a terceiros no sistema

de tecnologia da informação, a gama possível de dados pessoais pode exceder qualitativamente e em muito a que está associada à intervenção direcionada em arquivos de comunicação específicos, como a escuta de determinadas conversas. Consequentemente, terceiros podem ser afetados não apenas na medida em que isso seja "inevitável em casos individuais", mas também afetados potencialmente de forma geral e – presumivelmente frequentemente – sem qualquer limitação prévia e – naturalmente – sem serem capazes de se defenderem de forma "autodeterminada".

3. Esclarecimento sobre a natureza especial da situação de perigo e a correspondente proteção dos direitos fundamentais pelo BVerfG

a) Diferenciação ao nível do âmbito de proteção

Com efeito, poderia ser feita uma tentativa de conceder alguns dos interesses anteriormente mencionados, alargando ainda mais o direito fundamental à autodeterminação informativa. No entanto, tal construção teria de ser, então, transformada num baluarte plenamente utilizável contra a facilitação e implementação do acesso oficial não só a dados e processos de comunicação de todos os tipos, mas também às infraestruturas de comunicação utilizadas (*software* e *hardware*), além de contra o acesso correspondente por parte de entidades privadas. No interesse da capacidade de gestão jurídico-dogmática seria então necessária uma maior diferenciação do âmbito alargado da proteção através de uma afinada dogmática de limites e barreiras, que trabalhe elaborando barreiras especiais (particularmente elevadas) à infiltração e manipulação de sistemas informáticos que põem em perigo a proteção da personalidade e a coleta e utilização de dados tornadas possíveis por essa via. Em contraste, parecia constitucionalmente preferível ao *BVerfG* diferenciar ainda mais o direito fundamental geral à proteção da personalidade e encarar a proteção da integridade e da confidencialidade dos sistemas de tecnologia da informação utilizados pelo indivíduo e antes da coleta e exploração dos dados obtidos como resultado da infiltração, numa forma "especial", do direito fundamental geral relacionado ao sistema de tecnologia da informação – direito que não depende de ficções de proteção autodeterminada da personalidade, mas põe em primeiro plano a necessidade da proteção de expectativas de confiança. Isso torna mais fácil considerar a nova qualidade do perigo e da necessidade de proteção orientada para a confiança no sistema já ao nível do âmbito de proteção e reconhecer a necessidade de requisitos especiais para as barreiras, além de desenvolver medidas de proteção orientadas para perigos e risco relacionados.

A abordagem do tribunal também pode ser interpretada como uma reação ao fato de as dimensões da ameaça à confiança nas infraestruturas de comunicação e as necessidades de proteção correspondentes só terem sido abordadas até agora de forma limitada, se é que o foram de todo, na literatura jurídica, e de não existirem conceitos, pelo menos não mais detalhados ou mesmo reconhecidos na jurisprudência e literatura, sobre

a forma como a proteção da confidencialidade e integridade dos sistemas de tecnologia da informação utilizados pelo indivíduo pode ser integrada no direito fundamental à autodeterminação informativa sem inconsistências e lacunas. Em razão da falta de trabalho preparatório na literatura, é surpreendente que a maioria dos autores que analisam a nova decisão reivindique, sem mais diferenciação, que a proteção poderia ter sido alcançada apenas pelo direito fundamental à autodeterminação informativa. Isso é ainda mais surpreendente quando se nota que, antes da decisão, foi feita uma tentativa na literatura e nas peças processuais endereçadas ao tribunal para satisfazer a necessidade de proteção em particular através do Artigo 13º da Lei Fundamental[89] – ou também do Artigo 10º da Lei Fundamental.

b) Reação à qualidade específica do perigo

Em contraste, a denominação e ênfase explícita da proteção, de cunho de direito fundamental, à confidencialidade e à integridade dos próprios sistemas de tecnologia da informação, tal como defendida pelo *BVerfG*, deixa claro que existe uma situação de risco qualitativo particular e que, por conseguinte, devem existir medidas de proteção coordenadas de forma correspondente. Uma das diversas vantagens de especificar o âmbito da proteção é que isso permite que o critério da proporcionalidade em sentido lato seja conduzido de forma mais precisa. O potencial de perigo especial é compreendido, portanto, de forma tipificadora, realçando, então, o caráter especial do direito fundamental e estabelecendo-se a exigência de uma forma tipificada de proteção. Consequentemente, a proteção não depende exclusivamente de considerações *ad hoc* no contexto dos critérios de proporcionalidade. No entanto, as ponderações de caso a caso continuam sendo necessárias para o aperfeiçoamento em casos individuais.

