COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Convenção 108 +
Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal

---

Decisão do Comité de Ministros
(128.ª sessão do Comité de Ministros, Elsinore, 18 de maio de 2018)

Decisões

O Comité de Ministros

1. tomou conhecimento do Parecer n.º 296 (2017) da Assembleia Parlamentar sobre o projeto de Protocolo que altera a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal (STCE n.º 108);

2. adotou o Protocolo que altera a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal (STCE n.º 108), tal como consta do documento CM(2018)2-final, e, enquanto instrumento relacionado com o Protocolo, aprovou o Relatório Explicativo, tal como consta do documento CM(2018)2-addfinal;

3. sublinhou a importância de uma rápida adesão ao Protocolo pelo maior número possível de Estados Partes na Convenção n.º 108 a fim de facilitar a criação de um regime jurídico abrangente de proteção de dados ao abrigo da Convenção atualizada, bem como de assegurar a maior representação possível dos Estados no Comité da Convenção;

4. decidiu abrir o Protocolo à assinatura em 25 de junho de 2018* durante a 3.ª parte das sessões da Assembleia Parlamentar, em Estrasburgo;

5. instou os Estados-Membros e outras Partes na Convenção a tomarem, sem demora, as medidas necessárias para permitir a entrada em vigor do Protocolo no prazo de três anos a contar da sua abertura para assinatura e a estabelecerem imediatamente, mas, em todo o caso, o mais tardar um ano após a data em que o Protocolo foi aberto à assinatura, o processo de ratificação, aprovação ou aceitação do presente Protocolo, nos termos da respetiva legislação nacional;

6. sublinhou que, na sequência da entrada em vigor da Convenção alterada, em conformidade com o disposto no artigo 37.º, n.º 2 do Protocolo, apenas os Estados que tenham ratificado, aprovado ou aceite o Protocolo ficam vinculados às obrigações decorrentes da Convenção alterada;

7. instruiu os seus Delegados a analisarem, duas vezes por ano, e pela primeira vez um ano após a data de abertura à assinatura do Protocolo, os progressos globais realizados no sentido da ratificação, com base nas informações a fornecer ao Secretário-Geral por cada um dos Estados-Membros e outras Partes na Convenção, o mais tardar um mês antes dessa análise.

Convenção atualizada para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal[1]

Preâmbulo

Os Estados-Membros do Conselho da Europa e os restantes Signatários da presente Convenção,

Considerando que o objetivo do Conselho da Europa é alcançar uma maior unidade entre os seus membros, baseada, nomeadamente, no respeito do Estado de direito, bem como dos direitos humanos e das liberdades fundamentais;

Considerando que é necessário garantir a dignidade humana e a proteção dos direitos humanos e das liberdades fundamentais de todas as pessoas e, dada a diversificação, intensificação e globalização do tratamento de dados e dos fluxos de dados pessoais, a autonomia pessoal com base no direito de uma pessoa ao controlo dos seus dados pessoais e do tratamento desses dados;

Recordando que o direito à proteção dos dados pessoais deve ser considerado tendo em conta o seu papel na sociedade e que tem de ser conciliado com outros direitos humanos e liberdades fundamentais, incluindo a liberdade de expressão;

Considerando que a presente Convenção permite ter em conta, na aplicação das suas regras, o princípio do direito de acesso aos documentos oficiais;

Reconhecendo que é necessário promover, a nível mundial, os valores fundamentais do respeito pela primazia e pela proteção dos dados pessoais, comprometendo-se assim à livre circulação de informação entre as pessoas;

Reconhecendo o interesse de um reforço da cooperação internacional entre as Partes na Convenção;

Acordaram no seguinte:

[1]O Comité de Ministros decidiu adiar a abertura à assinatura para 10 de outubro de 2018.

Protocolo que altera a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento de Dados Pessoais, adotado pelo Comité de Ministros na sua 128.ª sessão, em Elsinore, em 18 de maio de 2018.

Capítulo I – Disposições gerais

Artigo 1 – Objeto e finalidade

A presente Convenção tem por finalidade proteger todas as pessoas, independentemente da sua nacionalidade ou residência, no que diz respeito ao tratamento dos seus dados pessoais, contribuindo assim para o respeito dos seus direitos humanos e liberdades fundamentais e, em especial, do direito à vida privada.

Artigo 2 – Definições

Para os efeitos da presente Convenção:

a. "dados pessoais" refere-se a qualquer informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados");

b. "tratamento de dados" refere-se a qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, tais como a recolha,armazenamento, preservação, alteração, recuperação, divulgação, disponibilização, supressão, destruição ou execução de operações lógicas e/ou aritméticas sobre esses dados;

c. Caso não seja utilizado o tratamento automatizado, "tratamento de dados" refere-se a uma operação ou a um conjunto de operações efetuadas sobre dados pessoais no âmbito de um conjunto estruturado desses dados, acessíveis ou recuperáveis de acordo com critérios específicos;

d. "responsável pelo tratamento" refere-se à pessoa singular ou coletiva, autoridade pública, serviço, agência ou qualquer outro organismo que, individualmente ou em conjunto com outros, tenha poder de decisão em matéria de tratamento de dados;

e. "destinatário" refere-se à pessoa singular ou coletiva, autoridade pública, serviço, agência ou qualquer outro organismo a quem sejam comunicados ou disponibilizados dados;

f. "subcontratante" refere-se a uma pessoa singular ou coletiva, autoridade pública, serviço, agência ou qualquer outro organismo que trate dados pessoais por conta do responsável pelo tratamento.

Artigo 3 – Âmbito

1. Cada Parte compromete-se a aplicar a presente Convenção ao tratamento de dados sob a sua jurisdição nos setores público e privado, garantindo assim o direito de todas as pessoas à proteção dos seus dados pessoais.

2. A presente Convenção não se aplica ao tratamento de dados efetuado por uma pessoa no exercício de atividades exclusivamente pessoais ou domésticas.

Capítulo II — Princípios básicos para a proteção de dados pessoais

Artigo 4 – Deveres das Partes

1. Cada Parte tomará as medidas necessárias na sua legislação para dar cumprimento às disposições da presente Convenção e garantir a sua aplicação efetiva.

2. Essas medidas serão tomadas por cada Parte e entrarão em vigor no momento da ratificação ou da adesão à presente Convenção.

3. Cada Parte compromete-se a:

a. permitir que o Comité da Convenção previsto no Capítulo VI avalie a eficácia das medidas adotadas na sua legislação para dar cumprimento às disposições da presente Convenção; e

b. contribuir ativamente para este processo de avaliação.

Artigo 5 – Legitimidade do tratamento de dados e qualidade dos dados

1. O tratamento de dados deverá ser proporcional à finalidade legítima prosseguida e refletir, em todas as fases do tratamento, um justo equilíbrio entre todos os interesses envolvidos, públicos ou privados, e os direitos e liberdades em causa.

2. Cada Parte deverá assegurar que o tratamento de dados possa ser efetuado com base no consentimento livre, específico, informado e inequívoco do titular dos dados ou em qualquer outro fundamento legítimo previsto na legislação.

3. Os dados pessoais sujeitos a tratamento deverão ser objeto de tratamento lícito.

4. Os dados pessoais sujeitos a tratamento deverão ser:

a. tratados de forma justa e transparente;

b. recolhidos para finalidades explícitas, específicas e legítimas e não tratados de forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos é, sob reserva de salvaguardas apropriadas, compatível com esses fins;

c. adequados, pertinentes e não excessivos relativamente às finalidades para as quais são tratados;

d. rigorosos e, se necessário, atualizados;

e. preservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para as quais esses dados são tratados.

Artigo 6 – Categorias especiais de dados

1. O tratamento de:

- dados genéticos;
- dados pessoais relativos a infrações, processos penais e condenações, bem como medidas de segurança conexas;
- dados biométricos que identifiquem uma pessoa de forma inequívoca;
- dados que revelem a origem racial ou étnica, as opiniões políticas, a filiação sindical, as crenças religiosas ou outras, a saúde ou a vida sexual;

só será permitido se estiverem previstas na lei garantias apropriadas que complementem as previstas na presente Convenção.

2. Essas garantias deverão prevenir os riscos que o tratamento de dados sensíveis possa representar para os interesses, os direitos e as liberdades fundamentais do titular dos dados, nomeadamente um risco de discriminação.

Artigo 7 – Segurança dos dados

1. Cada Parte deverá prever que o responsável pelo tratamento e, se for caso disso, o subcontratante, tomam as medidas de segurança apropriadas contra riscos como o acesso acidental ou não autorizado, a destruição, a perda, a utilização, a alteração ou a divulgação de dados pessoais.

2. Cada Parte deverá prever que o responsável pelo tratamento notifique, sem demora, pelo menos a autoridade de controlo competente, na aceção do artigo 15.º da presente Convenção, das violações de dados suscetíveis de interferir gravemente com os direitos e as liberdades fundamentais dos titulares dos dados.

Artigo 8 – Transparência do tratamento

1. Cada Parte deverá prever que o responsável pelo tratamento informa os titulares dos dados sobre:

a. a sua identidade e residência habitual ou estabelecimento;
b. o fundamento jurídico e as finalidades do tratamento previsto;
c. as categorias dos dados pessoais tratados;
d. os destinatários ou categorias de destinatários dos dados pessoais, se for caso disso; e
e. as modalidades de exercício dos direitos previstos no artigo 9.º, bem como qualquer informação adicional necessária para assegurar um tratamento justo e transparente dos dados pessoais.

2. O n.º 1 não se aplicará se o titular dos dados já dispuser da informação pertinente.

3. Se os dados pessoais não forem recolhidos junto dos titulares dos dados, o responsável pelo tratamento não será obrigado a fornecer essa informação se o tratamento for expressamente previsto por lei ou se tal se revelar impossível ou implicar esforços desproporcionados.

Artigo 9 – Direitos do titular dos dados

1. Todas as pessoas terão o direito de:

a. não ser objeto de uma decisão que as afete significativamente, com base exclusivamente num tratamento automatizado de dados, sem que os seus pontos de vista sejam tomados em consideração;

b. obter, mediante pedido, a intervalos razoáveis e sem demora ou despesas excessivas, a confirmação do tratamento dos dados pessoais que lhe digam respeito, a comunicação, sob forma inteligível, dos dados tratados, toda a informação disponível sobre a sua origem e o período de conservação, bem como qualquer outra informação que o responsável pelo tratamento seja obrigado a fornecer a fim de assegurar a transparência do tratamento nos termos do artigo 8.º, n.º 1;

c. obter, mediante pedido, informação sobre a fundamentação subjacente ao tratamento de dados, nos casos em que os resultados de tal tratamento lhe sejam aplicados;

d. se opor, em qualquer momento, por motivos relacionados com a sua situação, ao tratamento dos dados pessoais que lhe digam respeito, salvo se o responsável pelo tratamento demonstrar motivos legítimos para o tratamento que prevaleçam sobre os seus interesses ou direitos e liberdades fundamentais;

e. obter, mediante pedido, gratuitamente e sem demora excessiva, a retificação ou a supressão, consoante o caso, desses dados, se estes estiverem a ser ou tiverem sido tratados em violação das disposições da presente Convenção;

f. dispor de uma via de recurso nos termos do artigo 12.º, caso os direitos que lhe são conferidos pela presente Convenção tenham sido violados;

g. beneficiar, independentemente da sua nacionalidade ou da sua residência, da assistência de uma autoridade de controlo, na aceção do artigo 15.º, no exercício dos direitos que lhe são conferidos pela presente Convenção.

2. O n.º 1, alínea a), não será aplicável se a decisão for autorizada por uma lei à qual o responsável pelo tratamento esteja sujeito e que preveja igualmente medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados.

Artigo 10 – Obrigações adicionais

1. Cada Parte deverá prever que os responsáveis pelo tratamento e, se for caso disso, os subcontratantes, tomam todas as medidas apropriadas para cumprir as obrigações da presente Convenção e possam demonstrar, sob reserva da legislação interna adotada em conformidade com o artigo 11.º, n.º 3, em especial à autoridade de controlo competente prevista no artigo 15.º, que o tratamento de dados sob o seu controlo está em conformidade com as disposições da presente Convenção.

2. Cada Parte deverá prever que os responsáveis pelo tratamento e, se for caso disso, os subcontratantes, avaliarão o impacto provável do tratamento de dados previsto nos direitos e liberdades fundamentais dos titulares dos dados antes do início desse tratamento e conceberão o tratamento de dados de forma a evitar ou a minimizar o risco de interferência com esses direitos e liberdades fundamentais.

3. As Partes deverão prever que os responsáveis pelo tratamento e, se for caso disso, os subcontratantes, aplicam medidas técnicas e organizativas que tenham em conta as implicações do direito à proteção dos dados pessoais em todas as fases do tratamento de dados.

4. Cada Parte pode, tendo em conta os riscos para os interesses, os direitos e as liberdades fundamentais dos titulares dos dados, adaptar a aplicação das disposições dos n.os 1, 2 e 3 na legislação que transpõe as disposições da presente Convenção, de acordo com a natureza e o volume dos dados, a natureza, o âmbito e a finalidade do tratamento e, se for caso disso, a dimensão do responsável pelo tratamento ou do subcontratante.

Artigo 11 – Exceções e restrições

1. Não será permitida qualquer exceção ao disposto no presente capítulo, com exceção do disposto no artigo 5.º, n.º 4, no artigo 7.º, n.º 2, no artigo 8.º, n.º 1, e no artigo 9.º, quando tal exceção estiver prevista na legislação, respeitar a essência dos direitos e liberdades fundamentais e constituir uma medida necessária e proporcionada numa sociedade democrática para:

a. a proteção da segurança nacional, da defesa, da segurança pública, de interesses económicos e financeiros importantes do Estado, da imparcialidade e independência do poder judicial ou da prevenção, investigação e repressão de infrações penais e execução de sanções penais, bem como outros objetivos essenciais de interesse público geral;

b. a proteção do titular dos dados ou os direitos e liberdades fundamentais de terceiros, nomeadamente a liberdade de expressão.

2. A lei pode prever restrições ao exercício das disposições previstas nos artigos 8.º e 9.º no que diz respeito ao tratamento de dados para arquivo, fins de interesse público, fins de investigação científica ou histórica ou fins estatísticos, quando não existir um risco identificável de violação dos direitos e liberdades fundamentais dos titulares dos dados.

3. Para além das exceções previstas no n.º 1 do presente artigo, no que se refere às atividades de tratamento para fins de segurança e defesa nacionais, cada Parte pode prever, por lei e apenas quando constituir uma medida necessária e proporcionada numa sociedade democrática para cumprir esse objetivo, exceções ao artigo 4.º, n.º 3, ao artigo 14.º, n.os 5 e 6, e ao artigo 15.º, n.º 2, alíneas a), b), c) e d).

Tal não prejudica o requisito de as atividades de tratamento para fins de segurança e defesa nacionais estarem sujeitas a controlo e supervisão independentes e eficazes ao abrigo da legislação interna da respetiva Parte.

Artigo 12 – Sanções e vias de recurso

Cada Parte compromete-se a estabelecer sanções e vias de recurso judiciais e extrajudiciais apropriadas em caso de violação das disposições da presente Convenção.

Artigo 13 – Proteção alargada

Nenhuma das disposições do presente capítulo poderá ser interpretada como limitando ou afetando de qualquer outra forma a possibilidade de uma Parte conceder aos titulares dos dados em causa uma medida de proteção mais ampla do que a prevista na presente Convenção.

Capítulo III – Fluxos transfronteiras de dados pessoais

Artigo 14 – Fluxos transfronteiriços de dados pessoais

1. Uma Parte não deverá, exclusivamente para fins de proteção de dados pessoais, proibir ou sujeitar a autorização especial a transferência desses dados para um destinatário sujeito à jurisdição de outra Parte na Convenção. No entanto, essa Parte deverá fazê-lo se existir um risco real e sério de a transferência para outra Parte, ou dessa outra Parte para uma não Parte, conduzir à subtração das disposições da Convenção. Uma Parte deverá igualmente fazê-lo, se estiver vinculada por regras de proteção harmonizadas partilhadas por Estados pertencentes a uma organização regional internacional.

2. Quando o destinatário estiver sujeito à jurisdição de um Estado ou organização internacional que não seja Parte na presente Convenção, a transferência de dados pessoais só pode ser efetuada se for assegurado um nível de proteção apropriado com base nas disposições da presente Convenção.

