O direito de proteção de dados no processo penal e na segurança pública
Orlandino Gleizer, Lucas Montenegro e Eduardo Viana

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Gleizer, Orlandino
O direito de proteção de dados no processo penal e na segurança pública / Orlandino Gleizer, Lucas Montenegro, Eduardo Viana. -- 1. ed. -- Rio de Janeiro: Marcial Pons, 2021.

ISBN 978-65-994688-1-0

1. Processo Penal 2. Processo penal - Brasil 3. Proteção de dados - Leis e legislação 4. Proteção de dados pessoais 5. Segurança pública I. Montenegro, Lucas. II. Viana, Eduardo. III. Título.

21 - 63638 CDU - 342.721

www.marcialpons.com.br

Impresso no Brasil

C.

INTERVENÇÕES INFORMACIONAIS PARA FINS DE SEGURANÇA PÚBLICA

I. A segurança pública como atividade de proteção contra perigos

Um primeiro grupo de medidas interventivas no âmbito constitucionalmente protegido dos dados pessoais é o daquelas realizadas pelo Estado com o fim de *proteção contra perigos para a segurança pública*. Antes de passarmos à exposição concreta das diversas formas de intervenções e seus critérios, são necessárias breves considerações gerais para se compreender o tratamento de dados para fins de garantia da segurança pública no contexto geral dessa atividade estatal e do controle normativo específico que ela pressupõe.[144]

144. Optou-se aqui por não incorporar o uso do termo "polícia", corrente na Europa para se referir a essa atividade estatal dirigida à proteção contra perigos. No Brasil, o termo está muito vinculado aos órgãos denominados policiais (polícias civis e militares, polícia federal, polícia rodoviária federal etc.), ou seja, a um conceito institucional de polícia. Um conceito material de polícia, no entanto, refere-se a toda atividade voltada à proteção contra perigos para a segurança e ordem públicas, e abrange, com isso, também atividades de outros órgãos, como o corpo de bombeiros ou órgãos de controle de trânsito. Optamos, assim, por falar em garantia de segurança pública e direito de segurança pública, para deixar claro, desde o princípio, do que se trata. Sobre os diferentes conceitos de polícia, ver, p.ex., *Schenke* (nr. 88), § 1 nm. 1 ss; *Guedes Valente*, Teoria Geral do Direito Policial, 6. ed. 2019, pp. 54 ss.

A noção de Estado de Direito é profundamente marcada por uma diferenciação de funções estatais que extrapola a conhecida separação entre poderes legislativo, executivo e judiciário[145]. A clara determinação das funções exercidas pela administração pública implica não somente maior eficiência da ação estatal, senão também a possibilidade de ponderar corretamente a legitimidade da medida em face do fim perseguido. Para a atividade dos órgãos dedicados à segurança interna, isso implica *estrita diferenciação* entre atividade de segurança pública, persecução e punição de delitos e inteligência, ainda que essas atividades sejam em parte realizadas pelos mesmos órgãos e possam estar reunidas sob o escopo geral da segurança interna (cf., em mais detalhes, A.III.2).[146] Tratando-se de finalidades distintas, há outros pressupostos para a atuação, e o controle normativo, consequentemente, tem de ser específico para cada uma delas. É essa a razão pela qual o RGPD e a DPD referem-se de forma destacada a cada uma dessas atividades (art. 2° I d RGPD; art. 1° DPD).

Em especial quanto ao tema desta seção, as referidas normas destacam "a salvaguarda e prevenção de ameaças à segurança pública". A ideia de que a atividade de polícia restringe-se à proteção contra perigos para a segurança pública está intimamente vinculada ao desenvolvimento do Estado de Direito e surge, na Alemanha, em contraposição ao chamado Estado policial, em que a atividade de polícia abrange todas as atividades de realização do bem-comum.[147] A polícia, que antes se dedicava à promoção do bem comum em todos os seus aspectos, desde a combate à criminalidade até o controle de vestimenta

---

145. Para os fundamentos, cf. *Lewinski* (nr. 9), p. 55 ss. Para questões gerais da separação de poderes, cf. *Jellinek*, Allgemeine Staatslehre, 3. Aufl. 1914, p. 595 ss; *Schachtschneider*, Prinzipien des Rechtsstaats, 2006, p. 167 ss; *Zippelius*, Allgemeine Staatslehre: Politikwissenschaft, 14. Aufl. 2003, § 31, p. 319 ss. Para breve notícia sobre as origens do Estado de Direito e sua introdução na Alemanha, cf. *Novais*, Contributo para uma teoria do Estado de direito, 2006, p. 29 ss; *Ranieri*, Teoria do Estado, 2. ed. 2018, pp. 227 ss

146. Sobre o conceito de segurança interna, cf. *Götz*, Innere Sicherheit, in: Handbuch des Staatsrechts IV, 3. Aufl., 2006 § 85, p. 673, nm. 3 ss. Para uma análise da segurança como um campo do direito, *Gusy*, Sicherheitsrecht als Rechtsgebiet?, in: Dietricht/Gärditz (org.), Sicherheitsverfassung – Sicherheitsrecht, 2019, pp. 9 ss.

147. Sobre o desenvolvimento histórico do conceito de polícia na Alemanha, ver *Knemeyer*, Polizeibegriffe in Gesetzen des 15. bis 18. Jahrhunderts, AöR 92, 2 Heft, 1967, pp. 153 ss.

ou a realização de cultos religiosos, passa a ter como atribuição exclusiva a proteção contra perigos.

No Brasil, de forma genérica e confusa, a doutrina administrativista menciona um poder de polícia[148] e costuma distinguir entre polícia administrativa e polícia judiciária.[149] Há, no entanto, pouca clareza sobre o significado desses termos. Não há legislação comparável que regule a atividade da polícia preventiva, tampouco disciplina jurídica dedicada ao tema.[150] O próprio texto constitucional não é explícito sobre a quem compete legislar nessa matéria; se União, Estados ou Municípios. Na prática, muitas vezes a atividade de segurança pública é realizada sem amparo legal ou com base em normas do CPP (pensadas para situações distintas), as quais explicitamente se aplicam aos órgãos de polícia apenas quanto ao fim de apuração das infrações penais e da sua autoria (art. 4° CPP). Há, nisso, resquícios de um Estado policial, para cuja superação um direito de proteção de dados pode contribuir.

Um direito de segurança pública deve regular a atividade de órgãos públicos no exercício da competência de *proteção contra perigos*. É essa a principal atribuição da polícia preventiva, que no Brasil é exercida, sobretudo, pelas polícias militares (art. 144 § 5° CF). É possível, seguindo a doutrina alemã, distinguir pelo menos duas atribuições que integram esse conceito de proteção contra perigos.[151]

---

148. Em geral entende-se por poder de polícia os poderes da administração pública para restringir direitos individuais em nome de interesses públicos, ver, p.ex., *Di Pietro*, Direito Administrativo, 33. ed. 2020, capítulo 5. Com razão, *Binenbojm* inclui o chamado poder de polícia dentre os elementos de uma tradição autoritária no direito administrativo brasileiro, cf. *Binenbojm*, Uma Teoria do Direito Administrativo, 3. ed. 2014, p. 3 e pp. 121 ss. Não é correto falar em poder de polícia, simplesmente porque não existe tal poder em um sistema que reconhece direitos fundamentais. O que há, ou deveria haver, é uma série de *autorizações legais* para intervenções proporcionais no âmbito de proteção desses direitos. Somente se satisfeitos os pressupostos previstos em normas de autorização, e apenas dentro dos limites impostos, pode-se reconhecer algum espaço de discricionariedade.

149. Cf. *Bandeira de Mello*, Curso de Direito Administrativo, 32 ed. 2015, pp. 857 ss.; *Di Pietro*, Direito Administrativo, 33. ed. 2020, capítulo 5.4.

150. Embora tenha sido desenvolvido como disciplina jurídica, sobretudo na Alemanha, também se estuda o chamado direito policial em outros países. Em Portugal, p.ex., há inclusive considerável literatura manualística: *Valente* (nr. 144); *de Sousa*, Manual de Direito Policial, 2016; *Raposo*, Direito Policial, 2006.

151. Cf., por todos, *Schenke* (nr. 88), pp. 4 ss.

A primeira delas é a denominada *noção clássica de proteção contra perigos*. Em sua origem, a proteção contra perigos restringia-se à eliminação de potenciais concretos de dano, ou seja, aos casos em que se podia identificar objetivamente perigo concreto e causador. Essa noção clássica de proteção contra perigos tem sido relativizada, em um desenvolvimento intensificado nas últimas décadas, em favor da antecipação da atividade da polícia.[152] Fala-se aqui, especialmente, em *enfretamento preventivo a infrações penais*. Nesse caso, a proteção contra perigos abrange os que ainda não se concretizaram, de maneira que a atividade preventiva é antecipada a momento anterior à perturbação. Muitas medidas de tratamento de dados inserem-se no âmbito dessa atribuição de enfrentamento preventivo a infrações penais, como o controle de identidade ou a utilização de câmeras de vigilâncias. Vale ressaltar de antemão que, em face da inexistência de um perigo concreto e do caráter antecipado da medida, exige-se aqui um juízo mais rigoroso de proporcionalidade.[153]

Feitas essas considerações sobre as atribuições de órgãos estatais no exercício da atividade de segurança pública, serão apresentadas a seguir as bases para o desenvolvimento de normas de autorização para o tratamento de dados no âmbito dessa atividade.

II. Aspectos centrais de um direito de segurança pública: bem protegido, perigo e destinatários

Normas de autorização somente podem ser avaliadas em sua adequação quando consideradas em relação ao fim estatal específico que se busca realizar. Assim, normas que autorizem o tratamento de dados no âmbito da segurança pública pressupõem a compreensão precisa do que caracteriza essa atividade. Uma vez que um direito de segurança pública é praticamente inexistente no Brasil[154], impõem-se alguns esclarecimentos sobre aspectos centrais desse ramo jurídico.

---

152. Em detalhes, apontando os problemas da relativização da noção clássica de proteção contra perigos, *Denninger*, Polizeiaufgabe, in: Lisken/Denninger (org.), Handbuch des Polizeirechts, 5. Aufl., 2012; nm. 1 ss.

153. Cf. *Schenke* (nr. 88) p. 5.

154. Isso logo será notado: a parca referência à bibliografia brasileira é o atestado da nossa constatação.

O direito de segurança pública regula ações estatais que a) visam à proteção da *segurança pública* b) contra *perigos*, c) sendo que essas ações afetam determinados *destinatários*, geralmente, em âmbito constitucionalmente protegido. Analisemos então esses três aspectos centrais em separado.

