



**17/PT**

**GT 249**

**Parecer 2/2017 sobre o tratamento de dados no local de trabalho**

**Adotado em 8 de junho de 2017**

Este Grupo de Trabalho foi instituído pelo artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições são descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

O secretariado é assegurado pela Direção C (Direitos Fundamentais e Estado de Direito) da Comissão Europeia, Direção-Geral da Justiça e dos Consumidores, B-1049 Bruxelas, Bélgica, Gabinete n.º MO59 05/35

Sítio Web: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

# Índice

1	Resumo .....	4
2.	INTRODUÇÃO .....	4
3.	O quadro jurídico .....	6
3.1	Diretiva 95/46/CE — Diretiva «Proteção de Dados» («DPD»).....	6
3.1.1	<i>FUNDAMENTOS JURÍDICOS (ARTIGO 7.º)</i> .....	7
3.1.2	<i>TRANSPARÊNCIA (ARTIGOS 10.º E 11.º)</i> .....	9
3.1.3	<i>DECISÕES AUTOMATIZADAS (ARTIGO 15.º)</i> .....	10
3.2	Regulamento 2016/679 — Regulamento Geral sobre a Proteção de Dados («RGPD»)10	
3.2.1	<i>PROTEÇÃO SDE DADOS DESDE A CONCEÇÃO</i> .....	10
3.2.2	<i>AVALIAÇÕES DE IMPACTO SOBRE A PROTEÇÃO DE DADOS</i> .....	10
3.2.2	<i>«TRATAMENTO DE DADOS NO CONTEXTO LABORAL»</i> .....	10
4.	Riscos .....	11
5.	Cenários .....	12
5.1	Operações de tratamento durante o processo de recrutamento .....	13
5.2	Operações de tratamento decorrentes da verificação dos antecedentes laborais .....	15
5.3	Operações de tratamento decorrentes da utilização de monitorização das TIC no local de trabalho .....	15
5.4	Operações de tratamento decorrentes da utilização de monitorização das TIC fora do local de trabalho.....	20
5.5	Operações de tratamento relacionadas com a pontualidade e a assiduidade .....	23
5.6	Operações de tratamento que utilizam sistemas de vídeo de monitorização .....	24
5.7	Operações de tratamento que envolvem veículos utilizados pelos empregados .....	24
5.8	Operações de tratamento que envolvem a divulgação de dados dos empregados a terceiros .....	26
5.9	Operações de tratamento que envolvem transferências internacionais de dados de RH e de outros empregados.....	27
6.	Conclusões e recomendações .....	27
6.1	Direitos fundamentais .....	27
6.2	Consentimento; interesse legítimo .....	28
6.3	Transparência .....	28
6.4	Proporcionalidade e minimização dos dados .....	28
6.5	Serviços de computação em nuvem, aplicações em linha e transferências internacionais	29



## 1 Resumo

O presente parecer completa as publicações do anterior Grupo de Trabalho do artigo 29.º («GT 29»), *Parecer 8/2001 sobre o tratamento de dados pessoais no contexto laboral*(GT 48)<sup>1</sup>e o *documento de trabalho de 2002 sobre a vigilância das comunicações eletrónicas no local de trabalho* (GT 55)<sup>2</sup>. Desde a publicação destes documentos, foram adotadas várias novas tecnologias que permitem o tratamento de dados pessoais dos empregados no local de trabalho de uma forma mais sistemática, criando desafios importantes em matéria de proteção de dados e privacidade.

O presente parecer faz uma nova avaliação do equilíbrio entre o interesse legítimo dos empregadores e a expectativa razoável de privacidade dos empregados, sublinhando os riscos colocados pelas novas tecnologias e realizando uma avaliação da proporcionalidade de vários cenários em que poderiam ser aplicadas.

Embora principalmente relacionado com a Diretiva «Proteção de Dados», o parecer examina as obrigações suplementares impostas aos empregadores pelo Regulamento Geral sobre a Proteção de Dados. Reafirma também a posição e as conclusões do Parecer 8/2001 e do documento de trabalho GT 55, segundo as quais, aquando do tratamento dos dados pessoais dos empregados:

- os empregadores devem ter sempre em conta os princípios fundamentais da proteção de dados, independentemente da tecnologia utilizada;
- o conteúdo das comunicações eletrónicas feitas a partir de um estabelecimento comercial goza da mesma proteção dos direitos fundamentais que a das comunicações análogas;
- é muito improvável que o consentimento possa constituir uma base jurídica para o tratamento de dados no local de trabalho, a menos que os empregados possam recusar, sem consequências adversas;
- a execução de um contrato e o interesse legítimo podem, por vezes, ser invocados, desde que o tratamento seja estritamente necessário para uma finalidade legítima e respeite os princípios da proporcionalidade e da subsidiariedade;
- os empregados devem receber informações eficazes sobre a realização da monitorização; e
- qualquer transferência internacional de dados dos empregados apenas deve ser realizada nos casos em que seja garantido um nível de proteção adequado.