3. Um nível de proteção apropriado pode ser assegurado por:

a. legislação desse Estado ou organização internacional, incluindo os tratados ou acordos internacionais aplicáveis; ou

b. garantias normalizadas ad hoc ou aprovadas, previstas por instrumentos juridicamente vinculativos e executórios, adotados e aplicados pelas pessoas envolvidas na transferência e no tratamento posterior.

4. Não obstante o disposto nos números anteriores, cada Parte pode prever que a transferência de dados pessoais possa ter lugar se:

a. o titular dos dados tiver dado o seu consentimento explícito, específico e livre, depois de ter sido informado dos riscos que podem surgir na ausência de salvaguardas apropriadas; ou

b. os interesses específicos do titular dos dados o exijam no caso concreto; ou

c. os interesses legítimos prevalecentes, em especial interesses públicos importantes, estejam previstos na lei e essa transferência constitui uma medida necessária e proporcionada numa sociedade democrática; ou

d. or constitui uma medida necessária e proporcionada da liberdade de expressão numa sociedade democrática.

5. Cada Parte fornecerá à autoridade de controlo competente, na aceção do artigo 15.º da presente Convenção, toda a informação pertinente relativa às transferências de dados referidas no n.º 3, alínea b), e, mediante pedido, nos n.º 4, alíneas b) e c).

6. Cada Parte prevê igualmente que a autoridade de controlo tenha o direito de solicitar que a pessoa que transfere dados demonstre a eficácia das salvaguardas ou a existência de interesses legítimos prevalecentes e que a autoridade de supervisão pode, a fim de proteger os direitos e as liberdades fundamentais dos titulares dos dados, proibir essas transferências, suspendê-las ou sujeitá-las a condições.

Capítulo IV – Autoridades de controlo

Artigo 15 – Autoridades de controlo

1 Cada Parte garantirá que uma ou mais autoridades sejam responsáveis por assegurar o cumprimento das disposições da presente Convenção.

2 Para o efeito, essas autoridades:

a. deverão ter poderes de investigação e de intervenção;
b. deverão desempenhar as funções relacionadas com as transferências de dados previstas no artigo 14.º, nomeadamente a aprovação de garantias normalizadas;
c. deverão ter poderes para emitir decisões relativas a violações das disposições da presente Convenção e podem, nomeadamente, impor sanções administrativas;

d. deverão ter o poder de intervir em processos judiciais ou de chamar a atenção das autoridades judiciais competentes para violações das disposições da presente Convenção;
e. deverão promover:
   i. a sensibilização pública para as suas funções e poderes, bem como para as suas atividades;
   ii. a sensibilização pública para direitos dos titulares dos dados e para o exercício desses direitos;
   iii. a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as responsabilidades que lhes incumbem por força da presente Convenção ;

deverá ser dada especial atenção aos direitos de proteção de dados de crianças e de outras pessoas vulneráveis.

3. As autoridades de controlo competentes deverão ser consultadas sobre propostas de quaisquer medidas legislativas ou administrativas que prevejam o tratamento de dados pessoais.
4. Cada autoridade de controlo competente tratará os pedidos e reclamações apresentados pelos titulares dos dados relativamente aos seus direitos em matéria de proteção de dados e manterá os titulares dos dados informados dos progressos realizados.
5. As autoridades de controlo agirão com grande independência e imparcialidade no desempenho das suas funções e no exercício dos seus poderes e, ao fazê-lo, não solicitarão nem aceitarão instruções.
6. Cada Parte assegurará que as autoridades de controlo dispõem dos recursos necessários ao desempenho eficaz das suas funções e ao exercício dos seus poderes.
7. Cada autoridade de controlo elaborará e publicará um relatório periódico que descreva as suas atividades.
8. Os membros e o pessoal das autoridades de controlo estarão sujeitos a obrigações de confidencialidade no que respeita à informação confidencial a que tenham acesso ou a que tenham tido acesso no desempenho das suas funções e no exercício dos seus poderes.
9. As decisões das autoridades de controlo podem ser objeto de recurso judicial.
10. As autoridades de controlo não deverão ser consideradas como competentes rlativamente ao tratamento efetuado por organismos quando atuem na sua capacidade judicial.

Capítulo V – Cooperação e assistência mútua

Artigo 16 – Nomeação das autoridades de supervisão

1. As Partes acordam em cooperar e prestar assistência mútua tendo em vista a aplicação da presente Convenção.

2. Para o efeito:

a. cada Parte nomeará uma ou mais autoridades de controlo na aceção do artigo 15.º da presente Convenção, cujo nome e endereço comunicará ao Secretário-Geral do Conselho da Europa;
b. cada Parte que tenha nomeado mais do que uma autoridade de supervisão deverá especificar a competência de cada autoridade na sua comunicação referida na alínea anterior.

Artigo 17 – Formas de cooperação

1. As autoridades de controlo cooperarão entre si na medida do necessário para o desempenho das suas funções e exercício dos seus poderes, nomeadamente:

a. prestar assistência mútua através do intercâmbio de informação pertinente e útil e da cooperação mútua, na condição de que, no que diz respeito à proteção dos dados pessoais, sejam respeitadas todas as regras e salvaguardas previstas na presente Convenção;regards the protection of personal data, all the rules and safeguards of this Convention are complied with;

b. coordenar as suas investigações ou intervenções ou conduzir ações conjuntas;

c. fornecer informação e documentação sobre a sua legislação e práticas administrativas em matéria de proteção de dados.

2. A informação referida no n.º 1 não incluirá os dados pessoais sujeitos a tratamento, a menos que sejam essenciais para a cooperação ou que o titular dos dados em causa tenha dado o seu consentimento explícito, específico, livre e informado ao seu fornecimento.

3. A fim de organizar a sua cooperação e desempenhar as funções estabelecidas nos números anteriores, as autoridades de controlo das Partes deverão criar uma rede.

Artigo 18 – Assistência aos titulares dos dados

1. Cada Parte prestará assistência a qualquer titular de dados, independentemente da sua nacionalidade ou residência, no exercício dos direitos que lhe são conferidos pelo artigo 9.º da presente Convenção.

2. Se um titular de dados residir no território de outra Parte, ser-lhe-á dada a possibilidade de apresentar o pedido por intermédio da autoridade de supervisão nomeada por essa Parte.

3. O pedido de assistência deverá conter todos os elementos necessários, relacionados *inter alia* com:

a. nome, endereço e qualquer outro elemento relevante que identifiquem a pessoa em causa e que apresenta o pedido;
b. o tratamento a que o pedido diz respeito ou o seu responsável pelo tratamento;
c. a finalidade do pedido.

Artigo 19 – Garantias

1. Uma autoridade de controlo que tenha recebido informação de outra autoridade de controlo, quer acompanhando um pedido quer em resposta ao seu próprio pedido, não utilizará essa informação para fins diferentes dos especificados no pedido.

2. Uma autoridade de controlo não pode, em caso algum, ser autorizada a apresentar um pedido em nome de um titular dos dados por sua própria iniciativa e sem o consentimento expresso do titular dos dados em causa.

Artigo 20 – Indeferimento de pedidos

Uma autoridade de controlo à qual seja dirigido um pedido nos termos do artigo 17.º da presente Convenção não pode recusar-se a dar-lhe cumprimento, a menos que:

a. o pedido não seja compatível com os seus poderes;
b. o pedido não esteja em conformidade com as disposições da presente Convenção;
c. o cumprimento do pedido seja incompatível com a soberania, a segurança nacional ou a ordem pública da Parte pela qual foi nomeada, ou com os direitos e liberdades fundamentais das pessoas sob a jurisdição dessa Parte.

Artigo 21 – Custos e procedimentos

1. A cooperação e a assistência mútua entre as Partes nos termos do artigo 17.º e a assistência prestada aos titulares de dados nos termos dos artigos 9.º e 18.º não darão origem ao pagamento de quaisquer custos ou taxas para além dos incorridos por peritos e intérpretes. Estes últimos custos ou taxas deverão ser suportados pela Parte que apresenta o pedido.

2. Não podem ser cobrados ao titular dos dados quaisquer custos ou taxas relacionados com as medidas tomadas em seu nome no território de outra Parte para além das legalmente devidas pelos residentes dessa Parte.

3. Outros pormenores relativos à cooperação e à assistência, nomeadamente no que se refere aos formulários e procedimentos e às línguas a utilizar, serão estabelecidos diretamente entre as Partes em envolvidas.

Capítulo VI – Comité da Convenção

Artigo 22 – Composição do comité

1. Após a entrada em vigor da presente Convenção, será criado um Comité da Convenção.

2. Cada Parte nomeará um representante no comité e um representante adjunto. Qualquer Estado-Membro do Conselho da Europa que não seja Parte na Convenção terá o direito de ser representado no comité por um observador.

3. O Comité da Convenção pode, por decisão tomada por maioria de dois terços dos representantes das Partes, convidar um observador a estar representado nas suas reuniões.

4. Qualquer Parte que não seja membro do Conselho da Europa contribuirá para o financiamento das atividades do Comité da Convenção, de acordo com as modalidades estabelecidas pelo Comité de Ministros com o acordo dessa Parte.

Artigo 23 – Funções do comité

O Comité da Convenção:

a. pode formular recomendações com vista a facilitar ou a melhorar a aplicação da Convenção;
b. pode apresentar propostas de alteração da presente Convenção em conformidade com o artigo 25.º;
c. formulará o seu parecer sobre qualquer proposta de alteração da presente Convenção que lhe seja apresentada nos termos do n.º 3 do artigo 25.º;
d. pode pronunciar-se sobre qualquer questão relacionada com a interpretação ou a aplicação da presente convenção;
e. preparará, antes de qualquer nova adesão à Convenção, um parecer destinado ao Comité de Ministros sobre o nível de proteção dos dados pessoais do candidato à adesão e, se necessário, recomendará as medidas a tomar para garantir o cumprimento das disposições da presente Convenção;
f. pode, a pedido de um Estado ou de uma organização internacional, avaliar se o nível de proteção dos dados pessoais que o candidato proporciona está em conformidade com as disposições da presente Convenção e, se necessário, recomendar que sejam tomadas medidas para alcançar esse cumprimento;
g. pode desenvolver ou aprovar modelos de salvaguardas normalizadas a que se refere o artigo 14.º;
h. avaliará a aplicação da presente Convenção pelas Partes e recomendará as medidas a tomar caso uma Parte não esteja em conformidade com a presente Convenção;
i. facilitará, se necessário, a resolução amigável de todas as dificuldades relacionadas com a aplicação da presente Convenção.

Artigo 24 – Procedimento

1. O Comité da Convenção será convocado pelo Secretário-Geral do Conselho da Europa. A sua primeira reunião realizar-se-á no prazo de doze meses a contar da data de entrada em vigor da presente Convenção. Posteriormente reunir-se-á, pelo menos, uma vez por ano e, em qualquer caso, sempre que um terço dos representantes das Partes solicitar a sua convocação.

2. Após cada uma das suas reuniões, o Comité da Convenção apresentará ao Comité de Ministros do Conselho da Europa um relatório sobre o seu trabalho e sobre o funcionamento da presente Convenção.

3. As regras de votação no Comité da Convenção são estabelecidas nos elementos do Regulamento Interno anexo ao Protocolo STCE n.º [223].

4. O Comité da Convenção elaborará os outros elementos do seu Regulamento Interno e estabelecerá, em particular, os procedimentos de avaliação e análise referidos no artigo 4.º, n.º 3, e no artigo 23.º, alíneas e), f) e h) com base em critérios objetivos.

Capítulo VII – Alterações

Artigo 25 – Alterações

1. As alterações à presente Convenção podem ser propostas por uma Parte, pelo Comité de Ministros do Conselho da Europa ou pelo Comité da Convenção.
2. Qualquer proposta de alteração será comunicada pelo Secretário-Geral do Conselho da Europa às Partes na presente Convenção, aos outros Estados-Membros do Conselho da Europa, à União Europeia e a qualquer Estado não membro ou organização internacional que tenha sido convidado a aderir à presente Convenção em conformidade com o disposto no artigo 27.º

3. Além disso, qualquer alteração proposta por uma Parte ou pelo Comité de Ministros será comunicada ao Comité da Convenção, que apresentará ao Comité de Ministros o seu parecer sobre essa proposta de alteração.

4. O Comité de Ministros examinará a alteração proposta e qualquer parecer apresentado pelo Comité da Convenção, podendo aprovar a alteração.

5. O texto de qualquer alteração adotada pelo Comité de Ministros em conformidade com o n.º 4 do presente artigo será comunicado às Partes para aceitação.

6. Qualquer alteração aprovada em conformidade com o n.º 4 do presente artigo entrará em vigor no trigésimo dia após todas as Partes terem informado o Secretário-Geral da sua aceitação.

7. Além disso, o Comité de Ministros pode, após consulta do Comité da Convenção, decidir por unanimidade que uma determinada alteração entrará em vigor no termo de um prazo de três anos a contar da data em que foi aberta à aceitação, a menos que uma Parte notifique o Secretário-Geral do Conselho da Europa de uma objeção à sua entrada em vigor. Se tal objeção for notificada, a alteração entrará em vigor no primeiro dia do mês seguinte à data em que a Parte na presente Convenção que notificou a objeção depositou o seu instrumento de aceitação junto do Secretário-Geral do Conselho da Europa.

Capítulo VIII – Cláusulas finais

Artigo 26 – Entrada em vigor

1. A presente Convenção deverá estar aberta à assinatura dos Estados-Membros do Conselho da Europa e da União Europeia. A presente Convenção é submetida a ratificação, aceitação ou aprovação. Os instrumentos de ratificação, aceitação ou aprovação serão depositados junto do Secretário-Geral do Conselho da Europa.

2. A presente Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data em que cinco Estados-Membros do Conselho da Europa tenham expresso o seu consentimento em ficar vinculados pela Convenção em conformidade com o número anterior.

3. Relativamente a qualquer Parte que, subsequentemente, expresse o seu consentimento em ficar vinculado pela presente Convenção, esta entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data do depósito do instrumento de ratificação, aceitação ou aprovação.

Artigo 27 – Adesão de Estados não membros ou de organizações internacionais

1. Após a entrada em vigor da presente Convenção, o Comité de Ministros do Conselho da Europa pode, mediante consulta às Partes na presente Convenção e obtido o seu acordo unânime, e à luz do parecer elaborado pelo Comité da Convenção em conformidade com o artigo 23.º, alínea e), convidar qualquer Estado não membro do Conselho da Europa ou uma organização internacional, a ela aderir por decisão tomada pela maioria prevista no artigo 20.º, alínea d), do Estatuto do Conselho da Europa e por unanimidade de voto dos representantes dos Estados Contratantes com assento no Comité de Ministros.

2. Em relação a qualquer Estado aderente à Convenção, em conformidade com o n.º 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto do Secretário-Geral do Conselho da Europa.

Artigo 28 – Cláusula territorial

1. Qualquer Estado, a União Europeia ou outra organização internacional pode, no momento da assinatura ou do depósito do seu instrumento de ratificação, aceitação, aprovação ou adesão, especificar o território ou os territórios a que a presente Convenção será aplicável.

2. Qualquer Estado, a União Europeia ou outra organização internacional pode, em qualquer momento posterior, mediante declaração dirigida ao Secretário-Geral do Conselho da Europa, tornar extensível a aplicação da presente Convenção a qualquer outro território designado na declaração. A Convenção entrará em vigor em relação a esse território no primeiro dia do mês seguinte ao termo de um período de três meses após a data de receção da declaração pelo Secretário-Geral.

3. Qualquer declaração feita nos termos dos dois números anteriores pode ser retirada, no que diz respeito a qualquer território designado na declaração, mediante notificação dirigida ao Secretário-Geral. Esse levantamento produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de seis meses após a data de receção da referida notificação pelo Secretário-Geral.

Artigo 29 – Reservas

As disposições da presente Convenção não podem ser objeto de qualquer reserva.

Artigo 30 – Denúncia

1. Qualquer Parte pode, em qualquer momento, denunciar a presente Convenção através de notificação dirigida ao Secretário-Geral do Conselho da Europa.

2. A denúncia produzirá efeitos no primeiro dia do mês seguinte ao termo de um período de seis meses após a data de receção da notificação pelo Secretário-Geral.

Artigo 31 – Notificações

O Secretário-Geral do Conselho da Europa notificará os Estados-Membros do Conselho e qualquer Parte na presente Convenção sobre:

a. qualquer assinatura;
b. o depósito de qualquer instrumento de ratificação, aceitação, aprovação ou adesão;
c. qualquer data de entrada em vigor da presente Convenção em conformidade com os artigos 26.º, 27.º e 28.º;
d. qualquer outro ato, notificação ou comunicação respeitante à presente Convenção.