1. Bem protegido: a segurança pública

Por segurança pública entende-se, principalmente, determinado estado de coisas: *a ausência de violação da ordem jurídica*.[155] Embora se fale em bem protegido, segurança pública não designa um conteúdo material próprio, mas existe apenas em referência às demais normas que compõem a ordem jurídica. Papel de maior relevância cabe às normas que estabelecem delitos e contravenções penais, pois designam condutas violadoras do direito. Em relação a normas de direito privado, a intervenção de órgãos da segurança pública deve ser subsidiária à proteção jurisdicional, sendo lícita apenas nos casos em que, sem a atuação daqueles órgãos, a realização de um direito se torna impossível ou muito improvável.[156]

Em sua maior parte, a atividade de segurança pública se volta contra *violações* da ordem jurídica; no entanto, como a noção de violação pressupõe uma ação humana, a doutrina estrangeira menciona também outras duas concretizações do conceito de segurança pública: a *integridade de bens individuais* e a *existência e funcionamento de instituições estatais*. Essas duas concretizações são residuais e aplicam-se, sobretudo, em caso de eventos naturais que geram danos e perigos a direitos individuais e instituições – p.ex. no caso de incêndios, catástrofes naturais ou acidentes que gerem perigos para os bens referidos. Complementa-se, com isso, o conceito de segurança pública.[157] Além disso, boa parte da doutrina discute, sob a rubrica da integridade de bens individuais, medidas tomadas para evitar perigos

155. Cf., p.ex., *Kingreen/Poscher* (nr. 93), pp. 99 ss., nm. 2 ss.; *Gusy*, Polizei- und Ordnungsrecht, 10. Aufl. 2017, p. 39; *Götz/Geis*, Allgemeines Polizei- und Ordnungsrecht, 16. Aufl., 2017, p. 22 ss.; *Denninger* (nr. 152) nm. 17.

156. Essa subsidiariedade em relação à proteção jurisdicional de direitos privados está prevista, na Alemanha, nas próprias leis policiais. Ver, por exemplo, Art. 2 Abs. 2 da Lei Policial da Baviera ou § 1 Abs. 4 da Lei Policial de Berlim.

157. Cf. *Kingreen/Poscher* (nr. 93), p. 105, nm. 21.

que o próprio titular do direito gera para si mesmo, em especial, especialmente para evitar o suicídio.[158]

Nesse contexto, debate-se também a respeito da *ordem pública* como um bem protegido, considerando-se por ordem pública o conjunto de normas sociais e morais amplamente aceitas e necessárias para a convivência pacífica.[159] No Brasil, os conceitos de ordem e segurança pública são utilizados muitas vezes de forma indiscriminada.[160] Se por ordem pública entende-se determinada ordem social e moral, isso, em nossa opinião, não deve ser tido por um bem protegido, pois, nesse caso, emprega-se um conceito de difícil determinação, vulnerável a abusos e moralismos.[161]

2. Perigo

Perigo é o conceito mais importante para o direito de segurança pública. Por um lado, esse conceito distingue a atividade de segurança pública da atividade de persecução penal (que não se vincula a perigos, mas a suspeitas); de outro, ele a separa também das atividades dos órgãos de inteligência. Esses atuam previamente à segurança pública, prescindem da vinculação estrita à ocorrência de um perigo, mas não gozam de autorização para uma série de medidas a que a polícia está autorizada (busca e apreensão, detenção, identificação criminal etc.)[162]. Ou seja, a inteligência não pode agir (ver acima A.III.2).

---

158. Cf. *Götz/Geis* (nr. 155), p. 27 s., nm. 28, 30, 32 ss. Esses casos de autocolocação em perigo, inclusive o suicídio, são, no entanto, problemáticos, pois entram em conflito com a ideia de autodeterminação. Menos problemáticos são os casos em que o titular não sabe que está gerando perigos para seus bens, pois esses comportamentos não estariam abrangidos pelo direito à autdeterminação; assim, Cf. *Kingreen/Poscher*, (nr. 93), p. 106, nm. 25.

159. Assim, p.ex., a definição legal de ordem pública no § 3 II das Lei Policial de Sachsen-Anhalt: "O conjunto de regras não escritas para o comportamento de indivíduos em espaços públicos que se situem dentro dos limites constitucionais e cuja observação é tida, na concepção da maioria, como uma condição indispensável para a convivência pacífica dos cidadãos."

160. A própria CF, por exemplo, no capítulo intitulado "Da segurança pública", atribui às polícias militares a preservação da ordem pública (art. 144 § 5°). Também o Anteprojeto inclui a preservação da ordem pública como uma atribuição que define a atividade de segurança pública (art. 5 XXI).

161. Assim também *Kahl*, Verwaltungsarchiv 2008 451, 455 ss. Um panorama da discussão em torno do conceito de ordem pública na Alemanha, também com críticas à figura, é oferecido por *Bäcker*, Kriminalpräventionsrecht, 2015, pp. 312 ss.

162. Nesse sentido, *Götz* (nr. 146) § 85, p. 693 s. nm. 39.

Perigo deve ser compreendido como a *probabilidade suficiente* de que uma situação ou um comportamento produzirá um dano a um bem jurídico, caso não haja uma intervenção no curso esperado dos acontecimentos.[163] Obviamente, o adjetivo "suficiente" designa o grau de probabilidade que não pode ser determinado com perfeita exatidão, mas oferece algum parâmetro de controle. Ao mesmo tempo em que não é necessário ter absoluta certeza sobre a ocorrência do dano, tampouco é suficiente a mera possibilidade de produção desse dano, na forma de suposições sem fundamentos fáticos.

No direito de segurança pública, costuma-se distinguir perigos concretos de abstratos, conferindo-lhes sentido distinto do emprego tradicional em direito penal.[164] Perigos concretos dizem respeito a casos individuais em que há probabilidade suficiente de dano a bens jurídicos, como, por exemplo, uma colérica discussão entre dois jovens alcoolizados em um bar. Nesse caso, a ocorrência do dano pode ser previsivelmente concretizada em todos os aspectos relevantes: *material* (integridade corporal), *pessoal* (dois jovens), *espacial* (no bar) e *temporal* (momento da discussão). Perigos abstratos referem-se a situações ou a comportamentos que, notoriamente ou em razão de conhecimentos científicos, *tipicamente* geram perigos para bens jurídicos. O porte de armas de fogo e o consumo de bebidas alcoólicas em estádios de futebol, por exemplo, podem ser considerados como situações que tipicamente conduzem a perigos.

Por fim, nesse contexto, a *intensidade* do dano provável também assume relevância. Quanto maior a intensidade do dano, menores são as exigências de probabilidade para a verificação de um perigo relevante. Por outro lado, se o dano é irrelevante, assumindo a forma de meros incômodos, tampouco há que se falar em perigo no sentido acima referido. Esse é o caso, por exemplo, da prática de mendicância.[165]

---

163. Sobre essa definição e demais especificações do conceito de perigo apresentadas a seguir, cf. *Kingreen/Poscher* (nr. 93), pp. 114 ss.; *Götz/Geis* (nr. 155), p. 42 ss.; *Denninger* (nr. 155), nm. 39 ss.

164. Por todos, *Kingreen/Poscher* (nr. 93), pp. 117 ss. Sobre a distinção em direito penal, cf. *Roxin/Greco*, Strafrecht AT, § 10 nm. 123 s.

165. *Kingreen/Poscher* (nr. 93), p. 116. Anacrônica é a disposição na Lei de Contravenções Penais (Decreto-Lei 3.688) segundo a qual se devem presumir perigosos

Apesar de todos esses esforços de precisão, não há como negar certo grau de indefinição do conceito de perigo, mas os elementos referidos oferecem parâmetros não somente para excluir casos extremos, aos quais o conceito evidentemente não se aplica, senão também funcionam como *critérios para a proporcionalidade* da medida e do nível de intervenção tolerável em direitos fundamentais. Em geral, perigos concretos e danos mais intensos autorizam intervenções mais invasivas do que perigos abstratos e danos de menor intensidade.

3. Os destinatários

Em regra, as medidas de garantia da segurança pública devem ter por destinatário os denominados "perturbadores", isto é, aqueles a quem se pode atribuir a causa do perigo. Essa classe dos perturbadores subdivide-se em perturbadores por comportamento (*Verhaltensstörer*), quando o perigo é substanciado em uma ação ou omissão; e perturbadores por estado (*Zustandsstörer*), nos casos em que o perigo advém de algo pelo qual o destinatário é responsável.[166] Excepcionalmente, medidas de segurança pública podem também alcançar *terceiros inevitavelmente afetados*, nos chamados estados de necessidade policiais[167], que infelizmente não estão regulados no direito brasileiro. Seria esse o caso, por exemplo, quando a polícia, para resgatar a vítima de um sequestro, invade a propriedade de um terceiro.

Há além disso medidas que, por sua natureza, não permitem restrição à figura do perturbador, como o uso de câmeras de vigilância em espaços públicos. Em especial, essa ampliação é particularmente comum em regras que autorizem o tratamento de dados para fins de enfrentamento preventivo de crimes. Como consequência, a licitude da medida deve estar estritamente submetida à *proibição de excesso*. Assim, a verificação de identidade não deve ser autorizada em relação a toda pessoa, em qualquer circunstância, mas apenas em relação a pessoas, por exemplo, que se situem em locais com alto índice de criminalidade. No Brasil, embora a Lei 12.037/09 disponha sobre

os indivíduos condenados por mendicância ou vadiagem (art. 14 II), uma vez que foi revogado o art. 60 daquela mesma lei que proibia a mendicância.

166. Cf. *Kingreen/Poscher* (nr. 93), pp. 138 ss.; *Gusy* (nr. 155) pp. 203 ss.; *Götz/Geis* (nr. 155), pp. 87 ss.

167. Cf., por todos, *Schenke* (nr. 88), pp. 216 ss.

identificação criminal, não há regulação sobre em que situações a polícia está autorizada a verificar a identidade dos cidadãos. A possibilidade de levantamento indiscriminado de dados de identificação não é compatível com as exigências de proporcionalidade.

III. Autorizações para o levantamento de dados pessoais

É esse, portanto, o quadro geral em que se devem inserir as normas de autorização para tratamento de dados pessoais no âmbito da segurança pública. Além de requisitos formais de licitude dos respectivos atos, a elaboração de normas para o tratamento de dados tem sempre de considerar os bens protegidos, o perigo em questão e o grupo dos destinatários. Esses três elementos compõem também a base para o juízo de proporcionalidade da medida.

A primeira ação estatal a demandar autorização é o levantamento de dados, o qual está compreendido pelo conceito abrangente de tratamento de dados pessoais (art. 5° X LGPD, sob a denominação de coleta), e sua regulação deve constituir significativa – senão a principal – parte das normas de tratamento de dados para a segurança pública. As leis policiais alemãs, por exemplo, nesse ponto costumam valer-se da combinação entre normas específicas de autorização e cláusulas gerais que autorizam o levantamento de dados pessoais.[168] A cláusula geral, no entanto, *não* é subsidiária no sentido de ser aplicável caso os requisitos de uma autorização específica não estejam presentes. Ao contrário, sem a presença dos requisitos para o levantamento de dados por meio de uma infiltração *online*,[169] por exemplo, não é possível se valer de uma cláusula geral (cf. A.II) para realizar tal medida. Uma cláusula geral de autorização somente pode ser aplicável no caso de *medidas atípicas*, as quais, por sua natureza excepcional, não são passíveis de regulação por norma especial.[170]

---

168. Por exemplo, arts. 30 - 52 da Lei Policial da Baviera; §§ 19 – 25 da Lei Policial de Baden-Württemberg; §§ 13, 14 – 19 da Lei Policial de Hessen; §§ 30 – 36a das Lei Policial da Baixa-Saxônia; §§ 55 – 71 da Lei Policial da Saxônia.