c) Delimitações do direito à autodeterminação informativa

Um problema, porém, apresenta-se na distinção entre o direito à autodeterminação informativa e a proteção da integridade e da confidencialidade dos próprios sistemas informáticos – esta última tendo sido tratada neste artigo. De forma geral, e em princípio, a distinção funciona da seguinte forma: quando se trata da proteção contra a coleta de dados (e o processamento posterior de dados)[90] sem infiltração nos sistemas de tecnologia da informação e de proteção contra a criação de autorizações correspondentes, então, estamos diante de um caso em que o direito fundamental da autodeterminação

89. Ver evidências e argumentação em *Böckenförde*, JZ 2008, 925, 926, nota de rodapé n. 10.

90. A exploração por terceiros, ou seja, após a transmissão de dados, só é permitida de acordo com princípios gerais se as condições que justificam tal intervenção também estiverem preenchidas para esses terceiros.

informativa continua a exercer sua proteção.[91-92] Contudo, em contraste, quando se trata de caso em que um sistema informático complexo tenha sido infiltrado, espiado e, se for o caso, manipulado para coleta de dados, aplica-se, então, a nova dimensão de proteção de cunho de direito fundamental.[93] Essa proteção de cunho de direito fundamental da confidencialidade e da integridade do sistema informático não se aplica apenas à infiltração (e, se aplicável, à manipulação) enquanto tais, mas estende-se também à coleta e utilização de dados e informações obtidos (apenas) em resultado da infiltração:[94] com efeito, no âmbito da proteção à personalidade, os obstáculos que se prostram passam a ser maiores e se estendem ao tratamento dos dados pessoais que se tornaram acessíveis por meio da infiltração.

d) Necessidade de maior concretização

Os contornos da nova concretização dos direitos fundamentais não puderam ser definidos em todos seus aspectos pelo *BVerfG*, já que ele teve de tratar de um litígio específico e, consequentemente, teve de o fazer apenas na medida em que a questão em tela se referia ao objeto desse litígio específico, e não a partir de um ponto de vista geral. Subsequentemente, existe ainda uma necessidade considerável de concretização, também no que diz respeito ao objeto da proteção, em especial no que toca ao conceito (relacionado

91. É equivocado interpretar a frase introdutória do BVerfG (nota de rodapé n. 2), notas marginais n. 166 e 201, como significando que a nova dimensão da proteção é "subsidiária" ao direito à autodeterminação informativa. Não obstante, essa é a posição de *Petri*, DUD 2008, 444, por exemplo. O BVerfG diz, na verdade, que a nova forma de direito fundamental se aplica ali onde uma lacuna de proteção pode ser diagnosticada.

92. Além disso, no que respeita a qualquer concorrência remanescente, aplica-se o princípio geral segundo o qual os limites ao direito fundamental podem ser deduzidos da expressão do direito de personalidade que protege contra o perigo maior e, por conseguinte, impõe requisitos mais rigorosos. Em abordagem geral sobre tais regras de concorrência, ver *Jarass/Pieroth,* GG, 9. Aufl. 2007, nota marginal n. 18, Vorbemerkung vor Art. 1 – com mais referências.

93. Se a autorização legal permitir que outros organismos utilizem a infiltração ou os dados obtidos através dela, terão também de cumprir com os elevados requisitos de interferência em seu próprio sistema informático.

94. Essa extensão da proteção ao que foi "obtido" através da violação dos direitos fundamentais não é nada de anormal. Nesse sentido, o Art. 13 da Lei Fundamental protege não apenas contra a invasão de domicílio, mas também as informações ou objetos obtidos em decorrência de tal invasão.