Apêndice ao Protocolo: Elementos do Regulamento Interno do Comité da Convenção

1. Cada Parte tem direito de voto e disporá de um voto.

2. O quórum para as reuniões do Comité da Convenção é constituído por uma maioria de dois terços dos representantes das Partes. No caso de o Protocolo à Convenção alterado entrar em vigor em conformidade com o seu artigo 37.º, n.º 2, antes da sua entrada em vigor em relação a todos os Estados Contratantes da Convenção, o quórum para as reuniões do Comité da Convenção não deverá ser inferior a 34 Partes no Protocolo.

3. As decisões previstas no artigo 23.º são tomadas por maioria de quatro quintos. As decisões tomadas nos termos do artigo 23.º, alínea h), serão tomadas por maioria de quatro quintos, incluindo a maioria dos votos dos Estados Partes que não são membros de uma organização de integração regional que seja Parte na Convenção.

4. Se o Comité da Convenção tomar decisões nos termos do artigo 23.º, alínea h), a Parte visada pela avaliação não vota. Sempre que tal decisão diga respeito a uma matéria da competência de uma organização de integração regional, nem a organização nem os seus Estados-Membros votam.

5. As decisões relativas a questões processuais são tomadas por maioria simples.

6. As organizações de integração regional podem, em matérias da sua competência, exercer o seu direito de voto no Comité da Convenção, com um número de votos igual ao número dos seus Estados-Membros que são Partes na Convenção. Essa organização não exercerá o seu direito de voto se algum dos seus Estados-Membros exercer o seu direito de voto.

7. Em caso de votação, todas as Partes devem ser informadas do assunto e do período de votação, bem como se o voto será exercido pelas Partes individualmente ou por uma organização de integração regional em nome dos seus Estados-Membros.

8. O Comité da Convenção pode ainda alterar o seu Regulamento Interno por maioria de dois terços, exceto no que se refere às modalidades de votação, que só podem ser alteradas por unanimidade das Partes e às quais se aplica o artigo 25.º da Convenção.

Relatório explicativo

I. Introdução

1. Nos 35 anos que decorreram desde a abertura à assinatura da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, também conhecida como Convenção 108 (a seguir designada por "Convenção"), a Convenção serviu de base para a legislação internacional em matéria de proteção de dados em mais de 40 países europeus. Influenciou também a política e a legislação muito para além das fronteiras da Europa. Com os novos desafios que se colocam diariamente aos direitos humanos e às liberdades fundamentais, nomeadamente ao direito à vida privada, tornou-se claro que a Convenção deve ser modernizada, a fim de responder melhor aos desafios emergentes em matéria de privacidade decorrentes da utilização crescente das novas tecnologias da informação e da comunicação (TIC), da globalização das operações de tratamento e dos fluxos cada vez maiores de dados pessoais e, simultaneamente, reforçar o mecanismo de avaliação e de acompanhamento da Convenção.

2. Surgiu um amplo consenso sobre os seguintes aspetos do processo de modernização: o caráter geral e tecnologicamente neutro das disposições da Convenção deve ser mantido, a coerência e a compatibilidade da Convenção com outros quadros jurídicos devem ser preservadas; e o caráter aberto da Convenção, que lhe confere um potencial único enquanto norma universal, deve ser reafirmado. O texto da Convenção é de caráter geral e pode ser complementado por textos setoriais de disposições jurídicas não vinculativas mais pormenorizadas na forma, nomeadamente, de recomendações do Comité de Ministros, elaboradas com a participação dos intervenientes interessados.

3. O trabalho de modernização foi realizado no contexto mais alargado de várias reformas paralelas dos instrumentos nacionais de proteção de dados e tendo em devida conta as Diretrizes de 1980 (revistas em 2013) da Organização para a Cooperação e Desenvolvimento Económico (OCDE) para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, as Diretrizes das Nações Unidas sobre o Tratamento Informatizado dos Dados Pessoais de 1990, o quadro[2] da União Europeia (UE) desde 1995, o quadro de Proteção da Privacidade no domínio da Cooperação Económica Ásia-Pacífico (2004) e as "Normas Internacionais de 2009 relativas à Proteção da Privacidade no que diz respeito ao Tratamento de Dados Pessoais"[3]. No que diz respeito ao pacote de reforma da proteção de dados da UE, em particular, o trabalho decorreram em paralelo e foi tido o maior cuidado para assegurar a coerência entre ambos os quadros jurídicos. O quadro da UE em matéria de proteção de dados dá conteúdo e amplia os princípios da Convenção 108 e tem em conta a adesão à Convenção 108, nomeadamente no que diz respeito às transferências internacionais[4].

[2] Regulamento geral sobre a proteção de dados (UE) 2016/679 ("RGPD") e Diretiva relativa à proteção de dados das autoridades policiais e da justiça penal (UE) 2016/680 ("Diretiva Cooperação Policial").
[3] Saudado pela 31.ª Conferência Internacional dos Comissários para a Proteção de Dados e a Privacidade, realizada em Madrid, entre 4 e 6 de novembro de 2009.
[4] Ver, em especial, o considerando 105 do RGPD.

4. O Comité Consultivo instituído pelo artigo 18.º da Convenção elaborou projetos de propostas de modernização que foram adotados na sua 29.ª reunião plenária (27-30 de novembro de 2012) e apresentados ao Comité de Ministros. Posteriormente, o Comité de Ministros confiou ao Comité ad hoc para a proteção de dados (CAHDATA) a tarefa de finalizar as propostas de modernização. Este trabalho foi concluído por ocasião da 3.ª reunião da CAHDATA (1-3 de dezembro de 2014). Na sequência da finalização do quadro da UE em matéria de proteção de dados, foi criada outra CAHDATA com vista a analisar as questões pendentes. A última reunião da CAHDATA (15-16 de junho de 2016) finalizou as suas propostas e transmitiu-as ao Comité de Ministros para apreciação e adoção.

5. O texto do presente relatório explicativo destina-se a orientar e apoiar a aplicação das disposições da Convenção e fornece uma indicação sobre a forma como os redatores preveem o funcionamento da Convenção.

6. O Comité de Ministros aprovou o relatório explicativo. A este respeito, o relatório explicativo faz parte do contexto em que deve ser determinado o significado de certos termos utilizados na Convenção (nota: ref. artigo 31.º, n.os 1 e 2, da Convenção de Viena das Nações Unidas sobre o Direito dos Tratados).

O Protocolo foi adotado pelo Comité de Ministros em 18 de maio de 2018. O apêndice do Protocolo faz parte integrante do Protocolo e tem o mesmo valor jurídico que as outras disposições do Protocolo.

Este protocolo foi aberto à assinatura em Estrasburgo, em 10 de outubro de 2018.

II. Comentários

7. O presente Protocolo tem por objetivo modernizar a Convenção do Conselho da Europa para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais (STCE n.º 108) e o seu Protocolo Adicional relativo às autoridades de controlo e aos Fluxos Transfronteiriços (STCE n.º 181), bem como reforçar a sua aplicação. A partir da sua entrada em vigor, o Protocolo Adicional será considerado parte integrante da Convenção alterada.

8. Os relatórios explicativos da Convenção n.º 108 e do seu protocolo adicional continuam a ser pertinentes, na medida em que fornecem um contexto histórico e descrevem a evolução de ambos os instrumentos, podendo, para esse efeito, ser lidos em conjunto com o presente documento.

Preâmbulo

9. O preâmbulo reafirma o empenho dos Estados signatários nos direitos humanos e nas liberdades fundamentais.

10. Um dos principais objetivos da Convenção é colocar as pessoas em condições de conhecer, compreender e controlar o tratamento dos seus dados pessoais por terceiros. Por conseguinte, o preâmbulo refere expressamente o direito à autonomia pessoal e o direito de controlar os seus dados pessoais, que decorre, nomeadamente, do direito à vida privada, bem como da dignidade das pessoas. A dignidade humana exige a implementação de salvaguardas aquando do tratamento de dados pessoais, para que as pessoas não sejam tratadas como meros objetos.

11. Tendo em conta o papel do direito à proteção dos dados pessoais na sociedade, o preâmbulo sublinha o princípio segundo o qual os interesses, os direitos e as liberdades fundamentais das pessoas devem, sempre que necessário, ser conciliados entre si. Com vista a manter um equilíbrio cuidadoso entre os diferentes interesses, direitos e liberdades fundamentais, a Convenção estabelece determinadas condições e restrições no que diz respeito ao tratamento de informação e à proteção de dados pessoais. O direito à proteção de dados deve, por exemplo, ser abordado a par do direito à "liberdade de expressão", tal como estabelecido no artigo 10.º da Convenção Europeia dos Direitos do Homem (STCE n.º 5), que inclui a liberdade de opinião e de receber e transmitir informação. Além disso, a Convenção confirma que o exercício do direito à proteção de dados, que não é absoluto, não deve, nomeadamente, ser utilizado como meio geral para impedir o acesso do público aos documentos oficiais[5].

[5] Ver a Convenção do Conselho da Europa sobre o Acesso aos Documentos Oficiais (STCE n.º 205).

12. A Convenção n.º 108, através dos princípios que estabelece e dos valores que consagra, protege as pessoas, ao mesmo tempo que proporciona um quadro para os fluxos internacionais de dados. Este aspeto é importante, uma vez que os fluxos de informação a nível mundial desempenham um papel cada vez mais importante na sociedade moderna, permitindo o exercício dos direitos e liberdades fundamentais e, ao mesmo tempo, impulsionando a inovação e fomentando o progresso social e económico, enquanto tem, simultaneamente, um papel vital na garantia da segurança pública. O fluxo de dados pessoais numa sociedade da informação e da comunicação deve respeitar os direitos e liberdades fundamentais das pessoas. Além disso, o desenvolvimento e a utilização de tecnologias inovadoras devem também respeitar esses direitos. Tal contribuirá para reforçar a confiança na inovação e nas novas tecnologias e permitirá o seu desenvolvimento.

13. Uma vez que a cooperação internacional entre as autoridades de controlo é um elemento-chave para uma proteção eficaz das pessoas, a Convenção visa reforçar essa cooperação, exigindo, nomeadamente, que as Partes prestem assistência mútua e proporcionando a base jurídica apropriada para um quadro de cooperação e intercâmbio de informação para efeitos de investigação e execução.

Capítulo I – Disposições gerais

Artigo 1 – Objeto e finalidade

14. O primeiro artigo descreve o objeto e a finalidade da Convenção. Este artigo centra-se no tema da proteção: as pessoas singulares devem ser protegidas quando são tratados dados pessoais[6].

Mais recentemente, a proteção de dados foi incluída como um direito fundamental no artigo 8.º da Carta dos Direitos Fundamentais da UE, bem como nas constituições de várias Partes na Convenção.

15. As garantias estabelecidas na Convenção são alargadas a todas as pessoas, independentemente da nacionalidade ou da residência. Não é permitida qualquer discriminação entre cidadãos e nacionais de países terceiros na aplicação destas garantias[7]. As cláusulas que restringem a proteção de dados a nacionais de um Estado ou a cidadãos estrangeiros legalmente residentes seriam incompatíveis com a Convenção.

Artigo 2 – Definições

16. As definições utilizadas na presente Convenção destinam-se a assegurar a aplicação uniforme de termos que exprimem certos conceitos fundamentais na legislação interna.

Alínea a) — "dados pessoais"

17. "Pessoa identificável" refere-se a uma pessoa que possa ser, direta ou indiretamente, identificada. Uma pessoa não é considerada "identificável" se a sua identificação exigir tempo, esforço ou recursos excessivos. É o caso, por exemplo, quando a identificação do titular dos dados exige operações excessivamente complexas, longas e dispendiosas. A questão de saber o que constitui "tempo, esforço ou recursos excessivos" deve ser avaliada caso a caso. Por exemplo, poderá ser considerada a finalidade do tratamento e ter em conta critérios objetivos como o custo, os benefícios dessa identificação, o tipo de responsável pelo tratamento, a tecnologia utilizada, etc. Além disso, a evolução tecnológica e outras podem alterar o que constitui "tempo, esforço ou outros recursos excessivos".

18. A noção de "identificável" refere-se não só à identidade civil ou jurídica do indivíduo enquanto tal, mas também ao que pode permitir "individualizar" ou isolar (possibilitando assim tratar de forma diferente) uma pessoa em relação a outras. Esta "individualização" poderá ser realizada, por exemplo, referindo-se especificamente a uma pessoa, ou a um dispositivo ou combinação de dispositivos (computador, telemóvel, câmara, dispositivos de jogos, etc.) com base num número de identificação, num pseudónimo, em dados biométricos ou genéticos, em dados de localização, num endereço IP ou noutro identificador. A utilização de um pseudónimo ou de qualquer identificador digital/identidade digital não conduz à anonimização dos dados,

[6] Consultar Comissário do Conselho da Europa para os Direitos Humanos, The rule of law on the Internet and in the wider digital world, documento de análise, CommDH/IssuePaper(2014)1, 8 de dezembro de 2014, p. 48, ponto 3.3 'Everyone' *without discrimination*.

[7] Consultar Comissário do Conselho da Europa para os Direitos Humanos, The rule of law on the Internet and in the wider digital world, documento de análise, CommDH/IssuePaper(2014)1, 8 de dezembro de 2014, p. 48, ponto 3.3 'Everyone' *without discrimination.*

uma vez que o titular dos dados ainda pode ser identificável ou individualizado. A "proteção dos dados pessoais é de importância fundamental para que uma pessoa goze do seu direito ao respeito pela vida privada e familiar, tal como garantido pelo artigo 8.º" — TEDH MS v. Suécia, (Ação n.º 20837/92),1997, n.º 41.

Por conseguinte, os dados sob pseudónimo devem ser considerados dados pessoais e são abrangidos pelas disposições da Convenção. A qualidade das técnicas de pseudonimização aplicadas deverá ser devidamente tida em conta ao avaliar a adequação das salvaguardas aplicadas para mitigar os riscos para os titulares dos dados.

19. Os dados só devem ser considerados anónimos se for impossível reidentificar o titular dos dados ou se essa reidentificação exigir tempo, esforço ou recursos excessivos, tendo em conta a tecnologia disponível no momento do tratamento e a evolução tecnológica. Os dados aparentemente anónimos por não serem acompanhados de qualquer elemento de identificação óbvio podem, no entanto, em casos específicos (não exigindo tempo, esforço ou recursos excessivos), permitir a identificação de uma pessoa. É o caso, por exemplo, quando é possível ao responsável pelo tratamento ou a qualquer pessoa identificar a pessoa através da combinação de diferentes tipos de dados, tais como dados físicos, fisiológicos, genéticos, económicos ou sociais (combinação de dados sobre a idade, sexo, profissão, geolocalização, situação familiar, etc.). Se for esse o caso, os dados não podem ser considerados anónimos e estão sujeitos às disposições da Convenção.

20. Quando os dados são tornados anónimos, deverão ser utilizados meios apropriados para evitar a reidentificação dos titulares dos dados, em especial, todos os meios técnicos devem ser implementados a fim de garantir que a pessoa em causa não é, ou deixou de ser, identificável. Devem ser regularmente reavaliados à luz do ritmo acelerado do desenvolvimento tecnológico.

Alíneas b) e c) – "tratamento de dados"

21. O "tratamento de dados" começa a partir da recolha de dados pessoais e abrange todas as operações efetuadas sobre dados pessoais, parcial ou totalmente automatizadas. Caso não seja utilizado o tratamento automatizado, "tratamento de dados" refere-se a uma operação ou um conjunto de operações efetuadas em dados pessoais no âmbito de um conjunto estruturado desses dados, acessíveis ou recuperáveis de acordo com critérios específicos, que permitem ao responsável pelo tratamento ou a qualquer outra pessoa consultar, combinar ou correlacionar os dados relativos a um determinado titular de dados.

Alínea d) – "responsável pelo tratamento"

22. "Responsável pelo tratamento» refere-se à pessoa ou ao organismo com poder de decisão sobre as finalidades e os meios do tratamento, quer esse poder decorra de uma nomeação jurídica ou de circunstâncias factuais que devem ser avaliadas caso a caso. Em alguns casos, pode haver vários responsáveis pelo tratamento ou corresponsáveis pelo tratamento (responsáveis conjuntamente por um tratamento e, possivelmente, responsáveis por diferentes aspetos desse tratamento). Ao avaliar se a pessoa ou o organismo é responsável pelo tratamento, deverá ter-se especialmente em conta se essa pessoa ou organismo determina os motivos que justificam o tratamento, ou seja, as suas finalidades e os meios utilizados para o efeito.