169. A esse respeito, cf. *Greco/Gleizer* RBDPP vol. 5 n. 3, 1483, pp. 1498 ss.

170. Sobre a sistemática de cláusulas gerais e autorizações especiais para o levantamento de dados, cf. *Kingreen/Poscher* (nr. 93), p. 205. Sobre o emprego de cláusulas gerais do direito de policial de modo geral, ver, especialmente, *Vogel/Martens*, Gefahrenabwehr, 9. Aufl. 1985, pp. 219 ss.

No caso ideal, cláusulas gerais só devem autorizar intervenções de baixa intensidade (intervenções bagatelares). Na medida em que elas reduzem a previsibilidade por parte do indivíduo de quais medidas ele deve tolerar, é exigível que essas, pelo menos, não sejam graves. Medidas de maior grau interventivo exigem, assim, regramento específico. Isso é uma decorrência do mandato de determinação, um dos requisitos de constitucionalidade da intervenção (cf. A.IV). Para o levantamento de dados, são comuns, por exemplo, normas específicas de autorização para a seguintes medidas: verificação de identidade, medidas de identificação criminal, levantamento de dados em eventos públicos, utilização de câmeras de vigilância, controle de tráfico e identificação de veículos, observações duradouras, agentes infiltrados, gravações ambientais em domicílio, interceptações telefônicas e infiltrações online.[171]

A seguir serão oferecidas algumas balizas gerais para a criação de normas específicas de autorização para o levantamento, que serão então exemplificadas em duas medidas concretas.

1. Critérios para regras especiais de autorização

a) Licitude formal

Autorizações especiais devem estar submetidas a diferentes requisitos formais, a depender da natureza da medida em questão. Um primeiro aspecto importante é considerar se o levantamento é realizado explicitamente, como no caso da coleta de depoimentos ou da verificação de identidade. Neste caso, pode-se vincular a licitude do ato à instrução sobre o direito de permanecer calado ou ao esclarecimento sobre a razão da medida. Visto que a maioria das medidas não são explícitas, esses critérios têm pouca relevância.

Papel mais relevante, por outro lado, cabe à existência e aos requisitos de uma *ordem escrita* como pressuposto formal para algumas formas de tratamento de dados, em especial, para formas mais interventivas de levantamento. Quanto mais invasiva for a ação estatal, mais deve-se vincular a licitude do ato à determinação por superior hierárquico ou submetê-la a uma reserva de jurisdição, ainda

171. Para um breve panorama, ver *Becker/Ambrock* JA 2011, 561 (563 ss.).

que para uma atividade que – por natureza – prescinda de suspeita e, portanto, de um processo penal. Medidas extremamente invasivas ao indivíduo, como escutas ambientais, interceptações telefônicas e infiltrações *online*, portanto, somente podem ser praticadas mediante autorização judicial (com exceções autorizadas para casos de urgência, que preveem mecanismos de controle contra arbítrio). Nesses em que se exige autorização, a determinação escrita precisa também especificar o conteúdo, a forma e a duração da medida. Em que pese essas exigências terem sido parcialmente assimiladas no contexto do processo penal brasileiro, ainda não o foram em relação às atividades de proteção contra perigos, ou seja, de segurança pública.

b) Licitude material

Critérios materiais para a formulação de normas de autorização são concretizações dos três aspectos centrais expostos: o bem protegido, o perigo e os destinatários da medida de levantamento de dados.

Em primeiro lugar, portanto, o bem protegido serve de ponto de apoio para a criação de normas especiais. Poucas medidas especiais de tratamento de dados deveriam ter como bem protegido a segurança pública de forma ampla, sem que sejam discriminados bem jurídicos concretos. Para a maioria das medidas e para as mais gravosas, em especial, o princípio da proporcionalidade exige que a medida apenas seja autorizada para o afastamento de perigos a *bens jurídicos específicos*. Muitas leis policiais alemãs, por exemplo, vinculam o levantamento de dados por meios particularmente gravosos, como observações duradouras, infiltração de agentes ou localização eletrônica, à proteção da existência e segurança de instituições estatais ou da vida, saúde ou liberdade de uma pessoa[172]. Essa vinculação legal da legitimidade da medida em relação a determinados bens protegidos de particular relevância é um instrumento fundamental de controle e garantia da proporcionalidade do tratamento de dados.

Outra importante forma de controle legal vincula-se à natureza do perigo em questão. Fundamental, nesse sentido, é a diferenciação entre as *espécies de perigo*, sobretudo a distinção, antes menciona-

172. A exemplo da intervenção na confidencialidade e integridade de sistemas informáticos, vide BVerfGE 120, 274.

da, entre perigos concretos e abstratos. Em regra, as medidas são autorizadas para a proteção contra perigos concretos. A ampliação para perigos abstratos exige uma justificação específica e restrições correspondentes. Por exemplo, a verificação de identidade ou o uso de câmeras de vigilância autorizam intervenções podem prescindir da existência de perigo concreto, mas o levantamento de dados está restrito a determinadas localidades, nas quais se justifica proteção antecipada. Outra restrição possível é vincular o perigo abstrato a indícios concretos de que delitos especialmente graves serão cometidos.

Quanto aos destinatários, as medidas devem se voltar em primeira linha contra os perturbadores, ou seja, os responsáveis por causar o perigo concreto. A depender da situação, esse grupo pode ser ampliado para contatos do perturbador ou *terceiros inevitavelmente afetados*, nos chamados estados de necessidade policiais. E, como visto, há também medidas que, tendo por objeto perigos abstratos, não permitem restrição à figura do perturbador, como o emprego de câmeras de vigilância.

2. Dois exemplos de autorizações especiais no direito alemão

a) A identificação eletrônica de veículos automotivos

Atualmente, em vários países, órgãos de segurança pública contam com um sistema automatizado de identificação de automóveis. Por meio de câmeras de vídeo, faz-se o reconhecimento óptico da sequência que identifica os veículos, registrada e empregada para fins diversos. No Brasil, circulam na mídia notícias sobre a utilização dessa tecnologia não apenas por órgãos de trânsito, mas também por órgãos de segurança pública e investigação criminal, inclusive com a possibilidade de cruzamento dos dados levantados com outros, pertinentes a bancos de dados estatais.[173] Há, entretanto, pouca discussão sobre a forma e as condições em que o reconhecimento automatizado de placas pode ser empregado. Embora essa tecnologia

173. Ver, p.ex., matéria do Intercept Brasil sobre o sistema Córtex, supostamente utilizado pelo Ministério da Justiça. Acessível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/. Há também notícias que reportam a utilização dessa tecnologia pelas polícias estaduais. Ver, p.ex.: https://paranaportal.uol.com.br/geral/geral-geral/452-pre-testa-viaturas-placas/.

contribua inquestionavelmente para a maior eficiência das atividades de prevenção e investigação, ela permite um levantamento massivo e indiscriminado de dados pessoais, os quais, combinado com outras formas de tratamento, resulta em grave ameaça a um regime de proteção da personalidade.

Tornar a utilização dessa tecnologia compatível com um regime de proteção à autodeterminação informacional é uma tarefa das normas de autorização. Nisso a experiência alemã, que conta já com alguns anos de utilização dessa técnica e com uma regulação clara da matéria, inclusive com algumas decisões do BVerfG[174], também pode servir de ponto de partida para se pensar uma regulação própria para o Brasil. A seguir serão expostos os aspectos centrais da regulação dessa medida na Alemanha e uma versão traduzida de um dispositivo contendo uma norma autorizativa.

A tecnologia de reconhecimento automatizado de placas é, em geral, empregada na localização de pessoas ou objetos (*Fahndung*) e dá-se de acordo com o seguinte procedimento:[175] com base na imagem gerada por câmeras fixas ou móveis, um *software* faz o reconhecimento óptico da sequência de caracteres e números, que é armazenada e comparada com os dados referentes ao objeto da busca. No caso de coincidência, o sistema notifica os agentes públicos, que então realizam as medidas necessárias (apreensão do veículo, prisão do foragido etc.). Os contornos para o uso proporcional dessa medida foram estabelecidos, em boa parte, pela própria jurisprudência constitucional, que conta com algumas decisões especificamente sobre normas que autorizam a identificação eletrônica de veículos.

Em um primeiro momento, em decisão de 2008, o BVerfG analisou a constitucionalidade de dois dispositivos das leis de polícia dos Estados de Hessen e Eslésvico-Holsácia, que autorizavam o levantamento da identificação dos veículos para fins de localização de pessoas e coisas.[176] O tribunal considerou que o levantamento não implicava intervenção no âmbito de proteção do direito à autodetermi-

174. BVerfGE 120, 378; BVerfGE 150, 244.

175. Para uma descrição do procedimento, com mais referências, ver *Roßnagel* NJW 2008, 2547; *Guckelberger* NVwZ 2009, 352.

176. BVerfGE 120, 378.

nação informacional nos casos em que o sistema aponta um resultado negativo do cruzamento de dados, desde que os dados levantados fossem imediata e automaticamente eliminados e não permitissem a identificação dos afetados.[177] Nessa decisão estabeleceu-se, no entanto, que a autorização para o fim genérico de comparar os dados levantados com aqueles que se busca não seria suficiente. Seriam necessárias maiores especificações desse fim. Além disso, o princípio da proporcionalidade exigiria que a medida não fosse empregada de forma ampla e indiscriminada, desvinculada, portanto, de um *ensejo concreto*.[178]

Além disso, em uma decisão recente, o tribunal revisou a afirmação de que o levantamento massivo, seguido da imediata eliminação dos dados, não interviria no direito à autodeterminação informacional.[179] Tratava-se, no caso, de uma norma da Lei Policial da Baviera, que autorizava a criação de postos de controle. Considerou-se, nesse caso, que os afetados não tinham seus dados levantados de forma acidental ou como consequência necessária da tecnologia empregada, senão que eram objeto direto de controle dos órgãos policiais. O simples fato de saber que seus dados estão sendo controlados teria consequências para o exercício da liberdade, pois implicaria situação em que, sendo indiscriminadamente registrados, os cidadãos teriam um sentimento de vigilância constante. Isso acarretaria intervenção no direito à autodeterminação informacional e estaria sujeito a requisitos mais estritos.[180] Além da necessidade já afirmada de um ensejo concreto o emprego da medida, a proporcionalidade da intervenção exigiria também que a técnica fosse empregada apenas para a proteção de *bens jurídicos relevantes* ou *interesses públicos de correspondente peso*.[181]

Partindo-se dos critérios mencionados acima e de suas concretizações nas decisões referidas, chega-se, para o direito alemão, aos seguintes requisitos que uma norma de autorização para o emprego dos sistemas de reconhecimento de placas precisa conter. Quanto ao bem protegido, não é suficiente a mera referência à segurança