So schützt Art. 13 GG nicht nur vor dem Eindringen in die Wohnung, sondern auch die durch das Eindringen erlangten Informationen oder Gegenstände. Ver BVerfGE 109, 279, 374; com referência a BVerfGE 100, 313, 360 (o último com referência ao art. 10 GG). Sobre os paralelos entre as novas garantias dos direitos fundamentais e o art. 13 GG, ver: *Bäcker*, in: *Brink/Rensen* (nota de rodapé n. 32), *infra* III 1 vor a; *Pieroth/Schlink*, Grundrechte, 24. Aufl. 2008, nota marginal n. 377c.

com a personalidade) de "sistemas informáticos"[95] próprios (melhor: autoutilizados).[96] Também ainda não foi esclarecido de forma conclusiva como deve ser garantida a proteção dos sistemas informáticos contra interferências não secretas – uma proteção que foi expressamente mencionada pelo tribunal, mas não foi elaborada em detalhes.[97] Ademais, é igualmente necessário clarificar o alcance da proteção contra particulares. No entanto, a formulação do Tribunal Constitucional Alemão da dimensão dessa proteção de cunho de direito fundamental como uma "garantia" deixa claro que o Estado também é responsável por assegurar que a integridade e a confidencialidade dos sistemas informáticos – incluídos aí os casos em que elas sejam ameaçadas por outros meios que não a intervenção do Estado. O Estado dispõe, entretanto, de uma ampla margem de apreciação de ação para o desempenho das tarefas regulamentares correspondentes ao abrigo do direito objetivo.

Tal garantia de natureza de direito fundamental também protege contra interferências com fins repressivos. No entanto, as condições pelas quais isso pode ser possível e aplicável ainda carece de maior clarificação.[98] Aqui, o peso dos bens jurídicos – cuja proteção serve efetivamente à norma penal possivelmente violada no caso concreto – deverá ser determinado de forma semelhante à das medidas preventivas. Poder-se-ia afirmar, contudo, que também houve necessidade de uma maior concretização na formulação do direito fundamental à autodeterminação informativa há um quarto de século. Também naquele momento a nova perspectiva pôs um desafio à dogmática jurídica, à legislação e à jurisprudência de então. Hoje, isso acontece novamente.

VI. Limites de direitos fundamentais

O direito fundamental à garantia de integridade e confidencialidade de sistemas informáticos de uso próprio não existe de forma irrestrita. Tendo em vista o potencial de risco específico, o princípio de proporcionalidade conduz, em regra (embora isso dependa da intensidade da intervenção),[99] a um elevado obstáculo para as intervenções.

95. Ver as considerações *supra,* III.

96. Essa alternativa linguística evita ressonâncias inadequadas apenas no âmbito dos direitos reais. Ver também *Bäcker*, in: *Brink/Rensen* (nota de rodapé n. 32), *infra* III 2a. O uso de um computador em um cybercafé também configura um uso pessoal (ainda que seja apenas temporário).

97. Ver, de forma mais detalhada, *Böckenförde*, JZ 2008, 931; *Bäcker*, in: *Brink/Rensen* (nota de rodapé n. 32), infra III.

98. Ver, também, as considerações de *Kühne*, in: Roggan (nota de rodapé n. 34). p. 85 s.

99. O BVerfG não precisou decidir até que medida intervenções de menor alcance do que as buscas *on-line* poderiam ser permitidas sob condições menos rigorosas. Sobre o assunto: *Bäcker*, in: *Brink/Rensen* (nota de rodapé n. 32), *infra* III 3.

Ademais, o dever de proteção do Estado, ancorado objetiva e juridicamente, de tomar medidas contra ameaças de particulares, também é ativado aqui.[100]

1. Requisitos de direito material e direito processual

O *BVerfG* formulou requisitos para as autorizações legais no âmbito da prevenção de riscos que dizem respeito à infiltração e manipulação do sistema informático próprio, mas também à coleta e utilização de dados e informações obtidos dessa forma.