Outros fatores relevantes para esta avaliação incluem se a pessoa ou organismo tem controlo sobre os métodos de tratamento, a escolha dos dados a tratar e quem está autorizado a aceder-lhes. As pessoas que não estejam diretamente sujeitas ao responsável pelo tratamento e que efetuem o tratamento por conta do responsável pelo tratamento, e exclusivamente de acordo com as instruções do responsável pelo tratamento, devem ser consideradas subcontratantes. O responsável pelo tratamento continua a ser responsável pelo tratamento também quando um subcontratante procede ao tratamento dos dados em seu nome.

Alínea e) – "destinatário"

23. "Destinatário" é uma pessoa singular ou uma entidade que recebe dados pessoais ou à qual são disponibilizados dados pessoais. Dependendo das circunstâncias, o destinatário pode ser um responsável pelo tratamento ou um subcontratante. Por exemplo, uma empresa pode enviar determinados dados de empregados a um departamento da administração pública que os tratará como responsável pelo tratamento para efeitos fiscais. Pode enviá-los a uma empresa que disponibilize serviços de armazenamento e que atue na qualidade de subcontratante. O destinatário pode ser uma autoridade pública ou uma entidade à qual

tenha sido conferido o direito de exercer uma função pública, mas se os dados recebidos pela autoridade ou entidade forem tratados no âmbito de um inquérito específico em conformidade com a legislação aplicável, essa autoridade ou entidade pública não deve ser considerada um beneficiário. Os pedidos de divulgação das autoridades públicas devem ser sempre apresentados por escrito, fundamentados e ocasionais e não devem dizer respeito à totalidade de um sistema de ficheiros nem conduzir à interligação do sistema de ficheiros. O tratamento de dados pessoais por essas autoridades públicas deverá estar em conformidade com as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.

Alínea f) – "subcontratante"

24. "Subcontratante" é qualquer pessoa singular ou coletiva (que não seja um empregado do responsável pelo tratamento) que trata dados por conta do responsável pelo tratamento e de acordo com as instruções do responsável pelo tratamento. As instruções dadas pelo responsável pelo tratamento estabelecem o limite do que o subcontratante está autorizado a realizar com os dados pessoais.

Artigo 3 – Âmbito

25. Nos termos do n.º 1, cada Parte deve aplicar a Convenção a todos os tratamentos, quer no setor público quer no setor privado, sob a sua jurisdição.

26. Tornar o âmbito da proteção dependente da noção de "jurisdição" das Partes é justificado pelo objetivo de melhor manter o teste do tempo e de ter em conta a evolução tecnológica contínua.

27. O n.º 2 exclui do âmbito de aplicação da Convenção os tratamentos efetuados para atividades exclusivamente pessoais ou domésticas. Esta exclusão visa evitar a imposição de obrigações não razoáveis ao tratamento de dados efetuado por pessoas singulares na sua esfera privada para atividades relacionadas com o exercício da sua vida privada.

As atividades pessoais ou domésticas são atividades que estão estreita e objetivamente ligadas à vida privada de uma pessoa e que não afetam de forma significativa a esfera pessoal de terceiros. Estas atividades não têm aspetos profissionais ou comerciais e dizem exclusivamente respeito a atividades pessoais ou domésticas, como o armazenamento de fotografias familiares ou privadas num computador, a criação de uma lista dos dados de contacto de amigos e familiares, correspondência, etc. A partilha de dados na esfera privada abrange, nomeadamente, a partilha entre uma família, um círculo restrito de amigos ou um círculo limitado em termos de dimensão e com base numa relação pessoal ou numa relação de confiança específica.

28. O facto de as atividades serem "atividades exclusivamente pessoais ou domésticas" dependerá das circunstâncias. Por exemplo, quando os dados pessoais são disponibilizados a um grande número de pessoas ou a pessoas manifestamente exteriores à esfera privada, como um sítio Web público na Internet, a isenção não será aplicável. Do mesmo modo, o funcionamento de um sistema de câmara, através do qual é armazenada uma gravação vídeo de pessoas num dispositivo de gravação contínua, como um disco rígido, instalado por uma pessoa na sua habitação para proteger a propriedade, a saúde e a vida dos proprietários da habitação, mas que cobre, ainda que parcialmente, um espaço público e, por conseguinte, é dirigido para fora do contexto privado da pessoa que trata os dados dessa forma, não pode ser considerado uma atividade puramente "pessoal ou doméstica"[8].

29. No entanto, a Convenção aplica-se ao tratamento de dados efetuado por fornecedores dos meios de tratamento de dados pessoais para essas atividades pessoais ou domésticas.

30. Embora a Convenção diga respeito ao tratamento de dados relativos a pessoas singulares, as Partes podem alargar a proibição prevista no seu direito interno aos dados relativos a pessoas coletivas, a fim de proteger os seus legítimos interesses. A Convenção aplica-se às pessoas vivas: não se destina a ser aplicável aos dados pessoais relativos a pessoas falecidas. No entanto, tal não impede as Partes de alargarem a proteção às pessoas falecidas.

[8] Ver Tribunal de Justiça da UE, František Ryneš v. Úřad, 11 de dezembro de 2014, C212/13k.

Capítulo II – Princípios básicos da proteção dos dados

Artigo 4 – Deveres das Partes

31. Como indica este artigo, a Convenção obriga as Partes a integrarem as suas disposições na sua legislação e a garantirem a sua aplicação efetiva na prática; a sua realização depende do sistema jurídico aplicável e da abordagem adotada no que respeita à incorporação de tratados internacionais.

O termo "direito das Partes" designa, de acordo com o sistema jurídico e constitucional do país em causa, todas as regras aplicáveis, quer se trate da lei ou da jurisprudência.

32. Deve satisfazer os requisitos qualitativos de acessibilidade e previsibilidade. Tal implica que a lei deve ser suficientemente clara para permitir que as pessoas e outras entidades regulamentem o seu próprio comportamento à luz das consequências jurídicas esperadas dos seus atos, e que as pessoas suscetíveis de serem afetadas por esta lei devem ter acesso à mesma. Inclui regras que impõem obrigações ou conferem direitos a pessoas (singulares ou coletivas) ou que regem a organização, os poderes e as responsabilidades das autoridades públicas ou estabelecem o procedimento. Inclui, em especial, as constituições dos Estados e todos os atos escritos das autoridades legislativas (leis no sentido formal), bem como todas as medidas regulamentares (decretos, regulamentos, despachos e instruções administrativas) baseadas nessas leis. Abrange igualmente as convenções internacionais aplicáveis no direito interno, incluindo o direito da UE. Além disso, inclui todos os outros estatutos de caráter geral, de direito público ou privado (incluindo o direito dos contratos), bem como as decisões judiciais proferidas nos países de direito comum, ou em todos os países, e jurisprudência estabelecida que interpreta uma lei escrita. Ademais, inclui qualquer ato de uma entidade profissional ao abrigo de poderes delegados pelo legislador e em conformidade com os seus poderes de regulamentação independentes.

33. Pode ser útil que essa "legislação das Partes" seja restabelecida por medidas de regulamentação voluntária no domínio da proteção de dados, tais como códigos de boas práticas ou códigos de conduta profissional. No entanto, tais medidas voluntárias não são, por si só, suficientes para assegurar o pleno cumprimento da Convenção.

34. No que diz respeito às organizações internacionais[9], em algumas situações, o direito de tais organizações internacionais pode ser aplicado diretamente a nível interno nos Estados-Membros dessas organizações, em função de cada sistema jurídico nacional.

35. A eficácia da aplicação das medidas de execução das disposições da Convenção é de importância crucial. O papel da(s) autoridade(s) de controlo, em conjunto com quaisquer vias de recurso à disposição dos titulares de dados, deve ser tido em conta na avaliação global da eficácia da aplicação das disposições da Convenção por parte de uma Parte.

36. O n.º 2 estipula ainda que as medidas de execução da Convenção serão tomadas pelas Partes interessadas e entrarão em vigor no momento da ratificação ou da adesão, ou seja, quando as Partes ficam juridicamente vinculadas pela Convenção.

Esta disposição visa permitir ao Comité da Convenção verificar se foram tomadas todas as "medidas necessárias" para garantir que as Partes na Convenção respeitam os seus compromissos e proporcionam o nível esperado de proteção de dados na sua legislação nacional. O processo e os critérios utilizados para esta verificação deverão ser claramente definidos no Regulamento Interno do Comité da Convenção.

37. No n.º 3, as Partes comprometem-se a contribuir ativamente para a avaliação do cumprimento dos seus compromissos, com vista a assegurar uma avaliação regular da aplicação dos princípios da Convenção (incluindo a sua eficácia). A apresentação de relatórios pelas Partes sobre a aplicação da respetiva legislação em matéria de proteção de dados poderá constituir um elemento possível desta contribuição ativa.

38. No exercício dos poderes que lhe são conferidos pelo n.º 3, o Comité da Convenção não avaliará se uma Parte tomou medidas eficazes, na medida em que fez uso de exceções e restrições em conformidade com as disposições da presente Convenção. Por conseguinte, nos termos do artigo 11.º, n.º 3, uma Parte não é obrigada a fornecer informação confidencial ao Comité da Convenção.

39. A avaliação do cumprimento por uma Parte será efetuada pela Comissão da Convenção com base num procedimento objetivo, justo e transparente estabelecido pela Comissão da Convenção e plenamente descrito no seu regulamento interno.

[9] As organizações internacionais são definidas como organizações de direito internacional público.

Artigo 5 – Legitimidade do tratamento de dados e qualidade dos dados

40. O n.º 1 prevê que o tratamento de dados deve ser proporcionado, ou seja, apropriado à finalidade legítima prosseguida e tendo em conta os interesses, os direitos e as liberdades da pessoa em causa ou o interesse público. Esse tratamento de dados não deve conduzir a uma interferência desproporcionada nesses interesses, direitos e liberdades. O princípio da proporcionalidade deverá ser respeitado em todas as fases do tratamento, incluindo na fase inicial, ou seja, na decisão sobre a realização ou não do tratamento.

41. O n.º 2 estabelece dois pré-requisitos essenciais alternativos para um tratamento lícito: o consentimento individual ou um fundamento legítimo previsto na lei. Os n.os 1, 2, 3 e 4 do artigo 5.º são cumulativos e devem ser respeitados para garantir a legitimidade do tratamento de dados.

42. O consentimento do titular dos dados deve ser livre, específico, informado e inequívoco. Esse consentimento deve representar a livre expressão de uma escolha intencional, dada por uma declaração (que pode ser escrita, inclusive por meios eletrónicos, ou oral) ou por uma ação positiva clara e que indique inequivocamente, neste contexto específico, a aceitação da proposta de tratamento de dados pessoais.

O simples silêncio, a inatividade ou os formulários ou caixas pré-validados não devem, por conseguinte, constituir consentimento. O consentimento deve abranger todas as atividades de tratamento realizadas para a(s) mesma(s) finalidade(s) (no caso de múltiplas finalidades, o consentimento deve ser dado para cada finalidade diferente). Podem existir casos com decisões de consentimento diferentes (por exemplo, quando a natureza dos dados é diferente, mesmo que a finalidade seja a mesma — por exemplo, dados de saúde versus dados de localização: nesses casos, o titular dos dados pode consentir no tratamento dos seus dados de localização, mas não no tratamento dos dados de saúde). O titular dos dados deve ser informado das implicações da sua decisão (o que envolve o consentimento e em que medida é dado o consentimento). Nenhuma influência ou presunção indevida (que pode ser de natureza económica ou outra), direta ou indireta, pode ser exercida sobre o titular dos dados e o consentimento não deve ser considerado livre se o titular dos dados não tiver uma escolha genuína ou livre ou não puder recusar ou retirar o consentimento sem prejuízo.

43. No contexto da investigação científica, muitas vezes não é possível identificar plenamente a finalidade do tratamento de dados pessoais para fins de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados devem ser autorizados a dar o seu consentimento a determinados domínios da investigação científica, em conformidade com normas éticas reconhecidas na investigação científica. Os titulares dos dados deverão dispor da possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida.

44. A expressão do consentimento não dispensa a necessidade de respeitar os princípios básicos em matéria de proteção de dados pessoais estabelecidos no Capítulo II da Convenção, tendo ainda de ser tida em conta a proporcionalidade do tratamento.

45. O titular dos dados tem o direito de retirar o consentimento dado a qualquer momento (que deve ser distinguido do direito distinto de se opor ao tratamento). Tal não afetará a licitude do tratamento de dados que ocorreu antes de o responsável pelo tratamento ter recebido a retirada do seu consentimento, mas não permite a continuação do tratamento dos dados, a menos que tal se justifique por outro fundamento legítimo estabelecido por lei.

46. A noção de “fundamento legítimo estabelecido por lei”, a que se refere o n.º 2, abrange, inter alia, o tratamento de dados necessário para a execução de um contrato (ou de medidas pré-contratuais a pedido do titular dos dados) no qual o titular dos dados é parte; o tratamento de dados necessário à proteção de interesses vitais do titular dos dados ou de outra pessoa; o tratamento de dados necessário para o cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito; e o tratamento de dados efetuado com base em razões de interesse público ou em interesses legítimos superiores do responsável pelo tratamento ou de terceiros.

47. O tratamento de dados efetuado por razões de interesse público deverá ser previsto por lei, inter alia em questões monetárias, orçamentais e fiscais, de saúde pública e segurança social, prevenção, investigação, deteção e repressão de infrações penais e execução de sanções penais, proteção da segurança nacional, defesa, prevenção, investigação, deteção e repressão de violações da deontologia das profissões regulamentadas, aplicação de ações cíveis e proteção da independência judicial e processos judiciais. O tratamento de dados pode servir simultaneamente um motivo de interesse público e interesses vitais do titular dos dados, como, por exemplo, no caso de dados tratados para fins humanitários, incluindo o acompanhamento de uma epidemia que ponha a vida em perigo e a sua propagação ou em situações de emergência humanitária. Esta última pode ocorrer em situações de catástrofes naturais em que o tratamento

de dados pessoais de pessoas desaparecidas pode ser necessário por um período limitado para fins relacionados com o contexto de emergência — o que deve ser avaliado caso a caso. Pode também ocorrer em situações de conflito armado ou outros atos de violência[10]. O tratamento de dados pessoais pelas autoridades oficiais com vista a alcançar os objetivos estabelecidos pelo direito constitucional, pelo direito internacional público ou de associações religiosas oficialmente reconhecidas pode também ser considerado como efetuado por razões de interesse público.

48. As condições para o tratamento legítimo são estabelecidas nos n.os 3 e 4. Os dados pessoais devem ser tratados de forma lícita, leal e transparente. Os dados pessoais devem também ter sido recolhidos para finalidades explícitas, especificadas e legítimas, e o tratamento desses dados específicos deve servir essas finalidades ou, pelo menos, não ser incompatível com as mesmas. A referência a "finalidades" especificadas indica que não é permitido tratar dados para fins indefinidos, imprecisos ou vagos. O que é considerado um objetivo legítimo depende das circunstâncias, uma vez que o objetivo é assegurar um equilíbrio entre todos os direitos, liberdades e interesses em causa em cada caso; o direito à proteção dos dados pessoais, por um lado, e a proteção de outros direitos, por outro, como, por exemplo, entre os interesses do titular dos dados e os interesses do responsável pelo tratamento ou da sociedade.

49. O conceito de utilização compatível não deve prejudicar a transparência, a segurança jurídica, a previsibilidade ou a equidade do tratamento. Os dados pessoais não devem ser tratados posteriormente de uma forma que o titular dos dados possa considerar inesperado, inapropriado ou de outra forma questionável. A fim de verificar se uma finalidade de tratamento posterior é compatível com o objetivo para o qual os dados pessoais foram inicialmente recolhidos, o responsável pelo tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deve ter em conta, inter alia, qualquer ligação entre essas finalidades e as finalidades do tratamento posterior previsto; o contexto em que os dados pessoais foram recolhidos, em particular as expectativas razoáveis dos titulares dos dados com base na sua relação com o responsável pelo tratamento quanto à sua utilização posterior, a natureza dos dados pessoais, as consequências do tratamento posterior previsto para os titulares dos dados; e a existência de salvaguardas apropriadas tanto nas operações de tratamento originais como nas posteriores previstas.