## 2. INTRODUÇÃO

A rápida adoção das novas tecnologias da informação nos locais de trabalho, em termos de infraestruturas, aplicações e dispositivos inteligentes, possibilita novos tipos de tratamento de dados no local de trabalho de forma sistemática e potencialmente intrusiva. Por exemplo:

---

<sup>1</sup> GT 29, *Parecer 8/2001 sobre o tratamento de dados pessoais no contexto laboral*, GT 48, 13 de setembro de 2001, URL:

[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf)

<sup>2</sup> GT 29, *documento de trabalho sobre a vigilância das comunicações eletrónicas no local de trabalho*, GT 55, 29 de maio de 2002, URL:

[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_pt.pdf)

- as tecnologias de tratamento de dados no local de trabalho podem agora ser aplicadas por apenas uma fração dos custos de há alguns anos e, ao mesmo tempo, a capacidade de tratamento de dados pessoais por meio destas tecnologias aumenta exponencialmente;
- as novas formas de tratamento, tais como as referentes a dados pessoais na utilização de serviços em linha e/ou os dados de localização provenientes de dispositivos inteligentes, são muito menos visíveis para os empregados do que outros tipos mais tradicionais, tais como as câmaras de televisão em circuito fechado (sistemas CCTV) aparentes. Isto levanta questões quanto ao grau de conhecimento que os empregados têm dessas tecnologias, uma vez que os empregadores podem ilicitamente aplicar este tratamento sem aviso prévio aos empregados; e
- as fronteiras entre o domicílio e o local de trabalho são cada vez mais ténues. Por exemplo, quando os empregados trabalham à distância (por exemplo, a partir de casa), ou quando fazem viagens de negócios, a monitorização das atividades fora do ambiente físico de trabalho pode ser realizada e, eventualmente, incluir a monitorização da pessoa num contexto privado.

Por conseguinte, embora a utilização de tais tecnologias possa ser útil para detetar ou impedir a perda de propriedade intelectual e material de uma empresa, a melhoria da produtividade dos empregados e a proteção de dados pessoais pelo responsável pelo tratamento de dados também criam importantes desafios em matéria de proteção de dados e privacidade. Em consequência, é necessária uma nova avaliação relativa ao equilíbrio entre o interesse legítimo do empregador para proteger a sua empresa e a expectativa razoável de privacidade dos titulares dos dados: os empregados.

Embora o presente parecer incida sobre as novas tecnologias da informação, avaliando nove diferentes cenários em que podem figurar, também reflete resumidamente sobre os métodos mais tradicionais do tratamento de dados no local de trabalho onde os riscos aumentam, em consequência da evolução tecnológica.

No caso em que o termo «empregado» seja utilizado no presente parecer, o GT 29 não pretende restringir o âmbito deste termo apenas a pessoas com um contrato de trabalho reconhecido como tal, nos termos da legislação laboral aplicável. Ao longo das últimas décadas, novos modelos de negócio apresentados por diferentes tipos de relações laborais e, nomeadamente, o emprego em regime liberal, tornaram-se mais frequentes. O presente parecer pretende cobrir todas as situações em que exista uma relação de trabalho, independentemente da questão de saber se esta relação se baseia num contrato de trabalho.

É importante referir que os empregados raramente estão em posição de dar, recusar ou revogar livremente o consentimento, dada a dependência que resulta da relação entre o empregador e o empregado. Exceto em situações excecionais, o empregador tem de invocar outro fundamento jurídico que não o consentimento, como a necessidade de tratar os dados para o seu interesse legítimo. No entanto, um interesse legítimo em si mesmo não é suficiente para prevalecer sobre os direitos e liberdades dos empregados.

Independentemente da base jurídica para tal tratamento, um teste de proporcionalidade deve ser realizado antes do seu início, para considerar a questão de saber se o tratamento é necessário para atingir uma finalidade legítima, bem como as medidas que devem ser adotadas para garantir que as violações do direito à vida privada e à confidencialidade das comunicações sejam limitadas ao mínimo. Isto pode fazer parte de uma avaliação de impacto sobre a proteção de dados (AIPD).