Os requisitos constitucionais para as restrições incluem, em primeiro lugar, o requisito de certeza e clareza das normas de autorização – algo que, aliás, foi desde sempre derivado do princípio fundamental do Estado de direito.[101]

Além disso, para que se justifique uma investigação *on-line* é necessário indicar um bem jurídico suficiente (excepcionalmente) importante,[102] tais como o corpo, a vida e a liberdade de pessoas, bem como aqueles bens de interesse geral cuja ameaça afete as fundações ou a existência do Estado ou das fundações da existência humana.[103] Um exemplo deste último seriam ataques a serviços públicos que asseguram a existência de estruturas de fornecimento, abastecimento ou segurança pública, como barragens. Os requisitos constitucionais incluem também requisitos relativos ao tipo e à intensidade do perigo e, consequentemente, ao grau de probabilidade e à base factual do prognóstico do perigo.[104] Em particular, a exigência de uma probabilidade suficiente de ocorrência não pode ser dispensada e as hipóteses e conclusões devem ter um ponto de partida concretamente definido no mundo real e suporte fático. Os fatos devem, por um lado, permitir concluir que pelo menos a natureza do acontecimento é concreta e previsível e, por outro, que se trata de pessoas envolvidas determinadas cuja identidade é conhecida, pelo menos de tal forma que a medida de vigilância pode ser dirigida contra elas e amplamente restringida a elas.[105]

Além disso, as garantias processuais são também de suma importância,[106] em especial um controle pormenorizado a ser realizado por uma autoridade independente antes da infiltração. O acesso secreto aos sistemas de tecnologia da informação, que deve ser

100. Ver as referências na nota de rodapé n. 44 e 45. Por meio do conceito de "garantia" da confidencialidade e a integridade dos sistemas de tecnologia da informação, a Corte esclarece a existência de um dever para que o Estado proteja em todas as esferas da vida (ver também *Petri*, DUD 2008, p. 446 s.), sem, contudo, aprofundá-lo em detalhes.

101. Ver BVerfG (nota de rodapé n. 17), nota marginal n. 208, com mais referências.

102. Requisitos mais baixos podem, por exemplo, ser suficientes para a avaliação *off-line* do disco rígido de um computador confiscado.

103. *BVerfG* (nota de rodapé n. 17), nota marginal n. 247.

104. *BVerfG* (nota de rodapé n. 17), nota marginal n. 242 s., 249 s.

105. *BVerfG* (nota de rodapé n. 17), nota marginal n. 251.

106. *BVerfG* (nota de rodapé n. 17), nota marginal n. 257 s.

considerado particularmente importante, deve ser colocado sob reserva de uma decisão judicial, ou seja, só pode ser autorizado após sentença. Outro órgão, exceto em casos urgentes, só pode ser considerado se oferecer a mesma garantia de independência e neutralidade de que dispõe um juiz – uma segurança significativa que é muito difícil de se garantir. As razões da licitude das medidas de controle e monitoramento devem ser apresentadas por escrito.

2. O núcleo central da vida privada e suas formas de vida

Finalmente, são indispensáveis precauções para proteger o núcleo central da vida privada. Os sistemas informáticos utilizados exclusivamente para comunicações relevantes para esse núcleo central não devem ser infiltrados. Isso, todavia, não é algo previsível de antemão. A esse respeito, a proteção só pode tornar-se totalmente eficaz quando os dados são coletados como resultado da infiltração no sistema de tecnologia da informação. A coleta de dados relevantes para esse núcleo central da vida privada deve, em princípio, ser proibida.

A proteção só pode ser empurrada para a segunda fase – ou seja, para a avaliação –, quando e se a relevância dos dados recolhidos para o núcleo central não puder ser clarificada antes ou durante a coleta de dados, mas existirem, no entanto, indicações de que um objeto de proteção de importância excepcional corre risco presumível de ser colocado em perigo. No entanto, regras processuais adequadas devem garantir que a intensidade da violação do núcleo central e os seus efeitos sobre a personalidade e o desenvolvimento da pessoa em causa permaneçam tão baixos quanto possível.[107]

No entanto, a proteção por não coleta continua a ser a prioridade. Assim, o tribunal formula o requisito de se abster da recolha de dados se houver indicações de que o núcleo central é "afetado". O núcleo central da vida pessoal está protegido como tal. Não se trata (apenas) da proteção de uma determinada declaração que deve ser julgada isoladamente e que, devido ao seu conteúdo, não deve ser acessível ao Estado por razões de proteção da dignidade humana. Em vez disso, a proteção do núcleo central visa a proteção da parte do desenvolvimento pessoal privado que deve ser mantida livre do conhecimento do Estado em prol da dignidade humana. No entanto, no núcleo central da vida privada também se misturam as coisas íntimas e banais, significativas em termos de personalidade com aquelas menos significativas. Essa mistura comunicativa também é protegida, mesmo antes de a comunicação ser inquirida, e não apenas ao nível da avaliação. Nesse caso, a proteção só pode ser concedida dividindo o processo de comunicação em – visto isoladamente – conteúdo absolutamente protegido e apenas relativamente protegido.