O tratamento posterior de dados pessoais, a que se refere o n.º 4, alínea b), para fins de arquivo de interesse público, de investigação científica ou histórica ou estatísticos é, a priori, considerado como compatível, desde que existam outras salvaguardas (como, por exemplo, a anonimização dos dados ou a pseudoanonimização dos dados, exceto se for necessária a preservação da forma identificável; regras de sigilo profissional; disposições que regem o acesso e a comunicação restritos de dados para os fins acima referidos, nomeadamente no que diz respeito às estatísticas e a arquivos públicos; e outras medidas técnicas e organizacionais de segurança dos dados) e que as operações excluem, em princípio, qualquer utilização da informação obtida para decisões ou medidas relativas a uma determinada pessoa.

50. "Fins estatísticos" refere-se à elaboração de inquéritos estatísticos ou à produção de resultados estatísticos agregados. As estatísticas visam analisar e caracterizar fenómenos de massa ou coletivos numa população considerada[11]. Os objetivos estatísticos podem ser prosseguidos pelo setor público ou pelo setor privado. O tratamento de dados para "fins de investigação científica" tem por objetivo fornecer aos investigadores informação que contribua para uma compreensão de fenómenos em diversos domínios científicos (epidemiologia, psicologia, economia, sociologia, linguística, ciência política, criminologia, etc.) com vista a estabelecer princípios permanentes, leis de comportamento ou padrões de causalidade que transcendam todas as pessoas a quem se aplicam[12]. "Fins de investigação histórica" incluem a investigação genealógica. "Fins de arquivo de interesse público" podem incluir também arquivos originários de entidades públicas em que também está envolvido um interesse público.

51. Os dados pessoais sujeitos a tratamento devem ser adequados, pertinentes e não excessivos. Além disso, os dados devem ser exatos e, se necessário, atualizados regularmente.

52. O requisito do n.º 4, alínea c), de que os dados sejam "não excessivos" requer, em primeiro lugar, que o tratamento de dados se limite ao necessário para a finalidade para que é tratado.

Só deve ser objeto de tratamento se, e na medida em que, os fins não puderem ser razoavelmente alcançados através do tratamento de informação que não envolva dados pessoais. Além disso, este requisito não se refere apenas à quantidade, mas também à qualidade dos dados pessoais. Os dados pessoais que sejam adequados e pertinentes, mas que impliquem uma interferência desproporcionada nos direitos e liberdades fundamentais em causa, devem ser considerados excessivos e não ser tratados.

---

[10] Nos casos em que são aplicáveis as quatro Convenções de Genebra de 1949, os respetivos Protocolos Adicionais de 1977 e os Estatutos do Movimento Internacional da Cruz Vermelha e do Crescente Vermelho.

[11] Recomendação n.º Rec. (97) 18 do Comité de Ministros aos Estados-Membros relativa à proteção dos dados pessoais recolhidos e tratados para fins estatísticos, Apêndice, ponto 1, 30 de setembro de 1997.

[12] Exposição de Motivos da Recomendação n.º Rec. (97) 18 do Comité de Ministros aos Estados-Membros relativa à proteção dos dados pessoais recolhidos e tratados para fins estatísticos, pontos 11 e 14.

53. O requisito previsto no n.º 4, alínea e), no que respeita aos prazos de preservação de dados pessoais significa que os dados devem ser suprimidos uma vez alcançada a finalidade para que foram tratados, ou que só devem ser preservados de uma forma que impeça qualquer identificação direta ou indireta do titular dos dados.

54. São permitidas exceções limitadas ao artigo 5.º, n.º 4, nas condições especificadas no artigo 11.º, n.º 1.

Artigo 6 – Categorias especiais de dados

55. O tratamento de determinados tipos de dados, ou o tratamento de determinados dados para a informação sensível que revela, pode conduzir a violações de interesses, direitos e liberdades. Pode ser o caso, por exemplo, quando existe um potencial risco de discriminação ou lesão da dignidade ou da integridade física de uma pessoa, quando a esfera mais íntima do titular dos dados, como a sua vida sexual ou orientação sexual, está a ser afetada, ou quando o tratamento de dados pode afetar a presunção de inocência. Tal só deverá ser permitido se as salvaguardas apropriadas, que complementam as outras disposições de proteção da Convenção, estiverem previstas na lei. O requisito de salvaguardas apropriadas, que complementa as disposições da Convenção, não exclui a possibilidade prevista no artigo 11.º de permitir exceções e limitações aos direitos dos titulares dos dados concedidos ao abrigo do artigo 9.º

56. A fim de evitar efeitos adversos para o titular dos dados, o tratamento de dados sensíveis para fins legítimos deve ser acompanhado de salvaguardas apropriadas (adaptadas aos riscos em causa e aos interesses, direitos e liberdades a proteger), tais como, por exemplo, individual ou cumulativamente, o consentimento explícito do titular dos dados, uma lei que abranja a finalidade e os meios do tratamento ou indique os casos excecionais em que o tratamento desses dados será permitido, uma obrigação de sigilo profissional, medidas na sequência de uma análise de risco, uma medida de segurança técnica ou organizacional específica e qualificada (encriptação de dados, por exemplo).

57. Tipos específicos de tratamento de dados podem implicar um risco particular para os titulares dos dados, independentemente do contexto do tratamento. É o caso, por exemplo, do tratamento de dados genéticos, que podem ser permitidos por indivíduos e que podem revelar informação sobre a saúde ou a filiação da pessoa, bem como a de terceiros.

Os dados genéticos são todos os dados relativos às características genéticas de uma pessoa que foram herdados ou adquiridos durante o desenvolvimento pré-natal precoce, dado que resultam da análise de uma amostra biológica da pessoa em causa: análise de cromossomas, análise de ADN ou ARN ou análise de qualquer outro elemento que permita obter informação equivalente. Verificam-se riscos semelhantes com o tratamento de dados relacionados com infrações penais (que incluem suspeitas de infrações), condenações penais (com base no direito penal e no âmbito de processos penais) e medidas de segurança conexas (que impliquem, por exemplo, a privação de liberdade) que requeira a existência de salvaguardas apropriadas aos direitos e liberdades dos titulares dos dados.

58. O tratamento de dados biométricos, ou seja, dados resultantes de um tratamento técnico específico de dados relativos às características físicas, biológicas ou fisiológicas de uma pessoa que permita a sua identificação ou autenticação única, é igualmente considerado sensível quando é utilizado precisamente para identificar de forma inequívoca a pessoa em causa.

59. O contexto do tratamento de imagens está relacionado com a determinação da natureza sensível dos dados. O tratamento de imagens não envolverá, em geral, o tratamento de dados sensíveis, uma vez que as imagens só serão abrangidas pela definição de dados biométricos quando forem tratadas através de um meio técnico específico que permita a identificação ou autenticação única de uma pessoa. Além disso, sempre que o tratamento de imagens se destine a revelar informação sobre raça, etnia ou saúde (ver ponto seguinte), esse tratamento será considerado como tratamento de dados sensíveis. Pelo contrário, as imagens tratadas por um sistema de videovigilância apenas por razões de segurança numa zona comercial não serão, geralmente, consideradas como tratamento de dados sensíveis.

60. O tratamento de dados sensíveis pode afetar negativamente os direitos dos titulares dos dados quando são tratados para obter a informação específica que revelam. Embora o tratamento de nomes de família possa, em muitas circunstâncias, não envolver qualquer risco para as pessoas (por exemplo, finalidades comuns de processamento de salários), esse tratamento pode, em alguns casos, envolver dados sensíveis, por exemplo, quando a finalidade é revelar a origem étnica ou as convicções religiosas das pessoas com base na origem linguística dos seus nomes. A informação relativa à saúde inclui informação relativa à saúde passada, presente e futura, física ou mental de uma pessoa e que pode referir-se a uma pessoa doente ou saudável. O tratamento de imagens de pessoas com óculos de lentes grossas, uma perna

partida, pele queimada ou quaisquer outras características visíveis relacionadas com a saúde de uma pessoa só pode ser considerado como processamento de dados sensíveis se o tratamento se basear em informação de saúde que possa ser extraída das imagens.

61. Sempre que os dados sensíveis tenham de ser tratados para fins estatísticos, devem ser recolhidos de forma a que o titular dos dados não seja identificável. A recolha de dados sensíveis sem dados de identificação constitui uma salvaguarda na aceção do artigo 6.º. Sempre que exista uma necessidade legítima de recolher dados sensíveis para fins estatísticos de forma identificável (por exemplo, para que possa ser efetuado um inquérito repetido ou longitudinal), devem ser implementadas salvaguardas apropriadas[13].

Artigo 7 – Segurança dos dados

62. O responsável pelo tratamento e, se for caso disso, o subcontratante, devem tomar medidas de segurança específicas, tanto de natureza técnica como organizacional, para cada tratamento, tendo em conta: as potenciais consequências negativas para as pessoas, a natureza dos dados pessoais, o volume de dados pessoais tratados, o grau de vulnerabilidade da arquitetura técnica utilizada para o tratamento, a necessidade de restringir o acesso aos dados, os requisitos relativos à preservação no longo prazo, etc.

63. As medidas de segurança devem ter em conta o estado atual dos métodos e técnicas de segurança dos dados no domínio do respetivo tratamento. O seu custo deve ser proporcional à gravidade e à probabilidade dos potenciais riscos. As medidas de segurança deverão ser avaliadas e atualizadas sempre que necessário.

64. Embora as medidas de segurança se destinem a prevenir uma série de riscos, o n.º 2 contém uma obrigação específica nos casos em que a violação de dados se tenha, contudo, verificado, o que pode interferir gravemente com os direitos e liberdades fundamentais do indivíduo. Por exemplo, a divulgação de dados abrangidos pelo sigilo profissional, ou que possam resultar em danos financeiros, de reputação ou físicos ou em humilhação pode ser considerada uma interferência “grave”.

65. Caso tenha ocorrido uma violação de dados dessa natureza, o responsável pelo tratamento é obrigado a notificar o incidente às autoridades de controlo competentes, sob reserva da exceção permitida nos termos do artigo 11.º, n.º 1. Trata-se do requisito mínimo. O responsável pelo tratamento deve também notificar as autoridades de controlo de quaisquer medidas tomadas e/ou propostas para resolver a violação e as suas potenciais consequências.

66. A notificação realizada pelo responsável pelo tratamento às autoridades de controlo não exclui outras notificações complementares. Por exemplo, o responsável pelo tratamento pode também reconhecer a necessidade de notificar os titulares dos dados, em especial quando a violação de dados for suscetível de resultar num risco significativo para os direitos e liberdades das pessoas, como a discriminação, o roubo ou fraude de identidade, perdas financeiras, danos para a reputação ou perdas da confidencialidade dos dados protegidos pelo sigilo profissional ou qualquer outra desvantagem económica ou social significativa, e fornecer-lhes informação adequada e pertinente, nomeadamente sobre os pontos de contacto e eventuais medidas que possam tomar para mitigar os efeitos adversos da violação.

Nos casos em que o responsável pelo tratamento não informe espontaneamente o titular dos dados da violação de dados, a autoridade de controlo, tendo considerado os prováveis efeitos adversos da violação, deve ser autorizada a exigir que o responsável pelo tratamento o faça. A notificação a outras autoridades competentes, como as autoridades responsáveis pela segurança dos sistemas informáticos, pode também ser desejável.

Artigo 8 – Transparência do tratamento

67. O responsável pelo tratamento é obrigado a agir de forma transparente aquando do tratamento de dados, a fim de assegurar um tratamento leal e permitir que os titulares dos dados compreendam e exerçam plenamente os seus direitos no contexto desse tratamento de dados.

68. Certas informações essenciais têm de ser obrigatoriamente fornecidas de forma proativa pelo responsável pelo tratamento aos titulares dos dados quando, direta ou indiretamente (não através do titular dos dados, mas de um terceiro), recolhem os seus dados, sob reserva da possibilidade de prever exceções, em conformidade com o artigo 11.º, n.º 1. A informação sobre o nome e o endereço do responsável pelo tratamento (ou corresponsáveis pelo tratamento), o fundamento jurídico e as finalidades do tratamento de

[13] Ver Recomendação Rec. n.º (97)18 do Comité de Ministros, op cit.

dados, as categorias dos dados tratados e os destinatários, bem como os meios para exercer os direitos, pode ser fornecida em qualquer formato apropriado (através de um sítio Web, de ferramentas tecnológicas em dispositivos individuais, etc.), desde que a informação seja apresentada de forma justa e eficaz ao titular dos dados. A informação apresentada deve ser facilmente acessível, legível, compreensível e adaptada aos titulares dos dados pertinentes (por exemplo, numa linguagem adaptada às crianças, se necessário). Deve também ser fornecida toda a informação adicional que seja necessária para assegurar um tratamento leal dos dados ou que seja útil para esses fins, tais como o período de preservação, o conhecimento da fundamentação subjacente ao tratamento dos dados, ou informação sobre transferências de dados para um destinatário noutra Parte ou numa não Parte (incluindo se essa não Parte em causa proporciona um nível apropriado de proteção dos dados ou as medidas tomadas pelo responsável pelo tratamento para garantir esse nível apropriado de proteção de dados).

69. O responsável pelo tratamento não é obrigado a fornecer essa informação se o titular dos dados já a tiver recebido, ou, no caso de uma recolha indireta de dados por terceiros, se o tratamento for expressamente previsto por lei, ou se tal se revelar impossível ou implicar esforços desproporcionados pelo facto de o titular dos dados não ser diretamente identificável ou de o responsável pelo tratamento não ter qualquer forma de contactar a pessoa em causa. Essa impossibilidade pode ser de natureza jurídica (por exemplo, no contexto de uma investigação criminal) ou de uma natureza prática (por exemplo, quando um responsável pelo tratamento trata apenas fotografias e não conhece os nomes e os contactos dos titulares dos dados).

70. O responsável pelo tratamento dos dados pode utilizar qualquer meio disponível, razoável e com um custo acessível para informar os titulares dos dados coletivamente (através de um sítio Web ou de uma notificação pública) ou individualmente. Se for impossível fazê-lo no início do tratamento, este pode ser efetuado numa fase posterior, por exemplo, quando o responsável pelo tratamento é posto em contacto com o titular dos dados por qualquer novo motivo.

Artigo 9 – Direitos do titular dos dados

71. Este artigo enumera os direitos que cada pessoa deve poder exercer no que diz respeito ao tratamento dos dados pessoais que lhe digam respeito. Cada Parte assegurará, no âmbito da sua ordem jurídica, que todos esses direitos estão disponíveis a todos os titulares de dados, em conjunto com os meios jurídicos e práticos, adequados e eficazes necessários para os exercer.

72. Estes direitos incluem o seguinte:
– o direito de todas as pessoas a não serem objeto de uma decisão puramente automatizada que as afete de forma significativa, sem que a sua opinião seja tomada em consideração (alínea a));
– o direito de todas as pessoas a solicitarem a confirmação de um tratamento dos dados que lhes digam respeito e a acederem aos dados em intervalos razoáveis e sem demora ou custos excessivos (alínea b));
– o direito de qualquer pessoa a ser informada, mediante pedido, da fundamentação subjacente ao tratamento de dados, sempre que lhes sejam aplicados os resultados desse tratamento (alínea c));
– o direito de qualquer pessoa a opor-se, por motivos relacionados com a sua situação, a um tratamento de dados pessoais que lhe digam respeito, a menos que o responsável pelo tratamento demonstre motivos legítimos que prevaleçam sobre os seus interesses ou direitos e liberdades fundamentais (alínea d));
– o direito de todas as pessoas a retificar ou suprimir dados inexatos, falsos ou ilicitamente tratados (alínea e));
– o direito de qualquer pessoa a um recurso se algum dos direitos anteriores não for respeitado (alínea f));
– o direito de qualquer pessoa a obter assistência de uma autoridade de controlo (alínea g)).

73. Estes direitos podem ter de ser reconciliados com outros direitos e interesses legítimos. Em conformidade com o artigo 11.º, só podem ser limitados se tal estiver previsto na lei e constituir uma medida necessária e proporcionada numa sociedade democrática. Por exemplo, o direito à supressão de dados pessoais pode ser limitado na medida em que o tratamento seja necessário para o cumprimento de uma obrigação legal que exija o tratamento por lei ao qual o responsável pelo tratamento esteja sujeito ou para o desempenho de funções de interesse público ou o exercício da autoridade pública de que o responsável pelo tratamento está investido.
74. Embora a Convenção não especifique de quem um titular de dados pode obter a confirmação, a pronúncia, a retificação, etc., ou a quem se opor ou expressar a sua opinião, na maioria dos casos, será o responsável pelo tratamento ou o subcontratante em seu nome. Em casos excecionais, os meios para exercer os direitos de acesso, retificação e supressão podem envolver o intermediário da autoridade de controlo. No que diz respeito aos dados de saúde, os direitos podem também ser exercidos de forma

diferente do acesso direto. Podem ser exercidos, por exemplo, com a assistência de um profissional de saúde, quando tal seja do interesse do titular dos dados, nomeadamente para o ajudar a compreender os dados ou para assegurar que o estado psicológico da pessoa em causa é devidamente tido em conta aquando da transmissão de informação — de acordo, naturalmente, com princípios deontológicos.