177. BVerfGE 120, 378, 399.
178. BVerfGE 120, 378, 430.
179. BVerfGE 150, 244.
180. BVerfGE 150, 244, 266 ss.
181. BVerfGE 150, 244, 287 ss.

pública. É necessária a restrição a determinados bens jurídicos ou interesses públicos especialmente relevantes. O perigo em questão tanto pode ser concreto quanto abstrato. No último caso, contudo, é necessário um ensejo concreto, um motivo fundado, para a medida. A isso se vincula um requisito formal para a licitude da medida, a saber, a fundamentação da medida com base nos elementos fáticos que a justifiquem. Não há restrições quanto aos destinatários porque a medida afeta, em princípio, todas as pessoas que tomam parte no tráfico de veículos

O art. 39 das Lei Policial da Baviera, destinado exclusivamente à identificação eletrônica de veículos, oferece-nos um exemplo do que seria uma norma de autorização conforme os requisitos mencionados:

> **Art. 39 Sistemas automatizados de reconhecimento de placas**
>
> (1) [1]A polícia poderá, por meio do uso oculto de sistemas automatizados de reconhecimento de placas, levantar a identificação de veículos automotivos, bem como lugar, data, horário e direção, se a situação é correspondente à dos casos previstos no Art. 13 I 1 até 5. [2]No caso do art. 13 I 1 a, a autorização vale apenas em relação a um perigo para um bem jurídico relevante e, no caso do art. 13 I 5, apenas para rodovias europeias ou federais. [3]O cruzamento da identificação com os dados policiais de busca será permitido
>
> 1. para veículos ou placas
>
> a) extraviados por meio de crimes ou de outra forma ou
>
> b) em relação aos quais há indícios de que serão utilizados para cometer crimes,
>
> 2. para pessoas registradas
>
> a) para observação policial, controle dirigido ou registro oculto,
>
> b) em razão de persecução ou execução penal, extradição ou transferência,
>
> c) para a realização de medidas de direito estrangeiro,
>
> d) para que contra ela se realizem medidas determinadas para a proteção contra perigos.
>
> [4]Um cruzamento com arquivos policiais criados para a proteção contra perigos em casos concretos ou em relação a acon-

tecimentos que impliquem perigos de modo geral será permitido apenas quando necessário para a proteção contra aqueles perigos. [5]O levantamento da placa não será empregado de forma ampla e indiscriminada.

(2) [1]As medidas constantes de Abs. 1. serão apenas ordenadas pelas pessoas previstas no Art. 36 IV S. 2 e 3. [2]A ordem escrita deverá conter o destinatário e forma, amplitude e duração da medida concreta, bem como a seleção dos dados ou arquivos de busca e os motivos essenciais para sua determinação, inclusive a descrição das circunstâncias fáticas.

(3) [1]Os dados referentes às placas levantadas com base em Abs. 1 serão imediatamente eliminados após o cruzamento de dados, sempre que a placa não corresponder aos dados ou arquivos da busca. [2]Exceto nos casos previstos em Abs. 1 S. 3 Nr. 2, os reconhecimentos individuais não serão vinculados a uma imagem em movimento. [3]Cruzamentos segundo Abs. 1 não serão protocolados.

O art. 13 I, a que se refere o dispositivo traduzido, regula as hipóteses em que a polícia está autorizada a realizar o controle de identidade. Esse controle é cabível, especialmente, em face da existência de perigos concretos (art. 13 I 1) e em determinadas localidades tidas por perigosas (art. 13 I 2). O legislador bávaro optou, então, por aplicar essas hipóteses também ao uso de sistemas de levantamento de placas.

b) Câmeras de vigilância em espaços públicos

O emprego de câmeras de vigilância por órgãos de segurança pública é uma prática há muito corrente em várias cidades brasileiras. O amplo uso dessa tecnologia contrasta, todavia, com a extrema deficiência de sua regulação, embora sejam evidentes os riscos de uma vigilância descontrolada pelo poder estatal. A escassa regulação da matéria em lei, quando tal regulação existe, é claramente ilegítima. Assim, por exemplo, a Lei 15.518/04 do Estado de São Paulo, com o seguinte teor:

> Artigo 1º – Serão instaladas câmeras de monitoramento e vigilância nas áreas com índice de ocorrências policiais no Estado de São Paulo.

Artigo 2º – Vetado.

Artigo 3º – As despesas decorrentes da execução desta lei correrão à conta de dotações orçamentárias próprias, suplementadas se necessário.

Artigo 4º – Esta lei entra em vigor na data de sua publicação.

Um regime que leve a sério a proteção de dados como parte do direito fundamental ao livre desenvolvimento da personalidade não pode se contentar com uma regulação indeterminada e deficiente de uma prática com potencial tão invasivo quanto o uso de câmeras de vigilância e o posterior tratamento dos dados levantados.

Câmeras de vigilância em espaços públicos podem ser empregadas pelo menos de três formas distintas.[182] A primeira consiste na simples observação, sem que as imagens produzidas sejam gravadas. As câmeras seriam o correspondente automatizado do policial que faz a ronda nas ruas. A doutrina alemã discute se o denominado monitoramento panorâmico (*Übersichtsaufnahmen*), em que se produzem imagens aéreas de terminado local, sem direcionar a observação a uma pessoa específica, por si só, implicaria uma intervenção no direito à autodeterminação informacional.[183] A maior parte da doutrina parece considerar toda forma de monitoramento por câmeras como uma forma de intervenção, sempre que essa tecnologia ofereça possibilidades (*zoom*, câmera lenta e congelamento de imagens, movimento de câmeras etc.) não comparáveis à atividade de policias em ronda ou em postos de observação.[184] Ou seja, quase sempre.

A segunda forma consiste na gravação das imagens produzidas, técnica que aumenta o potencial de ação dos órgãos de segurança para além da reação imediata a delitos e do efeito inibidor da presença de câmeras. As gravações servem, sobretudo, como meios de prova para

182. Assim, *Zöller* NVwZ 2005, 1235, 1235 s.

183. Para um resumo da discussão, com mais referências, ver *Bartsch*, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und in den USA, 2004, pp. 114 ss.; *Roggan* NVwZ 2001, 134, 135 ss.

184. Cf. *Schnabel* NVwZ 2010, 1457; *Bartsch*, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und in den USA, 2004, pp. 118 ss.; *Roggan* NVwZ 2001, 134, 135 s.; *Keller*, Kriminalistik 2000, 188.

uma eventual instrução criminal. Discute-se, assim, se a regulação desse tipo de atividade diz respeito de fato à segurança pública ou se seriam medidas atinentes à garantia da persecução criminal efetiva.[185] Em todo caso, a gravação das imagens representa uma intervenção na autodeterminação informacional de natureza e intensidade distintas da mera observação e exige, por consequência, regulação em lei. Para o BVerfG, a mera regulação em lei não é suficiente, mas, em face do caráter invasivo da medida, haveria de se atentar às exigências particulares de determinação e clareza da norma. Concretamente, a gravação em espaços públicos não poderia se valer de cláusula geral de autorização, mas deveria estar regulada em autorização especial.[186]

Uma terceira e especialmente gravosa utilização de câmeras combina-a com um sistema de reconhecimento de dados biométricos, especialmente *reconhecimento facial*. De forma semelhante ao sistema de identificação de veículos, por meio de um *software* comparam-se os dados biométricos levantados, por exemplo, com o rosto de uma pessoa procurada[187]. Essa tecnologia ainda não é empregada na Alemanha[188], ao contrário de países como Inglaterra e China[189], nos quais é amplamente usada; é discutível se as normas existentes que autorizam o uso de câmeras se aplicariam também a essa modalida-

185. Sobre a intensa discussão em torno da competência para legislar sobre medidas preventivas de garantia da persecução criminal, ver, por exemplo, *Weßlau/Puschke*, SK-StPO, Vor § 474 StPO, nm. 19 ss.

186. BVerfG NVwZ 2007 688, 691.

187. Veja-se, por exemplo, dois casos emblemáticos ocorridos no Brasil em que se fez uso do sistema de reconhecimento facial. No primeiro, no carnaval do Rio de Janeiro, em 2019, quatro pessoas cujos mandados de prisão estavam em aberto foram detidas; no segundo, no carnaval de Salvador, um indivíduo, procurado por homicídio, também foi preso em razão do reconhecimento facial. Notícias disponíveis, respectivamente, in: https://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoes-no-carnaval-do-rio e https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml.

188. Havia, até pouco tempo atrás, um projeto do Ministério do Interior para utilização da tecnologia de reconhecimento facial em estações, o qual parece ter sido abandonado, ver: https://www.sueddeutsche.de/digital/seehofer-gesichtserkennung-bahnhof-polizei-gesetz-1.4769958.

189. Sobre o uso pela polícia metropolitana em Londres, p. ex., notícia disponível em: https://www.bbc.com/news/uk-51237665. Sobre o emprego massivo na China, notícia disponível em: https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled.

de sem que as exigências constitucionais de clareza, determinação e proporcionalidade restem desrespeitadas.[190]

Todos as leis policiais alemãs contam com uma norma específica de autorização para a observação e gravação por meio de câmeras em espaços públicos.[191] Em parte dessas normas, o levantamento dos dados restringe-se à proteção de bens públicos de particular relevância. As exigências referentes à natureza do perigo são semelhantes às da identificação automatizada de veículos. O emprego para a proteção contra perigos abstratos limita-se a locais públicos nos quais não há prática reiterada de delitos ou onde há motivos concretos para se esperar a sua ocorrência. Considera-se, em regra, que a adequação da medida exige o uso explícito de câmeras, pois, do contrário, não teriam o desejado efeito inibidor e não seriam adequadas para a prevenção contra perigos.[192] A utilização ampla e indiscriminada também é tida por inconstitucional.

A título de exemplo, recorremos mais uma vez à Lei Policial da Baviera, cujo art. 33, na parte que aqui nos interessa, dispõe:

> **Art. 33 Captação explícita de imagens e áudio**
>
> (1)...
>
> (2) A polícia poderá
>
> 1. para a proteção contra
>
> a) um perigo ou
>
> b) uma ameaça* para um bem jurídico relevante
>
> 2. nos locais enumerados no Art. 13 I 2, quando de acesso público, ou
>
> 3. em locais em relação aos quais há fundamentos fáticos para assumir que lá serão cometidas contravenções de particular relevância ou crimes, quando esses locais sejam de acesso público,

190. Heldt, MMR 2019, 285, 287.

191. Cf., com referências aos dispositivos nas leis policiais, *Kingreen/Poscher* (nr. 93), p. 233, nm. 97.

192. Cf. *Kingreen/Poscher* (nr. 93), p. 235, nm. 104, com mais referências.

* No original, "drohende Gefahr". É empregado como uma forma amenizada do perigo concreto, quando não se pode determinar suficientemente quando e onde o dano ocorrerá. Sobre o polêmico conceito de "drohende Gefahr", cf. *Kingreen/Poscher* (nr. 93), pp. 121 s., com mais referências.

realizar a captação explícita e a gravação de imagens e áudio de pessoas.