### 3. O quadro jurídico

Embora a análise que se segue seja principalmente efetuada no que respeita ao quadro jurídico em vigor nos termos da Diretiva 95/46/CE (Diretiva «Proteção de Dados» ou «DPD»)<sup>3</sup>, o presente parecer abordará também as obrigações nos termos do Regulamento 2016/679 (Regulamento Geral sobre a Proteção de Dados ou «RGPD»)<sup>4</sup>, que já entrou em vigor e que passará a ser aplicável em 25 de maio de 2018.

No que diz respeito à proposta do Regulamento «privacidade e comunicações eletrónicas»<sup>5</sup>, o Grupo de Trabalho convida os legisladores europeus a criar uma exceção específica para a interferência com dispositivos fornecidos aos empregados<sup>6</sup>. A proposta de regulamento não contém uma exceção adequada à proibição geral de interferência, e os empregadores normalmente não podem fornecer um consentimento válido para o tratamento de dados pessoais dos seus empregados.

#### 3.1 Diretiva 95/46/CE — Diretiva «Proteção de Dados» («DPD»)

No Parecer 8/2001, o GT 29 sublinhou anteriormente que os empregadores têm em conta os princípios fundamentais de proteção de dados da Diretiva «Proteção de Dados» quando procedem ao tratamento de dados pessoais no contexto laboral. O desenvolvimento de novas tecnologias e de novos métodos de tratamento neste contexto não vieram a alterar esta realidade, de facto, pode dizer-se que esse desenvolvimento tornou-os *mais* importantes para os empregadores o fazerem. Neste contexto, os empregadores devem:

- garantir que os dados são tratados para determinadas finalidades legítimas que são proporcionais e necessárias;
- ter em conta o princípio da limitação da finalidade, garantindo, ao mesmo tempo que os dados são adequados, pertinentes e não excessivos para a finalidade legítima;
- aplicar os princípios da proporcionalidade e da subsidiariedade, independentemente do fundamento jurídico aplicável;
- ser transparente com os empregados sobre a utilização e as finalidades das tecnologias de monitorização;
- permitir o exercício dos direitos dos titulares dos dados, incluindo os direitos de acesso e, quando adequado, os direitos de retificação, supressão ou bloqueio de dados pessoais;
- manter os dados exatos, e não os conservar mais tempo do que o necessário; e

---

<sup>3</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, *JO L 281 de 23/11/1995*, pp. 31-50, URL: <http://eur-lex.europa.eu/legal-content/EN-PT/TXT/?uri=CELEX:31995L0046&from=EN>

<sup>4</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), *JO L 119/1 de 4.5.2016*, pp. 1-88, URL: <http://eur-lex.europa.eu/legal-content/EN-PT/TXT/?uri=CELEX:32016R0679&from=EN>

<sup>5</sup> Proposta de regulamento do Parlamento Europeu e do Conselho, relativo ao respeito pela vida privada e a proteção de dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE, 2017/0003 (COD), URL: [ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-10-F1-PT-MAIN-PART-1.PDF](http://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-10-F1-PT-MAIN-PART-1.PDF)

<sup>6</sup> Ver GT 29, *Parecer 1/2017 sobre a Proposta de regulamento «privacidade e comunicações eletrónicas»*, GT 247, 4 de abril de 2017, página 29; URL: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44103](http://ec.europa.eu/newsroom/document.cfm?doc_id=44103)

- tomar todas as medidas necessárias para proteger os dados contra o acesso não autorizado e garantir que o pessoal tenha conhecimento suficiente das obrigações em matéria de proteção de dados.

Sem repetir os anteriores pareceres formulados, o GT 29 gostaria de salientar três princípios, a saber: os fundamentos jurídicos, a transparência e as decisões automatizadas.

### 3.1.1 *FUNDAMENTOS JURÍDICOS (ARTIGO 7.º)*

Quando o tratamento de dados pessoais no contexto laboral é realizado, pelo menos, um dos critérios definidos no artigo 7.º tem de ser satisfeito. Se os tipos de dados pessoais tratados envolverem categorias especiais (como definidas no artigo 8.º), o tratamento é proibido, a menos que seja aplicável uma exceção<sup>7,8</sup>. Mesmo que o empregador possa invocar uma dessas exceções, o fundamento jurídico do artigo 7.º ainda é necessário para o tratamento ser legítimo.