75. Alínea a) É essencial que uma pessoa que possa ser objeto de uma decisão puramente automatizada tenha o direito de contestar essa decisão apresentando, de forma significativa, o seu ponto de vista e os seus argumentos. Em especial, o titular dos dados deve ter a oportunidade de justificar a eventual inexatidão dos dados pessoais antes da sua utilização, a irrelevância do perfil a aplicar à sua situação específica ou outros fatores que tenham impacto no resultado da decisão automatizada. É o que acontece, nomeadamente, quando as pessoas são estigmatizadas pela aplicação de uma fundamentação algorítmica que resulta na limitação de um direito ou na recusa de uma prestação social ou quando veem a sua capacidade de crédito avaliada apenas por um software. No entanto, uma pessoa singular não pode exercer este direito se a decisão automatizada for autorizada por uma lei à qual o responsável pelo tratamento esteja sujeito e que preveja também medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados.

76. Alínea b) Os titulares dos dados devem ter o direito de ter conhecimento sobre o tratamento dos seus dados pessoais. O direito de acesso deve, em princípio, ser gratuito. No entanto, a redação da alínea b) visa permitir ao responsável pelo tratamento, em determinadas condições específicas, cobrar uma taxa razoável sempre que os pedidos sejam excessivos e abranger várias abordagens que possam ser adotadas por uma Parte em casos apropriados. Essa taxa deve ser excecional e, em qualquer caso, razoável, e não deve impedir nem dissuadir os titulares dos dados de exercerem os seus direitos. O responsável pelo tratamento ou o subcontratante pode também recusar-se a responder a pedidos manifestamente infundados ou excessivos, em especial devido ao seu caráter repetitivo. O responsável pelo tratamento deve, em todos os casos, justificar essa recusa. A fim de assegurar o exercício equitativo do direito de acesso, a comunicação “sob forma inteligível” aplica-se ao conteúdo, bem como à forma de uma comunicação digital normalizada.

77. Alínea c) Os titulares dos dados devem ter o direito de conhecer a fundamentação subjacente ao tratamento de dados, incluindo as consequências dessa fundamentação, que conduziu a quaisquer conclusões daí resultantes, em especial nos casos que envolvam a utilização de algoritmos para a tomada de decisões automatizada, incluindo a definição de perfis. Por exemplo, em caso de notação de crédito, devem ter o direito de conhecer a lógica subjacente ao tratamento dos seus dados e que conduz a uma decisão de “sim” ou “não”, e não apenas a informação sobre a própria decisão. A compreensão destes elementos contribui para o exercício efetivo de outras salvaguardas essenciais, como o direito de oposição e o direito de apresentar uma reclamação junto de uma autoridade competente.

78. Alínea d) No que diz respeito ao direito de oposição, o responsável pelo tratamento pode ter um motivo legítimo para o tratamento de dados, que prevalece sobre os interesses ou direitos e liberdades do titular dos dados. Por exemplo, a constituição, o exercício ou a defesa de uma ação judicial ou razões de segurança pública podem ser considerados motivos legítimos imperiosos que justificam a continuação do tratamento. Tal terá de ser demonstrado caso a caso e a não demonstração de tais motivos legítimos imperiosos durante a prossecução do tratamento pode ser considerada ilegal. O direito de oposição funciona de forma distinta e separada do direito de obter retificação ou supressão (alínea e)).

79. A oposição ao tratamento de dados para fins de comercialização deve conduzir à supressão ou eliminação incondicionais dos dados pessoais abrangidos pela objeção.

80. O direito de oposição pode ser limitado por força de uma lei, por exemplo, para efeitos de investigação ou repressão de infrações penais. Neste caso, o titular dos dados pode, consoante o caso, contestar a licitude do tratamento em que se baseia. Quando o tratamento de dados se fundamenta no consentimento válido dado pelo titular dos dados, o direito de retirar o consentimento pode ser exercido em vez do direito de oposição. O titular dos dados pode retirar o seu consentimento e, por conseguinte, tem de assumir as consequências eventualmente decorrentes de outros textos jurídicos, como a obrigação de indemnizar o responsável pelo tratamento. Do mesmo modo, quando o tratamento de dados se baseia num contrato, a pessoa em causa pode tomar as medidas necessárias para revogar o contrato.

81. Alínea e) A retificação ou a supressão, se tal se justificar, deve ser gratuita. No caso de retificações e supressões obtidas em conformidade com o princípio estabelecido na alínea e), essas retificações e supressões devem, sempre que possível, ser levadas ao conhecimento dos destinatários da informação original, a menos que tal se revele impossível ou implique esforços desproporcionados.

82. A alínea g) visa assegurar a proteção efetiva dos titulares dos dados, proporcionando-lhes o direito a assistência de uma autoridade de controlo no exercício dos direitos previstos na Convenção. Quando um titular de dados residir no território de outra Parte, poderá apresentar o pedido por intermédio da autoridade nomeada por essa Parte.

O pedido de assistência deve incluir informação suficiente para permitir a identificação do tratamento de dados em questão. Este direito pode ser limitado nos termos do artigo 11.º ou adaptado para salvaguardar os interesses de um processo judicial pendente.

83. São permitidas exceções limitadas ao artigo 9.º, nas condições especificadas no artigo 11.º, n.º 1.

Artigo 10 – Obrigações adicionais

84. A fim de assegurar a eficácia do direito à proteção dos dados pessoais, são impostas obrigações adicionais ao responsável pelo tratamento, bem como, se for caso disso, ao(s) subcontratante(s).

85. De acordo com o n.º 1, a obrigação do responsável pelo tratamento de assegurar uma proteção de dados adequada está associada à responsabilidade de verificar e estar em condições de demonstrar que o tratamento de dados está em conformidade com a legislação aplicável. Os princípios de proteção de dados estabelecidos na Convenção, que devem ser aplicados em todas as fases do tratamento, incluindo a fase de conceção, visam proteger os titulares dos dados e constituem também um mecanismo para reforçar a sua confiança. As medidas apropriadas que o responsável pelo tratamento e o subcontratante podem ter de tomar para assegurar o cumprimento incluem: formação dos trabalhadores, estabelecimento de procedimentos de notificação apropriados (por exemplo, para indicar quando os dados têm de ser apagados do sistema), estabelecimento de disposições contratuais específicas nos casos em que o tratamento é delegado a fim de dar execução à Convenção, bem como o estabelecimento de procedimentos internos que permitam a verificação e demonstração da conformidade.

86. Se, nos termos do artigo 11.º, n.º 3, uma Parte optar por limitar os poderes de uma autoridade de controlo na aceção do artigo 15.º com referência a atividades de tratamento para fins de segurança e defesa nacionais, o responsável pelo tratamento não tem a obrigação de demonstrar a essa autoridade de controlo o cumprimento dos requisitos em matéria de proteção de dados aplicáveis às atividades abrangidas pelo âmbito de aplicação da exceção acima referida.

87. Uma eventual medida que poderá ser tomada pelo responsável pelo tratamento para facilitar essa verificação e demonstração da conformidade será a nomeação de um "responsável pela proteção de dados" que dispõe dos meios necessários para cumprir o seu mandato. Esse responsável pela proteção de dados, cuja nomeação deve ser notificada à autoridade de controlo, pode ser interno ou externo ao responsável pelo tratamento.

88. O n.º 2 clarifica que, antes de realizar uma atividade de tratamento de dados, o responsável pelo tratamento terá de analisar o seu potencial impacto nos direitos e liberdades fundamentais dos titulares de dados. Essa análise pode ser realizada sem formalidades excessivas.

Terá igualmente de considerar o respeito do princípio da proporcionalidade com base numa visão global do tratamento previsto. Em algumas circunstâncias, sempre que um subcontratante esteja envolvido para além do responsável pelo tratamento, o subcontratante terá também de analisar os riscos. Os criadores de sistemas informáticos, incluindo profissionais de segurança ou designers, em conjunto com utilizadores e peritos jurídicos, podem ajudar a analisar os riscos.

89. O n.º 3 especifica que, a fim de melhor garantir um nível de proteção eficaz, os responsáveis pelo tratamento e, se for caso disso, os subcontratantes, devem assegurar que os requisitos em matéria de proteção de dados sejam integrados nas operações de tratamento de dados através de medidas técnicas e organizacionais (conceção da proteção de dados), tão cedo quanto possível, ou seja, idealmente na fase de arquitetura e conceção do sistema. Esta aplicação dos requisitos em matéria de proteção de dados deve ser alcançada não só no tocante à tecnologia utilizada para o tratamento dos dados, mas também ao trabalho e aos processos de gestão conexos. Devem ser criadas funcionalidades de fácil utilização que simplifiquem o cumprimento da legislação aplicável. Por exemplo, sempre que possível e pertinente, os titulares dos dados devem ter acesso seguro online aos seus próprios dados. Devem também existir instrumentos de fácil utilização que permitam aos titulares dos dados levar os seus dados a outro fornecedor da sua escolha ou conservar eles próprios os dados (ferramentas de portabilidade dos dados). Ao estabelecerem os requisitos técnicos para as definições por defeito, os responsáveis pelo tratamento e os subcontratantes devem escolher configurações normalizadas favoráveis à privacidade, de modo a que a utilização de aplicações e software não infrinja os direitos dos titulares dos dados (proteção de dados por defeito), nomeadamente para

evitar o tratamento de mais dados do que o necessário para alcançar a finalidade legítima. Por exemplo, as redes sociais devem ser configuradas por defeito, de modo a que as publicações ou imagens sejam partilhadas apenas com círculos restritos e selecionados e não com toda a Internet.

90. O n.º 4 permite que as Partes adaptem as obrigações adicionais enumeradas nos n.os 1 a 3, tendo em conta os riscos em questão para os interesses, os direitos e as liberdades fundamentais dos titulares dos dados. Essa adaptação deve ser efetuada considerando a natureza e o volume dos dados tratados, a natureza, o âmbito e as finalidades do tratamento de dados e, em determinados casos, a dimensão da entidade de tratamento. As obrigações poderão ser adaptadas, por exemplo, de modo a não envolver custos excessivos para as pequenas e médias empresas (PME) que tratem apenas dados pessoais não sensíveis recebidos de clientes no âmbito de atividades comerciais e não os reutilizem para outros fins. Certas categorias de tratamento de dados, como o tratamento que não envolve qualquer risco para os titulares dos dados, podem até estar isentas de algumas das obrigações adicionais previstas no presente artigo.

Artigo 11 – Exceções e restrições

91. Não são permitidas exceções às disposições do Capítulo II, exceto um número limitado de disposições (artigo 5.º, n.º 4, artigo 7.º, n.º 2, artigo 8.º, n.º 1, e artigo 9.º), desde que tais exceções estejam previstas na lei, respeitem a essência dos direitos e liberdades fundamentais e sejam necessárias, numa sociedade democrática, pelos motivos enumerados nas alíneas a) e b) do artigo 11.º, n.º 1. Uma medida "necessária numa sociedade democrática" deve prosseguir um objetivo legítimo e, por conseguinte, responder a uma necessidade social premente que não pode ser alcançada por meios menos intrusivos. Essa medida deve, além disso, ser proporcional ao objetivo legítimo prosseguido e as razões invocadas pelas autoridades nacionais para a justificar devem ser pertinentes e adequadas. Tal medida deve ser prescrita por uma lei acessível e previsível, que deve ser suficientemente pormenorizada.

92. Qualquer tratamento de dados pessoais deve ser lícito, leal e transparente em relação aos titulares dos dados e apenas para fins específicos. Tal não obsta, em si mesmo, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou videovigilância. Essas atividades podem ser realizadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais e execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança nacional e à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos dos titulares dos dados.

93. A necessidade de tais exceções deve ser analisada caso a caso e à luz dos objetivos essenciais de interesse público geral, tal como é especificado no n.º 1, alíneas a) e b). A alínea a) enumera alguns objetivos de interesse público geral do Estado ou da organização internacional que podem exigir exceções.

94. A noção de "segurança nacional" deve ser interpretada com base na jurisprudência pertinente do Tribunal Europeu dos Direitos do Homem[14].

95. A expressão "interesses económicos e financeiros importantes" abrange, em especial, os requisitos de cobrança de impostos e o controlo cambial. A expressão "prevenção, investigação e repressão de infrações penais e execução de sanções penais" nesta alínea inclui a repressão de infrações penais e a apl icação de sanções conexas.

A expressão "outros objetivos essenciais de interesse público geral" abrange, inter alia, a prevenção, a investigação, a deteção e a repressão de violações da deontologia das profissões regulamentadas e a aplicação de ações cíveis.

96. A alínea b) refere-se aos direitos e liberdades fundamentais dos particulares, tais como os do próprio titular dos dados (por exemplo, quando os interesses vitais do titular dos dados são ameaçados pela sua ausência) ou de terceiros, como a liberdade de expressão, incluindo a liberdade de expressão jornalística, académica, artística ou literária, o direito de receber e transmitir informação, a confidencialidade da correspondência e das comunicações, o sigilo empresarial ou comercial e outros segredos legalmente protegidos. Tal deve aplicar-se, em especial, ao tratamento de dados pessoais no domínio audiovisual e nos arquivos de notícias e bibliotecas de imprensa. Para ter em conta a importância do direito à liberdade de expressão em qualquer sociedade democrática, é necessário interpretar de forma ampla as noções associadas a esta liberdade, como por exemplo o jornalismo.

[14] A jurisprudência pertinente inclui, em especial, a proteção da segurança do Estado e da democracia constitucional contra, *inter alia*, a espionagem, o terrorismo, o apoio ao terrorismo e o separatismo. Sempre que esteja em causa a segurança nacional, devem ser previstas salvaguardas contra o poder soberano. As decisões pertinentes do Tribunal Europeu dos Direitos Humanos podem ser consultadas no sítio Web do Tribunal (hudoc.echr.coe.int).

97. O n.º 2 deixa em aberto a possibilidade de limitar as disposições previstas nos artigos 8.º e 9.º no que diz respeito a determinados tratamentos de dados efetuados para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos que não constituam um risco reconhecível de violação dos direitos e liberdades fundamentais dos titulares dos dados. Por exemplo, tal poderá ser o caso da utilização de dados para trabalhos estatísticos, tanto nos domínios público como privado, na medida em que estes dados sejam publicados de forma agregada e que existam salvaguardas apropriadas em matéria de proteção de dados (ver n.º 50).

98. As exceções adicionais permitidas ao artigo 4.º, n.º 3, ao artigo 14.º, n.os 5 e 6, e ao artigo 15.º, n.º 2, alínea a), b), c), e d), no que diz respeito às atividades de tratamento para fins de segurança e defesa nacionais, não prejudicam os requisitos aplicáveis em relação à independência e eficácia dos mecanismos de avaliação e supervisão[15].

Artigo 12 – Sanções e vias de recurso

99. Para que a Convenção garanta um nível eficaz de proteção de dados, as obrigações do responsável pelo tratamento e do subcontratante e os direitos dos titulares dos dados devem ser refletidos na legislação das Partes com as correspondentes sanções e vias de recurso.

100. Cabe a cada Parte determinar a natureza (civil, administrativa, pe. nal) destas sanções judiciais e extrajudiciais. Estas sanções devem ser efetivas, proporcionadas e dissuasoras. O mesmo se aplica às vias de recurso: os titulares dos dados devem ter a possibilidade de contestar judicialmente uma decisão ou prática, deixando a definição das modalidades de o realizar às Partes. Os titular dos dados também têm de ter acesso a vias de recurso extrajudiciais. Pode igualmente ser considerada uma compensação financeira por danos materiais e não materiais, se for caso disso, causados pelo tratamento e por ações coletivas.

Artigo 13 – Proteção alargada

101. Este artigo baseia-se numa disposição semelhante, o artigo 53.º da Convenção Europeia dos Direitos do Homem. A Convenção confirma os princípios da legislação em matéria de proteção de dados que todas as Partes estão prontas a adotar. O texto salienta que estes princípios constituem apenas uma base para as Partes criarem um sistema de proteção mais avançado. Por conseguinte, a expressão “medida de proteção mais ampla” refere-se a um nível de proteção mais elevado, não inferior ao já exigido pela Convenção.