(3) A polícia poderá, nos objetos elencados no Art. 13 I 3, realizar a captação explícita e a gravação de imagens e áudio de pessoas, desde que haja fundamentos fáticos para assumir que nos arredores ou no interior desses objetos serão cometidos crimes que ponham em perigo os próprios objetos, bem como pessoas ou coisas situadas em seu interior.

(4) ...

(5) Nas medidas contidas nos Abs. 1 até 3, poderão ser utilizados sistemas de reconhecimento e análise de padrões em relação a coisas, inclusive sistemas de direcionamento, na medida em que correspondam ao conhecimento dos perigos que a situação implica.

(6) [1]Nas medidas elencadas nos Abs. 1 até 4, a polícia sinalizará de forma apropriada a captação e gravação de imagens e áudio, exceto se estas forem evidentes ou no caso de urgência da medida. [2] O uso dos sistemas previstos no Abs. 5 deve ser sinalizado de forma destacada.

(7) As medidas previstas nos Abs. 1 até 5 serão permitidas também nos casos em que houver terceiros inevitavelmente afetados.

(8) [1]A captação e a gravação de imagens e áudio, bem como os documentos que daí resultarem, serão eliminados no prazo máximo de dois meses após o levantamento dos dados, exceto quando necessários

1. para a persecução de contravenções de particular relevância ou crimes,

2. para a verificação da licitude da medida policial, quando há a expectativa de que uma verificação será necessária, ou

3. para o fim de informação segundo o Art. 50 Abs. 1 S. 1 Nr. 1, quando o levantamento ocorre segundo o Art. 5 S. 2.

[2]A eliminação será documentada.

(9) ...

3. Critérios para criação de cláusulas gerais

Cláusulas gerais de levantamento de dados de forma alguma devem constituir carta branca aos órgãos de segurança pública. É isso,

exatamente, o que se quer evitar por meio da proteção jurídica de um direito fundamental. A aplicação dessas cláusulas é excepcional e cabível apenas se satisfeitos critérios claros. Como mencionado anteriormente (C.II), autorizações especiais têm sempre *prioridade*, e não é possível se valer de uma autorização geral para o emprego de uma medida prevista em autorização especial, caso os requisitos dessa não estejam satisfeitos. Assim, no exemplo das câmeras de vigilância, a polícia não recorre à cláusula geral para o levantamento caso não haja a ameaça para um bem jurídico relevante exigido pela norma especial de autorização. Além disso, essas apenas autorizam intervenções de *baixa intensidade* ou medidas tão *atípicas* que não seria possível prevê-las em norma especial. Exemplos frequentes seriam a coleta de depoimentos do titular dos dados ou de terceiros, observações breves, acesso e cópia de documentos e a obtenção de dados pessoais disponíveis a todos (mídia escrita, rádio, televisão, internet etc.).[193]

As cláusulas gerais devem permitir, em regra, apenas medidas explícitas, ou seja, medidas realizadas de forma que seja possível perceber o levantamento dos dados.[194] Medidas ocultas, seja por meio de dissimulação ou simplesmente porque seu uso não era perceptível, somente devem ser autorizadas por cláusula geral quando forem atípicas no sentido referido. Nos casos de algumas medidas explícitas, como a coleta de depoimentos, vincula-se a licitude da medida a um requisito formal, em especial, à instrução sobre o direito de permanecer calado (ver § 18 V, traduzido abaixo).

Quanto à licitude material, as cláusulas gerais se referem à segurança pública de forma abrangente, sem especificar infrações concretas.[195] Apenas para a finalidade de enfrentamento preventivo a crimes, ou seja, nos casos de prevenção sem que haja perigo concreto, restringe-se, em algumas leis policiais alemãs, a autorização a crimes de particular relevância. A ação dos órgãos de segurança volta-se, assim, tanto para perigos concretos quanto para perigos abstratos. O grupo dos destinatários afetados é de difícil determinação porque as

193. Cf. *Kingreen/Poscher* (nr. 93), p. 198, nm. 2.
194. Cf. *Kingreen/Poscher* (nr. 93), p. 202, nm. 17.
195. Sobre esse e os seguintes requisitos de licitude mencionados, cf., por todos, *Kingreen/Poscher* (nr. 93), p. 200 ss.

medidas se voltam contra perigos abstratos em um momento prévio à ocorrência de um perigo concreto para a segurança pública, podendo afetar não somente a perturbadores, mas, em princípio, a qualquer pessoa.[196] O que se pode afirmar, em todo caso, é que o levantamento mediato, ou seja, aquele em que se recorre a um terceiro para obter informações de outra pessoa, deve estar sujeito a um controle mais estrito de proporcionalidade do que nos de medidas imediatas, em que o titular dos dados é o próprio destinatário da medida.[197]

A título de exemplo, recorremos desta vez à autorização geral para o levantamento de dados prevista na Lei Policial de Berlim[198]:

> **§ 18 Investigações, tomada de depoimentos, levantamento de dados**
>
> (1) [1]Os órgãos de segurança pública poderão realizar esclarecimentos necessários ao cumprimento de suas atribuições em uma determinada circunstância, especialmente proceder à tomada de depoimentos segundo os incisos 3 e 4. Podem, nessas situações, levantar dados pessoais sobre as pessoas enumeradas nos §§ 13, 14 e 16 e outras pessoas, se necessário para coibir um perigo ou para a realização de atribuições que lhes forem conferidas por outras normas jurídicas. [2]A polícia também poderá levantar dados, se necessário
>
> 1. para o enfrentamento preventivo de crimes de particular relevância
>
> 2. para o enfrentamento preventivo de outros crimes cometidos de forma organizada, sobretudo, no contexto de um bando, de modo profissional ou reiterado, e para os quais seja cominada pena máxima de privação de liberdade superior a três anos,
>
> 3. para a proteção de direitos privados ou
>
> 4. para auxiliar em medidas de execução [*Vollzugshilfe*].
>
> (2) [1]Investigações devem ser realizadas explicitamente. [2]Excetuados os casos permitidos nesta lei, elas somente serão

196. O BVerfG exige que se delimite a classe do afetados, sem, no entanto, explicitar como essa concretização seria possível, cf. BVerfGE 113, 348, 380.

197. *Kingreen/Poscher* (nr. 93), p. 202 s.

198. Berlim, Bremen e Hamburgo são unidades federativas autônomas na condição de Cidades-Estado. Portanto, assim como os demais Estados, Berlim dispõe de uma lei policial própria.

ocultas quando, de outro modo, a realização das atribuições restar prejudicada ou quando se possa presumir que isso corresponde ao interesse preponderante da pessoa afetada.

(3) [1]Os órgãos de segurança pública podem tomar depoimento de uma pessoa, caso haja fatos que justifiquem a suposição de que aquela pessoa pode dar informações necessárias para a realização de uma determinada tarefa policial. [2]O depoente poderá ser sobrestado pelo tempo necessário para o depoimento. [3]O depoente está obrigado a informar prenome, nome, dia e lugar do nascimento e endereço. [4]Ele somente estará obrigado a prestar outras informações se houver dever legal de fazê-lo.

(4) Serão tomados, em regra, depoimentos da própria pessoa afetada; poder-se-á tomar depoimentos de terceiros sem que o afetado tome conhecimento, se o depoimento do afetado

1. não for possível em tempo hábil,

2. exigir esforços desproporcionais e não for contrário a interesses do afetado merecedores de proteção,

3. comprometer o cumprimento da tarefa policial.

(5) [1]O depoente será informado apropriadamente sobre

1. o fundamento jurídico da tomada de depoimento

2. a existência de um dever de informar ou do caráter voluntário do depoimento.

[2]A informação é prescindível, se por meio dela a realização das atribuições policiais restar sobremaneira dificultada ou comprometida.

A formulação de normas gerais de autorização é uma tarefa extremamente delicada e sua incorporação no Brasil exige cuidado redobrado, por haver risco evidente de má compreensão e abuso das cláusulas gerais. É fundamental, para coibir esse risco, que se atente para a relação acima exposta entre autorizações especiais e gerais. Além disso, é importante que cláusulas gerais, apesar de seu caráter genérico, contenham requisitos claros e precisos, e isso com um rigor ainda maior do que no dispositivo traduzido acima, visto que as normas de direito de polícia na Alemanha têm como pano de fundo uma longa tradição de controle jurisprudencial e doutrinário. Não é esse, contudo, o caso no Brasil, sobretudo em se tratando de segurança pública.

IV. Armazenamento, utilização e alteração

Até aqui, deu-se enfoque ao levantamento de dados, cuja regulação constitui uma das tarefas centrais de normas relativas à proteção de dados na segurança pública. As demais formas de tratamento constituem um necessário complemento ao levantamento, que é realizado justamente para que se faça uso dos dados. Excetuado o compartilhamento, que será tratado posteriormente em tópico apartado, as demais formas de tratamento podem ser resumidas em *armazenamento*, *alteração* e *utilização* de dados pessoais. Armazenamento é a retenção de dados em uma base de dados, seja em arquivos físicos ou em bancos automatizados. A alteração consiste na mudança de conteúdo de um dado armazenado, por exemplo, para incluir informações novas. Utilização serve como termo geral para abarcar as demais formas de emprego de dados.

De importância fundamental para as demais formas de tratamento é a noção de vinculação à finalidade (acima III.2 b, bb).[199] Em regra, o armazenamento, a utilização e a alteração só devem ser lícitos se perseguem *o mesmo fim* para o qual os dados foram levantados[200]. Ou seja, estão vinculados à finalidade do levantamento dos dados. Essa vinculação reflete-se nos requisitos concretos de licitude material. Se o levantamento de dados está vinculado a critérios quanto aos bens jurídicos protegidos, perigos e destinatários, as demais formas de tratamento também estarão vinculadas a esses mesmos critérios de licitude material. Compreende-se, com isso, a ênfase dada até aqui a autorizações para o levantamento, pois é ele quem determina toda a cadeia posterior de tratamento dos dados.

A regra, portanto, é a da vinculação à finalidade; há, contudo, importantes exceções. A polícia deve estar autorizada às demais formas de tratamento para outros fins, sempre que estiver autorizada a levantar os dados também para esse outro fim perseguido, e este fim se refira à proteção de bens jurídicos igualmente importantes (ver abaixo E.I.2,

199. *Kingreen/Poscher* (nr. 93), p. 258.