Se a proteção fosse requerida apenas dessa forma, não seria, em princípio, negado ao Estado o direito de se infiltrar no sistema informático e de registar primeiro todos os conteúdos, a fim de, em seguida, remover elementos individuais como absolutamente

107. *BVerfG* (nota de rodapé n. 17), nota marginal n. 281 s.

protegidos. Isso não faria justiça à ideia básica de proteção do núcleo central: A dignidade humana exige que o Estado se abstenha de exercer vigilância numa situação em que existem indícios de que a medida afetará esse bem mais importante. Tal "toque" está geralmente presente no momento da tomada de conhecimento. Uma renúncia à proteção já no nível de levantamento deve, portanto, permanecer uma exceção,[108] para a qual existem motivos, por exemplo, se o núcleo central for inesperadamente afetado[109] ou se houver indicações de que a comunicação serve para acordar ou planejar atos puníveis concretos,[110] ou porque *in-time* ou outro conteúdo com necessidade de proteção serve apenas como uma camuflagem para acordar ou discutir em mais detalhes ações que constituem um perigo.[111] Só se não for suficientemente previsível qual será o conteúdo dos dados coletados, ou se as tecnologias da informação ou as dificuldades de investigação entravarem a análise do conteúdo dos dados – por exemplo, no caso de documentos ou conversas em língua estrangeira – é que, com a maior cautela possível e se respeitando o bem jurídico cuja proteção é de extrema importância, pode ser efetuada uma primeira análise, mesmo após infiltração no sistema informático e a proteção constitucional ser transferida para o nível de avaliação (*conceito de proteção em dois níveis*).

O requisito de proteção núcleo central já e descumprido quando o levantamento de dados (apenas) deixa de ocorrer se tais constatações relevantes para núcleo central forem afetadas, tal como previsto no § 100 a (4) StPO (Código Processual Penal Alemão) e outras normas. O fato de que, na vida prática, conteúdos relevantes para o núcleo central sejam comunicados "sozinhos" – ou seja, apenas com conteúdo relevante para o núcleo central sem mais – será, provavelmente, extremamente raro; isso é ainda mais improvável de ocorrer de forma que se possa prever de antemão uma eventual separação de tipos de conteúdo. Ao limitar a proteção a esse tipo de utilização, a proteção de duas fases da área do núcleo seria anulada. Mesmo em uma conversa confidencial entre cônjuges, na qual conteúdos relacionados ao núcleo central são objeto de discussão, haverá também outros conteúdos, como conteúdo banal ou declarações sobre a conduta de terceiros ou eventos de natureza diferente: simplesmente permitir o monitoramento e a gravação, negando assim a proteção do núcleo central já no nível de investigação e transferindo-a para o nível de aplicação, não cumpre os requisitos constitucionais.[112]

---

108. *BVerfG* (nota de rodapé n. 17), nota marginal n. 281.

109. Ver BVerfGE 109, 297, 318.

110. Ver BVerfGE 113, 348, 391.

111. *BVerfG* (nota de rodapé n. 17), nota marginal n. 281.

112. Já na decisão BVerfGE 113, 348, 391 s. postula-se – embora com referência ao Art. 10º, par. 1 da GG, que, em princípio, concede uma proteção mais fraca do que o direito fundamental recentemente concretizado – : "Se, no caso concreto, existirem indícios concretos de que uma interceptação de telecomunicações captura conteúdos pertencentes a esta área fundamental, tal interceptação não pode ser justificada e não deve ocorrer". Utilizou-se, aqui, a palavra "capturar" (*erfassen*), mas não para significar que a comunicação "sozinha" contém conteúdo sobre a área

VII. Concorrência com outras normas de direito fundamental

O direito fundamental de proteger a confidencialidade e a integridade dos sistemas de tecnologia da informação pode competir com outras normas de direitos fundamentais, como os artigos 10º e 13º da Lei Fundamental.