Em resumo, os empregadores devem, por conseguinte, tomar nota do seguinte:

- relativamente à maioria de tal tratamento de dados no local de trabalho, **a base jurídica não pode, e não deve ser o consentimento dos empregados** (artigo 7.º, alínea a)), devido à natureza da relação entre empregador e empregado;
- o tratamento pode ser necessário para **a execução de um contrato** (artigo 7.º, alínea b)), nos casos em que o empregador tem de proceder ao tratamento de dados do empregado para cumprir tais obrigações;
- é bastante comum o **direito laboral poder impor obrigações jurídicas** (artigo 7.º, alínea c)) **necessárias ao tratamento de dados pessoais**; em tais casos, o empregado deve ser clara e plenamente informado de tal tratamento (a menos que seja aplicável uma exceção);
- caso o empregador procure invocar um **interesse legítimo** (artigo 7.º, alínea f)), a finalidade do tratamento deve ser legítima; o método escolhido ou a tecnologia específica devem ser necessários, proporcionais e aplicados da forma menos intrusiva possível, juntamente com a capacidade para permitir ao empregador demonstrar que **foram tomadas as medidas adequadas** para garantir um equilíbrio com as liberdades e os direitos fundamentais dos empregados<sup>9</sup>;
- as operações de tratamento devem cumprir também os **requisitos de transparência** (artigos 10.º e 11.º), e os empregados devem ser clara e plenamente informados do

<sup>7</sup> Como referido na parte 8 do Parecer 8/2001; por exemplo, o artigo 8.º, n.º 2, alínea b) prevê uma exceção para efeitos do cumprimento das obrigações e dos direitos específicos do responsável pelo tratamento de dados em matéria de direito laboral, desde que o mesmo seja autorizado pelo direito nacional, estabelecendo garantias adequadas.

<sup>8</sup> É de notar que, em alguns países, existem medidas especiais em vigor que os empregadores devem respeitar para proteger a vida privada dos empregados. Portugal é um exemplo dos países onde existem tais medidas especiais e medidas similares podem ser aplicáveis também em alguns outros Estados-Membros. As conclusões, no ponto 5.6, bem como os exemplos apresentados nos pontos 5.1 e 5.7.1 do presente parecer não são, por conseguinte, válidas em Portugal por estes motivos.

<sup>9</sup> GT 29, *Parecer 6/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento de dados na aceção do artigo 7.º da Diretiva 95/46/CE*, GT 217, adotado em 9 de abril de 2014, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf)

tratamento dos seus dados pessoais<sup>10</sup>, incluindo da existência de qualquer monitorização; e

- as **medidas técnicas e organizativas adequadas** devem ser adotadas para garantir a segurança do tratamento (artigo 17.º).

Os critérios mais pertinentes na aceção do artigo 7.º são descritos em pormenor a seguir.

- **Consentimento (artigo 7.º, alínea a))**

O consentimento, de acordo com a Diretiva «Proteção de Dados», é definido como qualquer manifestação de vontade, livre, específica e informada, pela qual o titular dos dados aceita que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. Para que o consentimento seja válido, o mesmo deve ser igualmente revogável.

O GT 29 sublinhou anteriormente no Parecer 8/2001 que, quando um empregador tenha de proceder ao tratamento de dados pessoais dos seus empregados, é enganoso partir da suposição de que o tratamento pode ser legitimado através do consentimento dos empregados. Nos casos em que um empregador afirme que é necessário o consentimento e exista um efetivo e potencial prejuízo que decorre do não consentimento do empregado (que pode ser altamente provável no contexto laboral, especialmente no que se refere ao acompanhamento por parte do empregador do comportamento do empregado ao longo do tempo), o consentimento não é válido, uma vez que não é, nem pode ser dado livremente. Assim, relativamente à maioria dos casos de tratamento de dados dos empregados, o fundamento jurídico de tal tratamento não pode, e não deve ser o consentimento dos empregados, sendo necessária uma base jurídica diferente.

Além disso, mesmo nos casos em que o consentimento pudesse ser considerado como constituindo uma base jurídica válida de tal tratamento (ou seja, se puder ser, sem qualquer dúvida, concluído que o consentimento é dado livremente), a manifestação de vontade do empregado tem de ser específica e informada. Os valores predefinidos nos dispositivos e/ou a instalação de *software* que facilitem o tratamento eletrónico de dados pessoais não podem ser qualificados como consentimento dado pelos empregados, uma vez que o consentimento exige uma manifestação ativa de vontade. A falta de ação (ou seja, não alterar os valores predefinidos) não pode, em geral, ser considerada como um consentimento específico para permitir tal tratamento<sup>11</sup>.