200. A relevante preocupação com a finalidade do levantamento dos dados não é nenhuma novidade na prática brasileira. No julgamento do Resp. n. 22.337/RS, o Rel. Min. Rosado de Aguiar, já em 1995, registrava seu desassossego com a crescente utilização de bancos de dados sem controle de finalidade.

com mais detalhes). Outra importante exceção precisa ser feita no caso de órgãos que reúnem atribuições preventivas e repressivas, como a Polícia Federal (art. 144 § 1º I, II CF). Nesse contexto, para fins de persecução penal, é possível o emprego de dados que tenham sido levantados para fins de prevenção contra perigos para a segurança pública, a exemplo do uso de gravações feitas por câmeras de vigilância em um inquérito policial; e inversamente, também o uso de dados obtidos no contexto de um inquérito, para fins de prevenção. No entanto, tratando-se de utilização para fim diverso daquele perseguido na ação de levantamento, exige-se autorização em lei, e a mudança de finalidade é aceita sob a condição de que os dados pudessem ter sido levantados também para o fim perseguido com o tratamento que se lhes quer conferir (*intervenção hipotética*, ver abaixo E.I).

Especialmente quanto ao armazenamento, há duas exigências importantes que compõem a sua proporcionalidade. A primeira é de natureza formal. Atualmente dados são quase sempre armazenados em bancos de dados automatizados. A criação desses bancos de dados deve estar condicionada a uma determinação hierarquicamente superior ou ao controle por encarregados ou por órgão externo de controle.[201] Na Alemanha, exige-se em geral uma ordem (*Errichtungsanordnung*) do ministro de assuntos interiores do respectivo Estado – o cargo equivalente ao nosso secretário de segurança, dentro dos Estados da Federação – ou a participação do encarregado da proteção de dados.[202] A segunda é a previsão de prazos para o armazenamento e controle dos dados. Não havendo previsão específica de prazo para medida em questão, opta-se por prazos gerais a depender da idade do titular dos dados, se adultos, jovens ou crianças.

O texto a seguir, contendo normas de autorização para as referidas formas de tratamento, é da Lei Policial do Estado de Baden-Württemberg:

> **§ 37 Regras gerais de armazenamento, alteração e utilização de dados**
>
> (1) [1]A polícia poderá armazenar, alterar ou utilizar dados pessoais, desde que necessário para o cumprimento de suas

201. *Kingreen/Poscher* (nr. 93), p. 256 ss.
202. *Kingreen/Poscher* (nr. 93), p. 257 s.

atribuições. [2]Quando do armazenamento em bancos de dados, deverá ser possível reconhecer a qual grupo de pessoas dentre os constantes do § 20 Abs. 2 a 5 o afetado pertence.[3] Deverá ser verificável também a quem incumbe a administração dos respectivos documentos.

(2) [1]O armazenamento, a alteração e a utilização de dados pessoais são permitidos apenas para a finalidade que condicionou o levantamento dos dados. [2]O armazenamento, a alteração e a utilização para outra finalidade são permitidos somente quando a polícia também dispuser de autorização para levantar os dados para essa outra finalidade.

(3) [1]A polícia e as instituições de formação policial poderão armazenar dados pessoais para a formação policial. [2]Os dados serão anonimizados. [3]Apenas se poderá prescindir da anonimização quando esta impedir a finalidade de formação, e os interesses legítimos do afetado no sigilo dos dados não sejam evidentemente preponderantes.

(4) A polícia poderá armazenar e utilizar dados pessoais para a produção de estatísticas policiais, para a documentação com prazo determinado e para o registro de ocorrências [*Vorgangsverwaltung*].

(5) Dados pessoais armazenados exclusivamente para fins de controle de proteção de dados, de segurança de dados ou para a garantia do bom funcionamento de uma estação de tratamento de dados somente poderão ser tratados se isso for necessário para a proteção contra um perigo atual para vida, integridade corporal ou liberdade de uma pessoa ou quando houver indícios de que, sem o tratamento, o combate preventivo ou a persecução de crimes de particular relevância se tornariam impossíveis ou significativamente mais difíceis.

As leis policiais costumam prever também autorizações especiais para algumas formas particularmente gravosas de tratamento. Exemplo disso é o tratamento conferido aos dados obtidos por câmeras de vigilância, já exemplificado acima. O artigo traduzido da Lei Policial da Baviera autoriza o arquivamento e estabelece prazo para a eliminação das imagens obtidas (art. 33 II, III e VIII). Outra forma importante de tratamento, devido a sua natureza particularmente gravosa, é a

busca padronizada computadorizada (*Rasterfahndung*)[203], em que se faz o cruzamento automatizado de dados da pessoa procurada com dados presentes em bancos de dados de outros órgãos.[204]

V. Síntese parcial

O direito de proteção de dados na segurança pública tem de levar em conta as características próprias desse ramo da atividade estatal, inserindo-se, portanto, no que se deve denominar direito de segurança pública. O direito de segurança pública designa o conjunto de regras que têm por objeto a atividade do Estado voltada para o fim de proteção contra perigos para a segurança pública. Reconhecido o status constitucional dos dados pessoais, medidas de tratamento de dados na segurança pública passam a ser intervenções em direitos fundamentais realizadas para persecução daquele fim estatal. Enquanto intervenções, as medidas precisam estar autorizadas em lei que satisfaça as exigências materiais de constitucionalidade. Elementos essenciais na avaliação da justificação constitucional das medidas de tratamento de dados são fornecidos pela natureza da atividade de segurança pública, em especial pelos conceitos de bem protegido, perigo e destinatário. É fundamental, além disso, que as normas de autorização considerem separadamente as diferentes formas de tratamento de dados, pois cada uma delas constitui uma intervenção distinta. Uma vez que um direito de segurança pública é praticamente inexistente no Brasil, há aqui ainda muito a ser feito em matéria legislativa, doutrinária e jurisprudencial.

---

203. Para alguns aspectos da técnica, cf. *Wolter*, Proteção de dados no processo penal, in: Wolter, O inviolável e o intocável no direito processual penal, org. por Luís Greco, São Paulo: Marcial Pons, 2018, pp. 159-210; para mais detalhes, *Wohlers/Greco*, SK-StPO, § 98a StPO, nm. 2 s.

204. Por exemplo, cruzar os dados dos titulares de contas de energia elétrica com os indivíduos que estão registrados como residentes na cidade. Cf. ainda, por exemplo, art. 46 da Lei Policial da Baviera; § 47 da Lei Policial de Berlim; § 40 da Lei Policial de Baden-Württemberg.

ORLANDINO GLEIZER
LUCAS MONTENEGRO
EDUARDO VIANA

O DIREITO DE PROTEÇÃO DE DADOS NO PROCESSO PENAL E NA SEGURANÇA PÚBLICA

Marcial Pons

MADRI | BARCELONA | BUENOS AIRES | SÃO PAULO

E.

O COMPARTILHAMENTO DE DADOS PESSOAIS DA SEGURANÇA PÚBLICA E DA PERSECUÇÃO PENAL

O compartilhamento de dados pessoais da segurança pública e da persecução penal contém muitas nuances e, por isso, é matéria merecedora de enorme atenção. Não sendo possível, nesta oportunidade, detalhar com profundidade todas essas nuances, serão apresentadas a seguir apenas algumas linhas gerais, ainda que assim muitos detalhes tenham de ser negligenciados.

Cada nova possibilidade de acesso a dados pessoais gera novos riscos para a autodeterminação do indivíduo. Por isso, na dogmática da proteção de dados, entende-se compartilhamento como qualquer tomada de conhecimento de dados pessoais por terceiros estranhos ao âmbito de responsabilidade de execução da tarefa que fundamentou o levantamento dos mesmos dados (cf. art. 4 nr. 10 RGPD).[265] Esse âmbito de responsabilidade é compreendido tanto de uma perspectiva *organizacional* quanto *funcional*.[266] Nesse sentido, fala-se em compartilhamento quando dois órgãos trocam informações, ainda que

265. *Tinnefeld et al.* (nr. 13), p. 390.
266. *Tinnefeld et al.* (nr. 13), p. 390.

ambos exerçam atividades de mesma natureza, e também quando há trocas de informações entre diferentes departamentos dentro do mesmo órgão. Essa ideia também tem seu fundamento na separação informacional de poderes.[267] Ou seja, se dados são levantados para investigação penal por uma equipe de um departamento da Polícia Federal, qualquer acesso a esses dados por membros de outra equipe ou por membros do Ministério Público são compreendidos como compartilhamento. Nesse sentido, até mesmo a vista de autos dessa investigação por advogados ou o acesso por terceiros a dados pessoais nos *websites* dos tribunais também são entendidos como compartilhamento e, portanto, carentes de fundamento formal e materialmente (cf. 1). Com isso, quer-se chamar atenção para o fato de que, aqui, compartilhamento não deve ser entendido apenas como um ato de encaminhamento formal de informações para outro órgão, como o termo poderia sugerir à primeira vista. Na realidade, a forma do compartilhamento não importa, mesmo a troca verbal de informações é uma forma de compartilhamento de dados, por também afetar a autonomia informacional do indivíduo,[268] uma vez que o afetado não pode prever integralmente os possíveis riscos a que está submetido.[269]

I. Fundamentos

1. Licitude formal: o modelo das duas portas

Todas as considerações anteriores são desenvolvidas a partir de único fio condutor: cada uma das formas de tratamento de dados pessoais por órgãos de segurança pública e persecução penal demanda autorização em lei e tem sua legitimidade avaliada separadamente em face da natureza de cada uma dessas atividades estatais. Por conseguinte, deve haver normas de direito de segurança pública que autorizem respectivamente levantamento, armazenamento, alteração e utilização, assim como também devem fazê-lo as normas atinentes ao processo penal. Com base nesses pressupostos, o compartilhamento de

267. *Tinnefeld et al.* (nr. 13), p. 390.

268. *Tinnefeld et al.* (nr. 13), p. 390.

269. Contudo, o acesso a dados por um encarregado do controlador, que processa os dados segundo instruções do controlador, não é considerado compartilhamento. Cf. *Tinnefeld et al.* (nr. 13), p. 391.

dados revela-se especialmente problemático, pois, por sua natureza, extravasa um âmbito de atuação específico. Dados pessoais podem ser transferidos de um órgão para outro, que termina por lhes atribuir uma finalidade distinta daquela pela qual os dados foram levantados e armazenados. Isso gera algumas peculiaridades a serem consideradas na hora de conceber normas de autorização para o compartilhamento.

Uma dessas peculiaridades consiste em um problema *normativo-material* (e, possivelmente, de competência legislativa[270]) das normas de compartilhamento. Normas que autorizam o compartilhamento são normas relativas à atividade do órgão que compartilha os dados (controlador primário) ou elas dizem respeito à atividade do órgão que os recebe (controlador secundário)? Por exemplo, se a polícia compartilha imagens produzidas por câmeras de vigilância com o Ministério Público, para que sirvam como prova em um processo criminal, as normas que regulam o compartilhamento seriam normas do direito de segurança pública ou do processo penal? Esse problema tem sido bastante discutido na doutrina estrangeira, com bons argumentos para ambas as respostas possíveis.[271]

A opinião majoritária na discussão alemã enxerga no denominado *modelo das duas portas* a melhor solução para o problema. E o BVerfG estabeleceu, inclusive, a obrigatoriedade desse modelo para autorizações de compartilhamento de dados.[272] Segundo esse modelo, o compartilhamento de dados pessoais pressupõe um *duplo fundamento legal*. Seria necessário, em primeiro lugar, uma norma que autorizasse o controlador primário, aquele que primeiro levantou e armazenou os dados, a dar acesso às informações. Além disso, exige-se também do controlador secundário, ou seja, do órgão que receberá os dados,

---

270. Como exposto acima (C.I), não se pode afirmar com clareza a quem compete no Brasil legislar sobre essa matéria. Na prática, tanto há leis federais quanto estaduais dispondo sobre segurança pública. Assim, p.ex., a Lei 15.518/04 do Estado de São Paulo, que dispõe sobre a instalação de câmeras de vigilância (ver acima C.III.2.b), ao passo que medidas de identificação criminal são objeto da Lei Federal 12.037/09.