1. Intervenção no âmbito do domicílio

O âmbito da proteção do artigo 13.º da GG é afetado quando uma intervenção é feita no domicílio (ver, anteriormente, IV 2 b). Existem, pois, obstáculos especiais, como aqueles do parágrafo 4º. É, contudo, duvidoso que o artigo 13.º da GG possa garantir a proteção de forma abrangente e, de fato, de forma adequada e suficientemente diferenciada, em especial se a proteção espacial do artigo 13.º da GG abrange o problema específico da infiltração e da modificação dos sistemas das tecnologias da informação: o artigo 13.º GG concede proteção espacial e proteção espacial de conduta, mas não proteção de funções relacionadas com a infraestrutura de comunicações pessoais. Além disso, a proteção prevista no artigo 13 da Lei Fundamental só seria considerada se o *hardware* infiltrado estivesse localizado em um apartamento, situação que nem sempre é o caso de *notebooks*, *smartphones* e outros.

Deve-se acrescentar, no entanto, que o artigo 13.º da Lei Fundamental salvaguarda aspectos importantes da proteção, como a proteção contra a medição das emissões eletromagnéticas para gravar palavras codificadas, contra a intrusão em domicílio, por exemplo, para fins de manipulação do dispositivo, ou contra a ativação de câmaras e microfones em computadores para monitorização de atividades que ocorrem em domicílio.[113] Tais medidas constituem igualmente uma intervenção independente no âmbito da proteção do artigo 13º, par. 1 da Lei Fundamental, que exige uma justificação se servirem para a pesquisa prática da infiltração em sistemas informáticos, como uma "investigação *on-line*". O domínio da proteção dos direitos fundamentais da confidencialidade e da integridade dos sistemas informáticos não deve ser mal interpretado de forma a substituir as garantias paralelas dos direitos fundamentais, de modo que as medidas possam, por assim dizer, ser autorizadas como um anexo, na medida em que se destinem a servir a implementação de uma interferência num sistema informático e isso é permitido enquanto tal – em comparação com o padrão da garantia de proteção da personalidade aqui discutido. Por um lado, tal "solução de anexo" não faria justiça à categoria do direito fundamental da inviolabilidade do domicílio, que é particularmente protegida pela Constituição. Por outro lado, também não consegue convencer sistematicamente, uma

fundamental da vida privada. Essa afirmação não foi corrigida pelo acórdão sobre as pesquisas e buscas *on-line*.

113. Ver – ainda que não compreendendo todos os exemplos mencionados anteriormente – *BVerfG* (nota de rodapé n. 17), nota marginal n. 193.

vez que as infiltrações nos sistemas de tecnologia da informação são, em princípio, tecnicamente possíveis sem violar o domicílio[114].

2. *Concorrência com o sigilo das telecomunicações, em especial com a vigilância de telecomunicações nas fontes* (Quellen-TKÜ)

Existe uma situação de concorrência entre o artigo 10.º da GG e o direito fundamental de proteger a confidencialidade e a integridade dos sistemas informáticos, em especial no que respeita à vigilância das telecomunicações na fonte (Quellen-TKÜ). A vigilância de telecomunicações na fonte (Quellen-TKÜ) é um processo de monitoramento que detecta a saída de telecomunicações antes da criptografia ou a entrada de telecomunicações após a descriptografia pelo destinatário. Enquanto a vigilância das telecomunicações costumava ter lugar e ter êxito durante o período de transmissão na rede – ou seja, nas vias físicas de transmissão –, isso já não é possível com a transmissão digitalizada e a utilização da cifragem. Ademais, existe ainda alguma incerteza quanto à segurança das tecnologias individuais de Voice-over-IP contra as escutas[115].