Capítulo III – Fluxos transfronteiriços de dados pessoais[16]

Artigo 14 – Fluxos transfronteiriços de dados pessoais

102. O objetivo deste artigo é facilitar a livre circulação de informação independentemente das fronteiras (recordada no preâmbulo), assegurando simultaneamente uma proteção apropriada das pessoas no que diz respeito ao tratamento dos dados pessoais. A transferência transfronteiras de dados ocorre quando os dados pessoais são divulgados ou disponibilizados a um destinatário sujeito à jurisdição de outro Estado ou organização internacional.

103. O objetivo do regime de fluxo transfronteiriço é assegurar que os dados pessoais inicialmente tratados no âmbito da jurisdição de uma Parte (dados aí recolhidos ou armazenados, por exemplo), que se encontram subsequentemente sob a jurisdição de um Estado que não é Parte na Convenção, continuam a ser tratados com as salvaguardas apropriadas. O importante é que os dados tratados no âmbito da jurisdição de uma Parte permaneçam sempre protegidos pelos princípios pertinentes da Convenção em matéria de proteção de dados. Embora possa haver uma grande variedade de sistemas de proteção, a proteção concedida tem de ser de qualidade que garanta que os direitos humanos não são afetados pela globalização e pelos fluxos transfronteiriços de dados.

[15] Para as Partes que são Estados-Membros do Conselho da Europa, esses requisitos foram desenvolvidos pela jurisprudência do Tribunal Europeu dos Direitos Humanos ao abrigo do artigo 8.º do TEDH (ver, em especial, o TEDH, Roman Zakharov v. Rússia (Ação n.º 47143/06), 4 de dezembro de 2015, ponto 233; Szabó and Vissy v. Hungria(Ação n.º 37138/14), 12 de janeiro 2016, n.º 75 e seg.).

[16] A partir da entrada em vigor do Protocolo de Alterações, o Protocolo Adicional relativo às autoridades de controlo e aos fluxos transfronteiriços (STCE n.º 181) deve ser considerado parte integrante da Convenção, tal como alterada.

104. O artigo 14.º aplica-se apenas ao fluxo de saída de dados e não de entrada, uma vez que estes últimos estão abrangidos pelo regime de proteção de dados da Parte destinatária.

105. O n.º 1 aplica-se aos fluxos de dados entre as Partes na Convenção. Os fluxos de dados não podem ser proibidos ou sujeitos a autorização especial "exclusivamente para fins de proteção de dados pessoais". No entanto, a Convenção não restringe a liberdade de uma Parte limitar a transferência de dados pessoais para outra Parte para outros fins, incluindo, por exemplo, a segurança nacional, a defesa, a segurança pública ou outros interesses públicos importantes (incluindo a proteção de segredos de Estado).

106. A fundamentação para a disposição do n.º 1 é a de que todas as Partes, tendo subscrito a base comum das disposições em matéria de proteção de dados estabelecidas na Convenção, deverão garantir um nível de proteção considerado apropriado e, por conseguinte, permitir, em princípio, a livre circulação dos dados. No entanto, poderá haver casos excecionais em que exista um risco real e sério de que esta livre circulação de dados pessoais conduza a que as disposições da Convenção sejam contornadas. A título de exceção, esta disposição tem de ser interpretada de forma restrita e as Partes não podem invocá-la nos casos em que o risco seja hipotético ou menor. Por conseguinte, uma Parte só pode invocar a exceção num caso específico se dispuser de elementos de prova claros e fiáveis de que a transferência dos dados para outra Parte pode afetar significativamente as proteções concedidas a esses dados ao abrigo da Convenção e que a probabilidade de tal acontecer é elevada. Esse poderá ser o caso, por exemplo, quando determinadas proteções concedidas ao abrigo da Convenção deixam de ser garantidas pela outra Parte (por exemplo, porque a sua autoridade de controlo já não está em condições de exercer eficazmente as suas funções) ou quando é provável que os dados transferidos para outra Parte sejam transferidos (transferência ulterior) sem que seja assegurado um nível de proteção apropriado. Existe uma outra exceção reconhecida no direito internacional quando as Partes estão vinculadas por regras de proteção harmonizadas, partilhadas pelos Estados pertencentes a organizações (económicas) regionais que procuram um nível de integração mais aprofundado.

107. Tal aplica-se, entre outros, aos Estados-Membros da UE. No entanto, tal como indicado explicitamente no Regulamento (UE) 2016/679 (Regulamento geral sobre a proteção de dados), a adesão de um país terceiro à Convenção n.º 108 e a sua aplicação serão um fator importante na aplicação do regime de transferências internacionais da UE, em especial ao avaliar se o país terceiro oferece um nível de proteção adequado (o que, por sua vez, permite a livre circulação de dados pessoais).

108. O n.º 2 prevê a obrigação de assegurar, em princípio, que "seja assegurado um nível de proteção apropriado com base nas disposições da Convenção". Ao mesmo tempo, nos termos do n.º 4, as Partes podem transferir dados mesmo na ausência de um nível apropriado de proteção, sempre que tal se justifique, entre outros, por "interesses legítimos prevalecentes, em especial interesses públicos importantes", na medida em que estejam previstos na lei, e tais transferências constituam uma medida necessária e proporcionada numa sociedade democrática (alínea c)). Por conseguinte, os dados pessoais podem ser transferidos por motivos semelhantes aos enumerados nos n.os 1 e 3 do artigo 11.º. Em todos os casos, as Partes continuam a ser livres, ao abrigo da Convenção, de restringir as transferências de dados a não Partes, quer para efeitos de proteção de dados, quer por outros motivos.

109. O n.º 2 refere-se aos fluxos transfronteiriços de dados pessoais para um destinatário que não está sujeito à jurisdição de uma Parte. Quanto a quaisquer dados pessoais que circulem para fora das fronteiras nacionais, deve ser garantido um nível de proteção apropriado. Nos casos em que o destinatário não seja Parte na Convenção, a Convenção estabelece dois mecanismos para assegurar que o nível de proteção de dados é efetivamente apropriado; por lei ou por garantias normalizadas ad hoc ou aprovadas que sejam juridicamente vinculativas e executórias, bem como devidamente aplicadas.

110. Os n.os 2 e 3 aplicam-se a todas as formas de proteção apropriadas, previstas por lei ou por salvaguardas normalizadas. A lei deve incluir os elementos pertinentes da proteção de dados previstos na presente Convenção. O nível de proteção deve ser avaliado para cada transferência ou categoria de transferências. Devem ser examinados vários elementos da transferência, tais como: o tipo de dados, as finalidades e a duração do tratamento para o qual os dados são transferidos, o respeito do Estado de direito pelo país de destino final, as normas jurídicas gerais e setoriais aplicáveis no Estado ou na organização em causa, e as regras profissionais e de segurança que aí se aplicam.

111. O conteúdo das salvaguardas ad hoc ou normalizadas deve incluir os elementos pertinentes da proteção de dados. Ademais, as cláusulas contratuais podem ser tais, por exemplo, que o titular dos dados disponha de uma pessoa de contacto entre os funcionários da pessoa responsável pelas transferências de dados, cuja responsabilidade é assegurar o cumprimento das normas substantivas de proteção. O titular dos dados é livre de contactar esta pessoa a qualquer momento e sem custos relativamente ao tratamento ou à transferência de dados e, se for caso disso, de obter assistência no exercício dos seus direitos.

112. A avaliação da adequação do nível de proteção deve ter em conta os princípios da Convenção, o grau do seu cumprimento no Estado ou organização destinatário — na medida em que sejam relevantes para o caso específico de transferência — e a forma como o titular dos dados pode defender os seus interesses em caso de incumprimento. O caráter executório dos direitos dos titulares dos dados e a possibilidade de recurso administrativo e judicial efetivo para os titulares dos dados cujos dados pessoais estão a ser transferidos devem ser tidos em consideração no avaliação.

Do mesmo modo, a avaliação pode ser feita em relação a todo um Estado ou organização, permitindo assim todas as transferências de dados para esse destino.

113. O n.º 4 possibilita às Partes apresentar uma derrogação ao princípio da exigência de um nível de proteção apropriado e permitir a transferência para um destinatário que não assegure essa proteção. Tais derrogações só são permitidas em situações limitadas: com o consentimento ou o interesse específico do titular dos dados e/ou quando existam interesses legítimos prevalecentes previstos na lei e/ou a transferência constitua uma medida necessária e proporcional à liberdade de expressão numa sociedade democrática. Essas derrogações devem respeitar os princípios da necessidade e da proporcionalidade.

114. O n.º 5 prevê uma salvaguarda complementar: nomeadamente, que seja fornecida à autoridade de controlo competente toda a informação pertinente relativa às transferências de dados referidas no n.º 3, alínea b), e, mediante pedido, no n.º 4, alíneas b) e c). A autoridade deve ter o direito de solicitar informação relevante sobre as circunstâncias e a justificação dessas transferências. Nas condições previstas no artigo 11.º, n.º 3, são permitidas exceções ao artigo 14.º, n.º 5.

115. Nos termos do n.º 6, a autoridade de controlo deve ter o direito de solicitar que seja demonstrada a eficácia das medidas tomadas ou a existência de interesses legítimos prevalecentes, bem como de proibir, suspender ou impor condições à transferência, se tal se revelar necessário para proteger os direitos e as liberdades fundamentais dos titulares dos dados. Nas condições previstas no artigo 11.º, n.º 3, são permitidas exceções ao artigo 14.º, n.º 6.

116. Os fluxos de dados cada vez maiores e a necessidade associada de aumentar a proteção dos dados pessoais exigem igualmente um aumento da cooperação internacional em matéria de aplicação da legislação entre as autoridades de controlo competentes.

Capítulo IV – Autoridades de controlo

Artigo 15.º – Autoridades de controlo

117. Este artigo visa assegurar a proteção eficaz das pessoas singulares, exigindo que as Partes prevejam uma ou mais autoridades públicas de controlo independentes e imparciais que contribuam para a proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais. Esses poderes podem ser um único comissário ou um órgão colegial. Para que as autoridades de controlo em matéria de proteção de dados possam prever uma solução adequada, devem dispor de poderes e funções eficazes e dispor de independência genuína no exercício das suas funções.

São uma componente essencial do sistema de controlo da proteção de dados numa sociedade democrática. Na medida em que seja aplicável o artigo 11.º, n.º 3, as Partes podem prever outros mecanismos apropriados para a avaliação e supervisão independentes e eficazes das atividades de tratamento para fins de segurança e defesa nacionais.

118. O n.º 1 clarifica que poderá ser necessária mais do que uma autoridade para responder às circunstâncias específicas de diferentes sistemas jurídicos (por exemplo, Estados federais). Podem também ser criadas autoridades de controlo específicas cuja atividade se limite a um setor específico (setor das comunicações eletrónicas, setor da saúde, setor público, etc.). O mesmo se aplica ao tratamento de dados pessoais para fins jornalísticos, se for necessário reconciliar o direito à proteção dos dados pessoais com o direito à liberdade de expressão. As autoridades de controlo devem dispor das infraestruturas e dos recursos financeiros, técnicos e humanos necessários (advogados, especialistas em TI) para tomar medidas rápidas e eficazes. A adequação dos recursos deve ser objeto de avaliação permanente. O artigo 11.º, n.º 3, prevê exceções aos poderes das autoridades de controlo no que diz respeito às atividades de tratamento para fins de segurança e defesa nacionais (sempre que tais exceções sejam aplicáveis, outros números do presente artigo podem, por conseguinte, não ser aplicáveis ou pertinentes). No entanto, tal não prejudica os requisitos aplicáveis em matéria de independência e eficácia dos mecanismos de controlo e supervisão[17].

[17] Ver nota de rodapé 14.

119. As Partes dispõem de um certo poder discricionário quanto à forma de criar as autoridades que lhes permitam desempenhar a sua missão. No entanto, nos termos do n.º 2, devem dispor, sob reserva da possibilidade de prever exceções em conformidade com o artigo 11.º, n.º 3, pelo menos dos poderes de investigação e de intervenção e dos poderes para emitir decisões relativas a violações das disposições da Convenção. Estas últimas podem implicar a aplicação de sanções administrativas, incluindo coimas. Caso o sistema jurídico da Parte não preveja sanções administrativas, o n.º 2 pode ser aplicado de modo a que a sanção seja proposta pela autoridade de controlo competente e imposta pelos tribunais nacionais competentes. Em qualquer caso, as sanções impostas devem ser efetivas, proporcionadas e dissuasoras.

120. A autoridade deve dispor de poderes de investigação, sob reserva da possibilidade de prever exceções em conformidade com o artigo 11.º, n.º 3, tais como a possibilidade de solicitar ao responsável pelo tratamento e ao subcontratante informação sobre o tratamento de dados pessoais e de os obter. Por força do artigo 15.º, essas informações devem ser disponibilizadas, em especial, quando a autoridade de controlo for contactada por um titular de dados que pretenda exercer os direitos consagrados no artigo 9.º.

Este último está sujeito às exceções previstas no artigo 11.º, n.º 1.

121. O poder de intervenção da autoridade de controlo, previsto no n.º 1, pode assumir diversas formas na legislação das Partes. Por exemplo, a autoridade pode dispor de poderes para obrigar o responsável pelo tratamento a retificar, apagar ou destruir dados inexatos ou ilegalmente tratados por conta própria ou se o titular dos dados não puder exercer pessoalmente esses direitos. O poder de tomar medidas contra os responsáveis pelo tratamento que não estejam dispostos a comunicar a informação exigida num prazo razoável será também uma demonstração particularmente eficaz do poder de intervenção. Este poder pode também incluir a possibilidade de emitir pareceres antes da implementação das operações de tratamento de dados (sempre que o tratamento apresente riscos específicos para os direitos e liberdades fundamentais, a autoridade de controlo deve ser consultada pelos responsáveis pelo tratamento desde a fase mais precoce da conceção dos processos), ou de remeter os casos, se for caso disso, para as autoridades competentes relevantes.

122. Além disso, nos termos do n.º 4, todos os titulares de dados devem dispor da possibilidade de solicitar à autoridade de controlo que investigue uma reclamação referente aos seus direitos e liberdades relativamente ao tratamento de dados pessoais. Tal contribui para garantir o direito a um recurso apropriado, em conformidade com os artigos 9.º e 12.º. Devem ser disponibilizados os recursos necessários para o cumprimento desta atribuição. De acordo com os seus recursos disponíveis, as autoridades de controlo devem ter a possibilidade de definir prioridades para o tratamento dos pedidos e reclamações apresentados pelos titulares dos dados.

123. As Partes devem conferir à autoridade de controlo o poder de intervir em processos judiciais ou de levar ao conhecimento das autoridades judiciais quaisquer violações das regras em matéria de proteção de dados, sob reserva da possibilidade de prever exceções em conformidade com o artigo 11.º, n.º 3. Este poder decorre do poder de proceder a investigações, o que pode levar a autoridade a descobrir uma violação do direito à proteção de uma pessoa. As Partes podem cumprir a obrigação de conferir esse poder à autoridade, permitindo-lhe tomar decisões.

124. Sempre que uma decisão administrativa produza efeitos jurídicos, qualquer pessoa afetada tem direito a um recurso judicial efetivo, em conformidade com o direito interno aplicável.

125. O ponto 2, alínea e), aborda o papel de sensibilização das autoridades de controlo. Neste contexto, afigura-se particularmente importante que a autoridade de controlo assegure proativamente a visibilidade das suas atividades, funções e poderes. Para o efeito, a autoridade de supervisão deve informar o público através de relatórios periódicos (ver o n.º 131). Pode também publicar pareceres, formular recomendações gerais sobre a correta aplicação das regras de proteção dos dados ou utilizar quaisquer outros meios de comunicação. Além disso, deve fornecer informação às pessoas e aos responsáveis pelo tratamento e subcontratantes sobre os seus direitos e obrigações em matéria de proteção de dados.
Ao mesmo tempo que sensibilizam para as questões da proteção de dados, as autoridades têm de estar atentas quando abordam especificamente as crianças e as categorias vulneráveis de pessoas através de formas e linguagens adaptadas.

126. Tal como previsto no n.º 3, as autoridades de controlo têm, nos termos da legislação nacional aplicável, o direito de emitir pareceres sobre quaisquer medidas legislativas ou administrativas que prevejam o tratamento de dados pessoais. Apenas as medidas gerais devem ser abrangidas por este poder consultivo e não as medidas individuais.

127. Para além desta consulta prevista no n.º 3, a autoridade pode também ser convidada a emitir o seu parecer quando estiverem em preparação outras medidas relativas ao tratamento de dados pessoais, como, por exemplo, códigos de conduta ou normas técnicas.