271. Para um resumo da discussão, com mais referências, ver *Weßlau/Puschke*, SK-StPO, Vor § 474 StPO, nm. 17.

272. A respeito, cf. *Gleizer*, A proteção por duas portas nas intervenções informacionais, REC vol. 19 n. 79, pp. 211-230, 2020, sobre recente decisão do BVerfG (NJW 2020, 2699) que estabelece a obrigatoriedade do modelo das duas portas também no compartilhamento de dados entre o Estado e empresas telefônicas; cf. também BVerfGE 141, 220; 130, 151.

autorização para isso. Somente se presentes ambos os fundamentos autorizadores – metaforicamente, apenas se abertas ambas as portas – seria possível o compartilhamento de dados pessoais.

Do ponto de vista dos direitos fundamentais, de fato parece ser essa uma solução consequente; até hoje, a mais consequente. Afinal, o compartilhamento de dados envolve duas intervenções distintas que demandam, cada uma, um fundamento formal próprio. A primeira intervenção, realizada pelo órgão que dá acesso aos dados, consiste na mudança da finalidade que determinou o levantamento dos dados. Atribui-se-lhes uma nova finalidade, diferente da original, o que representa uma quebra do princípio da vinculação à finalidade. Embora tal quebra seja possível, ela exige fundamento legal próprio, pois consiste em nova intervenção. Essa autorização legal tem de especificar, minimamente, a extensão dos dados compartilhados e as novas finalidades em relação às quais esse compartilhamento é aceitável. Com isso, compreende-se a razão para a existência da primeira porta. A segunda porta diz respeito ao armazenamento e utilização dos dados pelo controlador secundário. É necessário um fundamento legal próprio que especifique as condições de tratamento dos dados e assegure *standards* de proteção, em especial, deveres de controle e eliminação.

Se ambos os controladores estão submetidos a regimes jurídicos de competência de um único ente estatal (p.ex., se segurança pública e processo penal são, no caso, de competência da União), para evitar repetições desnecessárias, aceita-se, no direito alemão, que ambas as "portas" estejam previstas em único dispositivo.[273] Esse dispositivo tem, contudo, de autorizar e regular com clareza ambos os atos que compõem o compartilhamento. E, o principal, cada um dos envolvidos no compartilhamento (o que envia, e o que recebe) precisa verificar, autonomamente, se estão presentes os requisitos que autorizam tanto a faculdade de requerer quanto o dever de compartilhar os dados.

2. Licitude material: a vinculação à finalidade e o critério do levantamento hipotético

O modelo das duas portas, contudo, por si só não garante uma proteção adequada dos direitos informacionais. É necessário

273. Nesse sentido, também *Bäcker* (nr. 161), p. 482.

complementá-lo com requisitos materiais para a produção das normas de autorização em questão. Para seguir com a metáfora, tampouco se poderia falar em proteção adequada, caso as duas portas, embora existindo, fossem compostas de papel. Há, portanto, alguns requisitos materiais que as normas autorizadoras do compartilhamento têm de satisfazer.

O princípio material subjacente às normas de compartilhamento de dados consiste na *diferenciação segundo a proximidade* entre a finalidade do levantamento e a nova finalidade, perseguida com o compartilhamento. Aqui o princípio da vinculação finalística mais uma vez revela a sua importância fundamental. O tratamento autorizado dos dados está restrito à finalidade que determinou seu levantamento. Toda mudança de finalidade representa uma nova intervenção nos direitos informacionais, e essa intervenção é tanto mais gravosa, quanto díspares forem a finalidade original e a finalidade que determina o compartilhamento. Por conseguinte, as exigências a que deve estar submetido o compartilhamento serão tanto mais rigorosas quanto maior for a disparidade desses fins.

Uma concretização desse princípio fundamental é discutida na doutrina alemã sob a denominação de *intervenção hipotética* (hypothetischer Ersatzeingriff).[274] Esse critério material surge da necessidade de evitar que o compartilhamento sirva como um subterfúgio (circunvenção da lei[275]) para o acesso a dados nos casos em que um órgão não está autorizado a realizar determinadas medidas de levantamento. Chega-se, portanto, à seguinte exigência: o compartilhamento é possível se o órgão que recebe os dados contar com autorização semelhante para levantá-los. Em outros termos, somente pode ser favorecido por um compartilhamento aquele que tenha autorização legal para, ele mesmo, levantar os dados que estão sendo compartilhados.

O critério do levantamento hipotético permite não só submeter o compartilhamento à existência de uma autorização hipotética para levantar os dados, mas também que o controlador secundário esteja

---

274. Cf. BVerfGE 100, 313, 389; BVerfGE 109, 279, 377; BVerfG NJW 2016, 1781, 1801; *Weßlau/Puschke*, SK-StPO, Vor § 474 StPO, nm. 8; *Singelnstein*, MüKoStPO, § 475 StPO, nm. 27. Com críticas e oferecendo um modelo alternativo de regulação, *Bäcker* (nr. 161), p. 486 ss.

275. A respeito, cf. o texto de *Wolter* (nr. 218).

autorizado a empregar *meios* tão gravosos quanto os utilizados para levantar os dados pelo controlador primário. Portanto, o critério não implica apenas a exigência de que o órgão recebedor pudesse, de alguma forma, levantar os dados, mas também a de que ele pudesse realizar esse levantamento recorrendo a medidas com *nível de intensidade semelhante* ao daquelas efetivamente utilizadas pelo controlador primário ao obter os dados. Assim, sobretudo em se tratando de medidas ocultas de levantamento de dados (observações duradouras, agentes infiltrados, interceptações telefônicas, infiltrações *online* etc.), o compartilhamento deve estar submetido à existência de autorização para se utilizar de meios com intensidade interventiva comparável aos utilizados para levantar os dados em questão.[276]

II. Compartilhamento de dados pessoais obtidos pelos órgãos de segurança pública

Apresentados esses critérios gerais, podem-se desenvolver algumas considerações sobre o compartilhamento de dados obtidos especificamente para fins de garantia da segurança pública. Essas considerações não são mais do que a concretização dos critérios acima expostos.

Assim, a forma menos problemática de compartilhamento de dados é a que se dá entre órgãos policiais com as mesmas atribuições (p. ex. entre a Polícia Militar do Estado do Rio de Janeiro e a Polícia Militar do Estado do Ceará). Ambas têm como atribuição a garantia da segurança pública[277], havendo, portanto, semelhança dos fins perseguidos quando do levantamento de dados pessoais. Se o compartilhamento se dá, contudo, entre polícia militar e outros órgãos de segurança pública (por exemplo, corpo de bombeiros ou órgãos de polícia de trânsito), é necessário que reste satisfeito o critério acima explanado do levantamento hipotético, que o órgão recebedor dos dados em regra estivesse, ele mesmo, autorizado a levantar esses dados, valendo-se inclusive de medidas semelhantes àquelas efetivamente utilizadas para levantá-los. Não é aceitável, por exemplo, que

---

276. Assim, ver, especialmente, BVerfG NJW 2016, 1781 (1802).

277. Segundo a CF, cabem às polícias miliares a polícia ostensiva e a defesa da ordem pública (art. 144 § 5º). Para uma interpretação de ordem pública no sentido mais estrito de segurança pública, ver acima C.I.2.a.

órgãos de controle de trânsito recebam informações obtidas por meio de interceptação telefônica, pois estes órgãos não devem dispor de autorização legal para realizar medida semelhante.

A requisitos mais estritos devem estar submetidos órgãos públicos que exercem atribuições distintas, inclusive órgãos de investigação e persecução penal, como as polícias civis ou o Ministério Público. Esses requisitos podem consistir na restrição ao compartilhamento para determinados fins de especial relevo. Nas leis policiais alemãs, permite-se em regra o compartilhamento para casos de graves danos para o bem comum ou de lesão grave a direitos de uma pessoa.[278]

Segue traduzida parte do § 22 da Lei Policial de Hessen, que trata do compartilhamento intraestatal de dados. Pode-se perceber da leitura do primeiro inciso a autorização geral para o compartilhamento no caso de órgãos com as mesmas atribuições, sem que se façam maiores exigências, e, em seguida, a autorização para o compartilhamento com outros órgãos, que está submetido a pressupostos mais restritos.

§ 22 Compartilhamento intraestatal de dados e compartilhamento de dados no âmbito da União Europeia e de seus Estados-Membros

(1) [1]É permitido o compartilhamento de dados pessoais entre os órgãos de polícia, desde que os dados tenham sido obtidos no exercício de suas atribuições segundo o § 1, e o compartilhamento seja necessário para o cumprimento daquelas atribuições. [2]O mesmo vale para o compartilhamento de dados pessoais com órgãos policiais da União e de outros Estados. [3]Entre os órgãos de segurança pública ou demais órgãos a que cabe a proteção contra perigos e os órgãos policiais é permitido o compartilhamento de dados pessoais, se o acesso a esses dados se revelar necessário para o exercício das atribuições dos órgãos que os receberá.

(2) [1]Não estando presentes os pressupostos do Abs. 1, os órgãos policiais e de proteção contra perigos poderão compartilhar dados pessoais com órgãos públicos, se necessário

1. para a cumprimento de atribuições policiais ou de proteção contra perigos,

278. Cf., *Kingreen/Poscher* (nr. 93), p. 274, com referências aos respectivos dispositivos nas leis policiais.

2. para a proteção contra um perigo para o órgão que receberá os dados,

3. para a realização de uma tarefa de proteção contra perigos pelo órgão que receberá os dados, quando houver fundamentos fáticos para tal,

4. para a prevenção ou supressão de prejuízos consideráveis para o bem-comum ou

5. para a prevenção ou supressão de uma lesão grave a direitos de outra pessoa.

[2]Nos casos do S. 1 Nr. 5, a pessoa cujos dados foram compartilhados será informada, se não o opuser a finalidade do compartilhamento.

(3)... (4)... (5)... (6)...