A vigilância de telecomunicações na fonte (Quellen-TKÜ) pode levar a perigos, que vão além daqueles de uma intercepção das telecomunicações atuais durante a transmissão da rede.[116] O Tribunal Constitucional Alemão (*BVerfG*) assumiu que as situações de risco não podem ser combatidas, ou não podem ser suficientemente combatidas, pelo artigo 10.1 da Lei Fundamental, quando consistem na coleta de dados sem referência a telecomunicações contínuas após uma infiltração. Ao mesmo tempo, afirmou que o artigo 10.º da Lei Fundamental constitui o único critério de revisão, na medida em que abrange exclusivamente as telecomunicações atuais. A ideia de base dessa afirmação é que a circunstância técnica – quer a monitorização tenha lugar durante a transmissão da rede, quer no dispositivo final – não pode ter qualquer significado para a atribuição do artigo 10.º GG se a intervenção se limitar ao registo da comunicação em curso e, por conseguinte, o potencial de risco especial para a confidencialidade e integridade de sistemas informáticos complexos não for ativado. No

114. Ver, sob a perspectiva do lado da técnica, *Buermeyer,* HRRS 2007, 154, 163 s. Por sua vez, *Böckenförde* (JZ 2008, 925, 933, nota de rodapé n. 95) sublinha que os acessos *on-line* segundo os princípios da proporcionalidade podem, em casos individuais, pesar mais que a instalação de *hardware* em domicílio.

115. O *software* Skype, por exemplo, há muito tempo é considerado à prova de escutas e o exemplo-padrão para a necessidade das *Quellen-TKÜ* [N.T.: uma forma específica de monitoramento e vigilância de telecomunicações criptografadas]. Enquanto isso, entretanto, há indícios crescentes de que existe uma "chave duplicada" (*Nachschlüssel*) para o procedimento de criptografia secreta que também pode ser usada pelas autoridades, de modo que a interceptação também seria possível sem a técnica *Quellen-TKÜ* de monitoramento de telecomunicações criptografadas; ver [www.heise.de/newsticker/meldung/113281].

116. *BVerfG* (nota de rodapé n. 17), nota marginal n. 188 s.

entanto, a turma do Tribunal acrescentou que isso deve ser assegurado por precauções técnicas e garantido adicionalmente por via legal[117].

No entanto, é duvidoso que tais acordos técnicos sejam possíveis atualmente. Na audiência de 10 de outubro de 2007, vários peritos interrogados pelo tribunal negaram tal possibilidade. Na literatura existem também votos afirmativos[118]. No entanto, já existem dúvidas quanto à possibilidade prática de se infiltrar num sistema informático sem obter uma quantidade mínima de informação, por exemplo, sobre as suas vulnerabilidades; o conhecimento dessas vulnerabilidades pode desencadear novas ameaças. Acima de tudo, existem dúvidas quanto ao fato de as arquiteturas informáticas atuais ou previsíveis permitirem um acesso limitado: Uma vez que o *software* tenha sido executado em um sistema, ele pode ser usado universalmente.

As condições prévias para que uma medida diga apenas respeito ao âmbito de aplicação da proteção do artigo 10.º da Lei Fundamental e, por conseguinte, seja considerada apenas por essa norma, não são, de qualquer modo, preenchidas se o sistema de vigilância das telecomunicações depender da infiltração no sistema informático, algo que provoca ou pode causar intervenções relevantes para a personalidade. Aplica-se identicamente essa hipótese se o risco de uma modificação técnica do sistema for criado por infiltração ou em resultado da sua utilização por terceiros. Essas ameaças à proteção da personalidade não podem ser evitadas apenas pelo artigo 10.º da Lei Fundamental.

O teste do direito fundamental à proteção da confidencialidade e da integridade dos próprios sistemas informáticos também não é dispensável pelo fato de a intervenção só ter lugar quando é "necessária" para permitir o controle e a gravação de telecomunicações sob forma não cifrada[119]. Em especial, a proteção mais estrita dos sistemas de tecnologias da informação não deixará de ser aplicável se uma medida promissora de vigilância das telecomunicações não puder ser implementada com êxito sem essa intervenção.

A proteção também não é invalidada pelo fato de o procedimento poder ser anulado posteriormente.[120] Se a integridade e a confidencialidade dos sistemas de tecnologia da informação forem ameaçadas ou mesmo prejudicadas pela intervenção, então a proteção dos direitos fundamentais é ativada, sem que isso seja revertido por uma posterior eliminação das consequências da intervenção – além do fato de que, do ponto de vista técnico, de acordo com os especialistas consultados pelo *BVerfG,* uma restauração completa do *status quo ante* não seria viável. Portanto, também são necessários requisitos substantivos e processuais especiais para uma vigilância de telecomunicações na

117. *BVerfG* (nota de rodapé n. 17), nota marginal n. 190.