128. O artigo 15.º não impede a atribuição de outros poderes às autoridades de controlo.

129. O n.º 5 clarifica que as autoridades de controlo só podem salvaguardar efetivamente os direitos e as liberdades individuais se exercerem as suas funções com total independência. Vários elementos contribuem para salvaguardar a independência da autoridade de controlo no exercício das suas funções, incluindo a composição da autoridade, o método de nomeação dos seus membros, o período de exercício e as condições de cessação das suas funções, a possibilidade de participarem nas reuniões pertinentes sem restrições indevidas, a possibilidade de consultar peritos técnicos ou outros ou de realizar consultas externas, a disponibilidade de recursos suficientes para a autoridade, a possibilidade de contratar o seu próprio pessoal, ou a adoção de decisões sem serem objeto de interferência externa, direta ou indireta.

130. A proibição de solicitar ou aceitar instruções abrange o exercício das funções de autoridade de supervisão. Tal não impede as autoridades de controlo de procurarem aconselhamento especializado sempre que tal seja considerado necessário, desde que as autoridades de controlo exerçam a sua própria apreciação independente.

131. A transparência do trabalho e das atividades das autoridades de controlo é exigida nos termos do n.º 7 através, por exemplo, da publicação de relatórios anuais de atividade que incluam, inter alia, informação relacionada com as suas medidas de execução.

132. Não obstante esta independência, as decisões das autoridades de controlo devem poder ser objeto de recurso judicial, em conformidade com o princípio do Estado de direito previsto no n.º 9.

133. Além disso, embora as autoridades de controlo devam dispor de capacidade jurídica para atuar judicialmente e solicitar a execução, a intervenção (ou a ausência) de uma autoridade de controlo não deve impedir uma pessoa afetada de intentar uma ação judicial (ver n.º 124).

134. O artigo 15.º, n.º 10, estabelece que as autoridades de controlo não deverão ser consideradas como competentes no que diz respeito ao tratamento efetuado por organismos independentes quando atuem na sua capacidade judicial. Essa isenção dos poderes de supervisão deve ser rigorosamente limitada a atividades judiciais genuínas, em conformidade com o direito interno.

Capítulo V – Cooperação e assistência mútua

Artigo 16 – Nomeação das autoridades de controlo

135. O Capítulo V (artigos 16.º a 21.º) constitui um conjunto de disposições em matéria de cooperação e assistência mútua entre as Partes, através das suas várias autoridades, para a aplicação da legislação em matéria de proteção de dados nos termos da Convenção. Estas disposições são obrigatórias, exceto nos casos referidos no artigo 20.º. Nos termos do artigo 16.º, as Partes nomeiam uma ou mais autoridades e comunicam os respetivos dados de contacto, bem como as respetivas competências substantivas e territoriais, se for caso disso, ao Secretário-Geral do Conselho da Europa. Os artigos subsequentes preveem um quadro pormenorizado para a cooperação e a assistência mútua.

136. Embora a cooperação entre as Partes seja, em geral, realizada pelas autoridades de controlo estabelecidas nos termos do artigo 15.º, não se pode excluir que uma Parte nomeie outra autoridade para dar cumprimento ao disposto no artigo 16.º

137. A cooperação e a assistência geral são relevantes para os controlos a priori, bem como para os controlos a posteriori (por exemplo, para verificar as atividades de um responsável específico pelo tratamento de dados). A informação partilhada pode ser de natureza jurídica ou factual.

Artigo 17 – Formas de cooperação

138. Nos termos do artigo 17.º, as autoridades de controlo, na aceção do artigo 15.º, cooperarão entre si na medida do necessário para o desempenho das suas funções e o exercício dos seus poderes. Dado que o artigo 17.º limita a cooperação das autoridades de controlo ao necessário “para o desempenho das suas

funções e o exercício dos seus poderes" e o facto de a capacidade de cooperação de uma autoridade de controlo depender do âmbito dos seus poderes, a disposição não se aplica na medida em que uma Parte faça uso do artigo 11.º, n.º 3, o que implica uma limitação dos poderes das autoridades de controlo nos termos do artigo 15.º, n.º 2, alíneas a) a d).

139. A cooperação pode assumir várias formas, algumas formas "por coerção", como a aplicação da legislação em matéria de proteção de dados através da assistência mútua, em que a legalidade da ação de cada autoridade de controlo é indispensável, a algumas formas "brandas", como ações de sensibilização, formação e intercâmbio de pessoal.

140. A enumeração de possíveis atividades de cooperação não é exaustiva. Em primeiro lugar, as autoridades de controlo prestarão assistência mútua, nomeadamente através da partilha de toda a informação pertinente e útil. Esta informação pode ter uma dupla natureza: "informação e documentação sobre a sua legislação e práticas administrativas em matéria de proteção de dados" (que normalmente não suscita quaisquer questões, podendo essa informação ser livremente partilhada e disponibilizada ao público), bem como informação confidencial, incluindo dados pessoais.

141. No que diz respeito aos dados pessoais, esses dados só podem ser objeto de intercâmbio se forem essenciais para a cooperação, ou seja, se, sem a sua disponibilização, a cooperação se tornar ineficaz ou se o "titular dos dados em causa tenha dado o seu consentimento explícito, específico, livre e informado". Em qualquer caso, a transferência de dados pessoais deve respeitar as disposições da Convenção e, em especial, o Capítulo II (ver também o artigo 20.º que estabelece os motivos de recusa).

142. Para além da prestação de informação pertinente e útil, os objetivos da cooperação podem ser alcançados através de investigações ou intervenções coordenadas, bem como de ações conjuntas. No que se refere aos procedimentos aplicáveis, as autoridades de controlo remeterão para a legislação interna aplicável, como os códigos de processo administrativo, civil ou penal, ou os compromissos supranacionais ou internacionais a que as suas jurisdições estão vinculadas, por exemplo, os tratados de assistência jurídica mútua, tendo avaliado a sua capacidade jurídica para celebrar uma cooperação desse tipo.

143. O n.º 3 refere-se a uma rede de autoridades de controlo, como forma de contribuir para a racionalização do processo de cooperação e, por conseguinte, para a eficácia da proteção dos dados pessoais. É importante salientar que a Convenção se refere a "uma rede" no singular. Tal não impede que as autoridades de controlo originárias das Partes participem noutras redes pertinentes.

Artigo 18 – Assistência aos titulares dos dados

144. O n.º 1 garante que os titulares dos dados, quer numa Parte na Convenção quer num país terceiro, terão a possibilidade de exercer os seus direitos reconhecidos no artigo 9.º, independentemente do seu local de residência ou da sua nacionalidade.

145. De acordo com o n.º 2, se o titular de dados residir noutra Parte, é-lhe dada a possibilidade de exercer os seus direitos quer diretamente no país onde a informação relativa ao titular de dados em causa é objeto de tratamento, quer indiretamente, por intermédio da autoridade designada.

146. Além disso, os titulares dos dados que residem no estrangeiro podem também dispor da oportunidade de exercer os seus direitos com a assistência dos agentes diplomáticos ou consulares do seu próprio país.

147. O n.º 3 especifica que os pedidos devem ser tão específicos quanto possível para que o processo seja expedito.

Artigo 19 – Garantias

148. O presente artigo garante que as autoridades de controlo estão sujeitas à mesma obrigação de respeitar os poderes discricionários e a confidencialidade em relação às autoridades de proteção de dados de outras Partes e aos titulares dos dados residentes no estrangeiro.

149. A assistência de uma autoridade de controlo em nome de um titular de dados só pode ser prestada em resposta a um pedido deste último. A autoridade deve ter recebido um mandato do titular dos dados e

não pode agir de forma autónoma em seu nome. Esta disposição é de importância fundamental para a confiança mútua, na qual se baseia a assistência mútua.

Artigo 20 – Indeferimento de pedidos

150. Este artigo estabelece que as Partes são obrigadas a satisfazer os pedidos de cooperação e de assistência mútua. Os motivos de indeferimento de cumprimento são exaustivamente enumerados.

151. O termo "conformidade", utilizado na alínea c), deve ser entendido em sentido lato como abrangendo não só a resposta ao pedido, mas também a ação que o precede. Por exemplo, uma autoridade requerida pode recusar uma ação não só se a transmissão à autoridade requerente da informação solicitada for suscetível de prejudicar os direitos e as liberdades fundamentais de uma pessoa, mas também se o próprio facto de solicitar a informação for suscetível de prejudicar os seus direitos e liberdades fundamentais. Além disso, a autoridade requerida pode ser obrigada, nos termos da legislação interna aplicável, a assegurar a proteção de outros interesses de ordem pública (por exemplo, garantindo a confidencialidade de uma investigação policial). Para o efeito, uma autoridade de controlo pode ser obrigada a omitir determinada informação ou documentos na sua resposta a um pedido.

Artigo 21 – Custos e procedimentos

152. As disposições deste artigo são análogas às de outros instrumentos internacionais.

153. A fim de não sobrecarregar a Convenção com um conjunto enorme de pormenores de aplicação, o n.º 3 deste artigo prevê que os procedimentos, os formulários e a língua a utilizar podem ser acordados entre as Partes envolvidas. O texto deste número não exige quaisquer procedimentos formais, mas permite disposições administrativas, que podem ser mesmo limitadas a casos específicos. Além disso, é aconselhável que as Partes deixem às autoridades de controlo competentes o poder de celebrar tais acordos. As formas de cooperação e assistência podem também variar de caso para caso. É evidente que a transmissão de um pedido de acesso a informação médica sensível terá requisitos diferentes dos inquéritos de rotina sobre as entradas num registo da população.

Capítulo VI – Comité da Convenção

Artigo 22 – Composição do comité

154. O objetivo dos artigos 22.º, 23.º e 24.º é facilitar a aplicação efetiva da Convenção e, se necessário, completá-la. O Comité da Convenção constitui outro meio de cooperação das Partes na aplicação da legislação em matéria de proteção de dados implementada nos termos da Convenção.

155. Um Comité da Convenção é composto por representantes de todas as Partes, das autoridades nacionais de controlo ou do governo.

156. A natureza do Comité da Convenção e o procedimento provável seguido poderão ser semelhantes aos instituídos ao abrigo de outras convenções celebradas no âmbito do Conselho da Europa.

157. Uma vez que a Convenção aborda um tema em constante evolução, é de esperar que surjam questões tanto no que diz respeito à aplicação prática da Convenção (artigo 23.º, alínea a)) como no tocante ao seu significado (mesmo artigo, alínea d)).

158. O Regulamento Interno do Comité da Convenção contém disposições relativas ao direito de voto das Partes e às modalidades do exercício desse direito, estando anexado ao Protocolo de Alterações.

159. Qualquer alteração ao Regulamento Interno está sujeita a uma maioria de dois terços, à exceção das alterações às disposições relativas ao direito de voto e às modalidades correspondentes, às quais se aplica o artigo 25.º da Convenção.

160. Aquando da adesão, a UE deve fazer uma declaração que clarifique a repartição de competências entre a UE e os seus Estados-Membros no que diz respeito à proteção dos dados pessoais ao abrigo da Convenção. Subsequentemente, a UE informará o Secretário-Geral de qualquer alteração substancial na repartição de competências.

161. Nos termos do artigo 25.º, o Comité da Convenção pode propor alterações à Convenção e analisar outras propostas de alteração formuladas por uma Parte ou pelo Comité de Ministros (artigo 23.º, alíneas b) e c)).

162. A fim de garantir a aplicação dos princípios de proteção de dados estabelecidos pela Convenção, o Comité da Convenção terá um papel fundamental na avaliação do cumprimento da Convenção, quer aquando da preparação de uma avaliação do nível de proteção dos dados proporcionado por um candidato à adesão (artigo 23.º, alínea e)), quer aquando da avaliação periódica da aplicação da Convenção pelas Partes (artigo 23.º, alínea h)). O Comité da Convenção terá igualmente competência para avaliar a conformidade do sistema de proteção dos dados de um Estado ou organização internacional com a Convenção, se o Estado ou organização o solicitar ao Comité (artigo 23.º, alínea f)).

163. Ao emitir tais pareceres sobre o nível de conformidade com a Convenção, o Comité da Convenção trabalhará com base num procedimento justo, transparente e público descrito no seu Regulamento Interno.

164. Ademais, o Comité da Convenção pode aprovar modelos de salvaguardas normalizadas para as transferências de dados (artigo 23.º, alínea g)).

165. Por último, o Comité da Convenção pode ajudar a resolver as dificuldades que surjam entre as Partes (artigo 23.º, alínea i)). Em caso de litígio, o Comité da Convenção procurará encontrar uma solução através de negociação ou de qualquer outro meio amigável.

Capítulo VII – Alterações

Artigo 25 – Alterações

166. O Comité de Ministros que adotou o texto original da presente Convenção é igualmente competente para aprovar quaisquer alterações.

167. Em conformidade com o n.º 1, a iniciativa de alteração pode ser tomada pelo próprio Comité de Ministros, pelo Comité da Convenção ou por uma Parte (quer se trate ou não de um Estado-Membro do Conselho da Europa).

168. Qualquer proposta de alteração que não tenha sido elaborada pelo Comité da Convenção deve ser-lhe submetida, em conformidade com o n.º 3, para obtenção do respetivo parecer.

169. Em princípio, qualquer alteração entrará em vigor no trigésimo dia após todas as Partes terem informado o Secretário-Geral do Conselho da Europa da sua aceitação. No entanto, o Comité de Ministros pode decidir, por unanimidade que, em determinadas circunstâncias e após consulta do Comité da Convenção, essas alterações entram em vigor após o termo de um prazo de três anos, a menos que uma Parte notifique o Secretário-Geral de uma objeção. Este procedimento, cujo objetivo é acelerar a entrada em vigor das alterações, preservando simultaneamente o princípio do consentimento de todas as Partes, é aplicável às alterações menores e técnicas.

Capítulo VIII – Cláusulas finais

Artigo 26 – Entrada em vigor

170. Uma vez que, para a eficácia da Convenção, é considerado essencial um vasto âmbito geográfico, o n.º 2 fixa em cinco o número de ratificações por Estados-Membros do Conselho da Europa necessário para a sua entrada em vigor.

171. A Convenção está aberta à assinatura da União Europeia[18].

[18] As alterações à Convenção aprovadas pelo Comité de Ministros em 15 de junho de 1999 perdem o seu objeto a partir da entrada em vigor do Protocolo.

Artigo 27 – Adesão de Estados não membros e de organizações internacionais

172. A Convenção, que foi inicialmente elaborada em estreita cooperação com a OCDE e vários Estados não europeus, está aberta a qualquer Estado de todo o mundo que cumpra as suas disposições. O Comité da Convenção tem por missão avaliar esse cumprimento e elaborar um parecer destinado ao Comité de Ministros sobre o nível de proteção dos dados do candidato à adesão.

173. Tendo em conta a natureza sem fronteiras dos fluxos de dados, procura-se a adesão dos países e das organizações internacionais de todo o mundo. As organizações internacionais que podem aderir à Convenção são exclusivamente organizações internacionais que são definidas como organizações de direito internacional público.

Artigo 28 – Cláusula territorial

174. A aplicação da Convenção a territórios remotos sob a jurisdição das Partes ou em nome dos quais uma Parte pode assumir compromissos reveste-se de importância prática, tendo em conta a utilização que é feita de países distantes para operações de tratamento de dados, quer por razões de custo e de mão-de-obra, quer tendo em vista a utilização da capacidade alternada de tratamento de dados noturnos e diurnos.

Artigo 29 – Reservas

175. As regras contidas na presente Convenção constituem os elementos mais básicos e essenciais para uma proteção eficaz dos dados. Por este motivo, a Convenção não permite a formulação de reservas às suas disposições, que são, além disso, razoavelmente flexíveis, tendo em conta as exceções e restrições permitidas por determinados artigos.

Artigo 30 – Denúncia

176. Qualquer Parte pode denunciar a Convenção a qualquer momento.

Artigo 31 – Notificações

177. Estas disposições estão em conformidade com as cláusulas finais habituais constantes de outras convenções do Conselho da Europa.

Embora os princípios fundamentais contidos na Convenção n.º 108 de 1981 tenham resistido ao teste do tempo e a sua abordagem generalista e tecnologicamente neutra constitua uma força inegável, o Conselho da Europa considerou necessário modernizar o seu instrumento de referência.

A modernização da Convenção n.º 108 visa dois objetivos principais: enfrentar os desafios decorrentes da utilização das novas tecnologias da informação e da comunicação e reforçar a aplicação efetiva da Convenção.