III. Compartilhamento de dados pessoais obtidos por órgãos da persecução penal

As atividades de processo penal também envolvem muitas ações de compartilhamento de dados pessoais. Pode-se pensar em vista dos autos às partes ou a terceiros, divulgação de decisões e sentenças, transferência de dados a órgãos de segurança pública (como as polícias e as secretarias de segurança pública) e outros órgãos de persecução penal (inclusive estrangeiros), julgamentos públicos e, no Brasil, também na chocante – para não dizer tosca– prática de televisionamento de julgamentos.[279]

---

279. Embora seja essa uma prática subversiva dos direitos da personalidade dos acusados e, por vários ângulos, incompatível com um regime de proteção de dados, ela ainda encontra admiradores; cf., por todos, o recente texto de *Streck*, O Supremo deveria pôr fim às transmissões ao vivo dos julgamentos da corte? Não, Folha de São Paulo, 1.1.2021, acessível em: https://www1.folha.uol.com.br/fsp/fac-simile/2021/01/02/, que aquiesce a correções na forma (ou na "metodologia") dos julgamentos televisionados, como a duração da leitura de votos dos julgadores, mas enxerga benefícios, ainda que às custas da garantia de livre desenvolvimento da personalidade dos envolvidos, no "acompanhamento dos interessados". A afirmação desses benefícios, contudo, está baseada somente em recursos de uma retórica flagrantemente vazia, como uma citação de Bobbio sobre a diferença entre ovos e caixa de ovos, a indispensabilidade de veiculação de notícias diante de um "estado de natureza informacional das redes sociais" (que vem desacompanhado de qualquer justificação/explicação), a citação de Platão sobre linguagem como um "pharmakon", a indiscriminada afirmação de que "transparência nunca é demais" e a anedótica circunstância de que, uma vez ainda promotor, participara

Aqui também se aplicam as ideias gerais anunciadas acima. A princípio, os dados pessoais só podem ser utilizados para os propósitos que fundamentaram seu levantamento. Sua utilização para outros propósitos só é legítima caso esteja permitida por lei.[280] Além disso, o propósito que fundamentou o levantamento não pode ser incompatível com o propósito que fundamenta o compartilhamento.[281] E, como já mencionado, a incompatibilidade é concretizada pela ideia de intervenção hipotética. Portanto, em relação, por exemplo, a dados levantados por medidas de investigação invasivas, que estão submetidas a severos pressupostos, como, p.ex., a interceptação telefônica e a escuta ambiental, o compartilhamento estaria autorizado apenas caso o propósito que o fundamenta fosse suficiente para permitir, hipoteticamente, um novo levantamento dos dados.[282] Nesse sentido, é vedado o compartilhamento de dados de escuta telefônica para uso em ações cíveis ou mesmo em ações penais que julgam crimes não constantes do (já desproporcionalmente alargado) rol do art. 1º LIT.

Além do mais, a alteração de propósito, que justifica as exigências por um novo fundamento para o compartilhamento de dados, está

de júris transmitidos por rádio. É importante chamar a atenção para o fato de que, em primeiro lugar, não está explicado por que as regras brasileiras sobre julgamento são ovos enquanto as alemãs ou americanas são caixas de ovos (ou o contrário?), quando, na verdade, têm todas elas os mesmos objetos de regulação (a publicidade do processo, os direitos dos afetados, a democracia, a liberdade de imprensa etc.). Não se trata de simplesmente fazer comparações com outros países, mas de ser coerente com os direitos e garantias individuais. E alguns países, que tradicionalmente levam a sério essas ideias, terminam por servir de modelo a outros. Mas a reprodução de dados pessoais de processos judiciais em formato digital e sua disponibilização pública – atualmente, é possível encontrar até mesmo depoimentos de delatores premiados na plataforma eletrônica YouTube, de acesso universal irrestrito(!) – esvaziam totalmente a garantia de controle das informações pessoais assegurada pelo direito fundamental à autodeterminação informacional. Além disso, também é preciso atentar para o fato de que a máxima "transparência nunca é demais" é incompatível com todo o regime jurídico de proteção de dados e de reconhecimento da privacidade – devemos tornar transparentes também nossos extratos bancários e nossas caixas de e-mails? Seguindo essa lógica, julgar acusados em praça pública seria ainda mais legítimo, por garantir ainda mais transparência. É fácil antever o encontro marcado que tem o direito brasileiro, em um futuro breve, com a discussão sobre a ilegítima transmissão televisiva de audiências e julgamentos, caso queira adequar-se, de fato, às novas exigências de respeito à autodeterminação informacional.

280. Assim também, *Weßlau/Puschke*, SK-StPO, Vor § 474 StPO, nm. 8.

281. Cf. *Weßlau/Puschke*, SK-StPO, Vor § 474 StPO, nm. 8, com numerosas referências jurisprudenciais.

282. BVerfG NJW 2016, 1781 (1801).

presente não apenas quando órgãos da persecução penal dão acesso aos dados a órgãos com outras atribuições, senão também quando o mesmo órgão que levantou os dados ou que os tem em posse lhes confere outro uso, p.ex., armazenando-os para investigações futuras.[283] Sendo assim, a vinculação à finalidade do levantamento não está relacionada a tarefas abstratas dos órgãos de persecução (como investigar, acusar ou julgar fatos penais), mas ao alcance das finalidades da respectiva norma que autorizou o levantamento dos dados em questão.[284] Em tese, compreende-se que a finalidade original está vinculada aos fatos objeto da persecução penal, de modo que outros fatos significam alteração de finalidade.[285] Contudo, compreende-se não haver alteração de finalidade quando a transferência é realizada entre processos que julgam corréus sobre o mesmo fato.[286] Por fim, em razão do imperativo de separação das atividades, a forma menos problemática de compartilhamento de dados oriundos do processo penal é aquela que se dá entre diferentes órgãos, departamentos e agentes responsáveis pela persecução penal; por exemplo, a troca de dados entre diferentes órgãos de polícia investigativa ou entre diferentes juízos criminais para instrução de processos penais distintos, de modo que a troca com órgãos alheios à persecução penal, como órgãos da segurança pública, da inteligência ou de outros ramos de atividade devem ser objeto de uma inspeção ainda mais rigorosa.

Um coerente reconhecimento da autodeterminação informacional enquanto direito fundamental exige autorização e regulação legais para atos de compartilhamento de dados pessoais de cada órgão envolvido na persecução penal (polícias, promotorias e tribunais). E isso tanto em relação a dados provenientes de autos processuais quanto àqueles armazenados, em virtude da persecução, de outras formas, como em bancos de dados ou em arquivos de documentos (p. ex., arquivos do cartório que contenham mandados judiciais diversos). A regulação também deve levar em consideração os propósitos do compartilhamento: esse compartilhamento pode estar a serviço tanto de finalidades diversas da persecução penal (p. ex., estudos estatísticos ou

283. *Weßlau/Puschke*, SK-StPO Vor § 474 StPO, nm. 8.
284. *Weßlau/Puschke*, SK-StPO Vor § 474 StPO, nm. 9.
285. *Weßlau/Puschke*, SK-StPO Vor § 474 StPO, nm. 10.
286. *Weßlau/Puschke*, SK-StPO Vor § 474 StPO, nm. 10.

segurança pública – que implicam, portanto, alteração de finalidade) como do próprio processo (como vista dos autos).

O primeiro título do oitavo livro da StPO (§§ 474-482), por exemplo, abrange o acesso a informações e aos autos do processo penal. Ali, encontram-se regras sobre acesso a informações e vista dos autos por órgãos judiciais e outras instituições públicas (§ 474), por pessoas privadas e outras entidades (§ 475) e para propósitos de pesquisa (§ 476), compartilhamento *ex officio* de dados (§ 477), formas do compartilhamento (§ 478), proibições de compartilhamento e limitações de usos de dados (§ 479), decisão sobre o compartilhamento de dados (§ 480), utilização de dados pessoais para propósitos policiais (§ 481), comunicação à polícia sobre a numeração do processo e seu resultado (§ 482).

Na medida em que a contingência contemporânea fundamentadora do reconhecimento de um direito amplo como a autodeterminação informacional é o processamento eletrônico de dados por computadores, a atual existência de autos digitais e sistemas informáticos – muitas vezes *online* – de acesso a informações processuais representa um perigo especial para esse direito fundamental. Nesse sentido, requer-se redobrado cuidado na regulação desses mecanismos digitais.

Por essa razão, diante da impossibilidade de, neste espaço, apresentarmos todas as normas de autorização e regulação de compartilhamento de dados do processo penal alemão, tomado aqui como modelo de compatibilização das exigências da autodeterminação informacional, elegeremos, a título de exemplo, a norma que permite acesso aos autos a pessoas privadas.

§ 475 Informações e vista dos autos para particulares e outras entidades

(1) Sem prejuízo do disposto no § 57 da lei federal sobre proteção de dados, um advogado pode obter para um particular ou para outras entidades informações de autos que estiverem à disposição do tribunal, ou teriam que ter sido apresentadas ao tribunal no caso da propositura de uma denúncia, e o solicitante demonstrar um interesse legítimo[287] para isso. As informações serão negadas se o afetado tiver, nessa recusa, um interesse digno de proteção.

287. O conceito de legítimo interesse abre, aqui, espaço para um juízo de pon-

(2) A vista dos autos pode ser permitida atendidos os pressupostos do Abs. 1, se o fornecimento das informações requerer um esforço desproporcional ou, de acordo com a declaração da pessoa que solicita o acesso aos autos, for insuficiente para a salvaguarda do interesse legítimo.

(3) Atendidos os pressupostos do Nr. 2., as provas oficialmente armazenadas podem ser examinadas/vistas.

(4) Atendidos os pressupostos do Nr. 1, particulares e outros organismos também podem receber informações dos autos.

IV. Síntese parcial

Qualquer tomada de conhecimento de dados pessoais por terceiros estranhos ao âmbito de responsabilidade de execução da tarefa que fundamentou o levantamento dos mesmos dados é um ato de compartilhamento, na acepção técnica do termo. As tarefas de segurança pública e de persecução penal envolvem muitos atos de compartilhamento de dados pessoais. Esses atos não estão fundamentados na justificação que autorizou o levantamento dos dados. Eles também carecem, enquanto intervenções autônomas, de autorização legal específica e devem ser proporcionais. Neste capítulo, foram feitas algumas considerações sobre a forma de compatibilizar os atos de compartilhamento com essas exigências, em especial, com a necessidade de permitir ao indivíduo previsibilidade quanto ao caminho que seus dados, uma vez levantados, podem percorrer nas estruturas estatais.

deração. O conceito empregado pelo legislador alemão é extremamente abrangente e não se limita a um interesse de natureza jurídica. Há grande discussão a respeito de seu significado, mas a concretização do conceito se dá, principalmente, por meio de considerações sistemáticas e casuísticas. Para ficar com poucos exemplos, afirma-se um interesse legítimo caso os dados requeridos sejam necessários para a preparação de uma defesa criminal ou para a defesa contra pretensões cíveis relacionadas a uma causa criminal. Por outro lado, considera-se não ser legítimo, nesse caso, o interesse daquele que, simplesmente, quer saber se algum de seus dados pessoais foi mencionado em um processo específico. Nesse último caso, argumenta-se que os interesses do possível afetado estariam suficientemente protegidos pelos direitos dos titulares ou afetados (§ 57 BDSG). Cf., por todos, *Puschke/Weßlau*, SK-StPO, § 475 StPO, nm. 19 ss., com valiosas referências.