118. *Bär* (MMR 2008, 423), por exemplo, responde de forma afirmativa e diz que existe um *software* especial que só abre durante as conversas reais e não requer acesso a outros dados no computador.

119. Cf. a formulação em § 20 l par. 2 n. 1 Nr. 2 do projeto de uma Lei Relativa ao Serviço Federal de Polícia Criminal (*BKA – Gesetz über das Bundeskriminalamt),* BR-Drs. 404/08 de 5. 6. 2008.

120. A suposição por detrás do § 20 l par. 2 Satz 2 em conexão com § 20 k par. 2 Satz 1 Nr. 2 do projeto da Lei-BKA (nota de rodapé n. 119) difere claramente desse ponto.

fonte (Quellen-TKÜ) de acordo com padrões como aqueles do § 100 a StPO (Código de Processo Penal da Alemanha), que foram criados para a vigilância tradicional de telecomunicações, também não contêm autorizações para intervenções dessa intensidade particular; eles também não têm uma limitação a uma "pura" vigilância de telecomunicações na fonte, ou seja, uma garantia legal de que a vigilância das telecomunicações é limitada à comunicação contínua e que isso é tecnicamente garantido[121]. Nesse sentido, não são observados os requisitos de limite formulados pelo Tribunal Constitucional Alemão quanto ao direito fundamental de proteger a confidencialidade e a integridade de sistemas de tecnologia da informação próprios.

Conclusão

Em resumo, pode-se afirmar que o Tribunal Constitucional Alemão reagiu a um potencial de perigo especial, destacando uma necessidade especial de proteção para os sistemas de tecnologia da informação, algo que surgiu como resultado do desenvolvimento da tecnologia informática, de novas constelações das redes, e de muitos novos serviços e possibilidades de infiltração e manipulação nelas baseadas. O objetivo da proteção continua a ser a proteção da personalidade como base para o desenvolvimento autodeterminado. O tribunal afirmou a necessidade constitucional de uma salvaguarda especial da confidencialidade e integridade dos sistemas complexos de tecnologia da informação utilizados pela pessoa em causa, que são particularmente importantes para a liberdade de desenvolvimento pessoal nas condições atuais e aos quais a pessoa em causa se confia sem que seja possível e admissível esperar que ela própria os possa controlar. A proteção oferecida é direcionada contra impactos no próprio sistema de tecnologia da informação, mas ela também inclui proteção contra a coleta e o uso subsequente dos dados resultantes de infiltração no sistema de tecnologia da informação. A Constituição não exige uma proibição estrita de tais efeitos, mas os associa a requisitos especiais de direito material e de direito processual.

Na sua decisão sobre as investigações em linha, o Tribunal Constitucional Alemão não criou um direito fundamental novo, mas fundamentou a decisão no direito fundamental há muito reconhecido à proteção da personalidade; chegando a esse resultado por meio de uma maior diferenciação. Nesse contexto, o tribunal, que deve ser cauteloso com *obiter dicta*, não pode comentar todas as questões em aberto. A jurisprudência e a dogmática jurídica, mas também o legislador, são então chamados a definir os contornos futuros da proteção dos direitos fundamentais.

---

121. *Bär* (MMR 2008, 326) negligencia esse ponto.

Pesquisas do Editorial

Veja também Doutrinas relacionadas ao tema

- Lei Geral de Proteção de Dados em vigor: impactos imediatos e possíveis desafios à luz da experiência da União Europeia, de Marcela Joelsons – *RT* 1022/175-194 (DTR\2020\14365);
- Lei Geral de Proteção de Dados: um estudo comparativo em relação à efetividade dos direitos fundamentais, de Ana Luiza Liz Dos Santos – *RT* 1013/105-126 (DTR\2020\1812);
- O regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência, de Laura Schertel Mendes e Bruno R. Bioni – *RDC* 124/157-180 (DTR\2019\39947); e
- Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de dados no Brasil, de Gianfranco Faggin Mastro Andréa, Higor Roberto Leite Arquite e Juliana Moreira Camargo – *RDCI* 121/115-139 (DTR\2020\11423).

Veja também Jurisprudência relacionada ao tema

- Conteúdo exclusivo web: JRP\2018\1262921, JRP\2018\1262510 JRP\2018\1022656.