- **Execução de um contrato (artigo 7.º, alínea b))**

As relações de trabalho baseiam-se frequentemente num contrato de trabalho entre o empregador e o empregado. Quando se cumprem as obrigações nos termos deste contrato, tais como o pagamento do empregado, o empregador é obrigado a proceder ao tratamento de determinados dados pessoais.

- **Obrigações legais (artigo 7.º, alínea c))**

---

<sup>10</sup> Nos termos do artigo 11.º, n.º 2, da Diretiva «Proteção de Dados», o responsável pelo tratamento de dados está isento da obrigação de prestar informações ao titular dos dados, nos casos em que o registo ou a recolha de dados seja expressamente estabelecido por lei.

<sup>11</sup> Ver também GT 29, *Parecer 15/2011 sobre a definição de consentimento*, GT 187, 13 de julho de 2011, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pt.pdf), página 24.

É muito comum o direito laboral impor obrigações jurídicas ao empregador, cujo tratamento de dados pessoais é necessário (por exemplo, para efeitos de cálculo de imposto e de administração de salários). Obviamente, em tais casos, tal direito constitui a base jurídica para o tratamento de dados.

- **Interesse legítimo (artigo 7.º, alínea f))**

Se um empregador pretender invocar o fundamento jurídico do artigo 7.º, alínea f), da Diretiva «Proteção de Dados», a finalidade do tratamento deve ser legítima, assim como o método escolhido ou a tecnologia específica com que o tratamento é realizado deve ser necessário para o interesse legítimo do empregador. Assim, o tratamento deve ser proporcional às necessidades da empresa, ou seja, a finalidade, a que se pretende dar resposta. O tratamento de dados no local de trabalho deve ser realizado da forma menos intrusiva possível e ser dirigido para as áreas específicas de risco. Além disso, se invocado o artigo 7.º, alínea f), o empregado reserva-se o direito de oposição ao tratamento por fundamentos legítimos e imperiosos nos termos do artigo 14.º.

A fim de invocar o artigo 7.º, alínea f) como o fundamento jurídico para o tratamento, é essencial que existam medidas específicas de atenuação para garantir um equilíbrio adequado entre o interesse legítimo do empregador e os direitos e liberdades fundamentais dos empregados<sup>12</sup>. Tais medidas, dependendo da forma de monitorização, devem incluir limitações em matéria de monitorização, por forma a garantir que a privacidade do empregado não é violada. Tais limitações poderiam ser:

- geográficas (por exemplo, a monitorização apenas em lugares específicos; a monitorização de áreas sensíveis como locais religiosos e espaços sanitários e de convívio deve ser proibida),
- orientadas por dados (por exemplo, os ficheiros eletrónicos pessoais e a comunicação não devem ser objeto de monitorização); e
- relacionadas com o tempo (por exemplo, a amostragem em vez da monitorização contínua).

### **3.1.2 TRANSPARÊNCIA (ARTIGOS 10.º E 11.º)**

Os requisitos em matéria de transparência dos artigos 10.º e 11.º aplicam-se ao tratamento de dados no local de trabalho; Os empregados devem ser informados da existência de qualquer monitorização, das finalidades para as quais os dados pessoais são tratados e de quaisquer outras informações necessárias para garantir um tratamento justo.

Com as novas tecnologias, a necessidade de transparência torna-se mais evidente, uma vez que permitem a recolha e o tratamento posterior de, possivelmente, enormes quantidades de dados pessoais de uma forma discreta.

---

<sup>12</sup> Para um exemplo de equilíbrio que deve ser encontrado, ver o processo *Köpke contra a Alemanha*, [2010] CEDH 1725, (URL: <http://www.bailii.org/eu/cases/ECHR/2010/1725.html>), em que um empregado que foi despedido em consequência de uma operação de videovigilância discreta realizada pelo empregador e uma agência de detetive privado. Embora, neste processo, o Tribunal concluísse que as autoridades nacionais tinham encontrado um equilíbrio justo entre o interesse legítimo do empregador (na proteção dos seus direitos patrimoniais), o direito do empregado ao respeito pela vida privada, e o interesse público na administração da justiça, observou também que aos vários interesses em causa poderia ser dada uma ponderação diferente no futuro como consequência do desenvolvimento tecnológico.

### **3.1.3 DECISÕES AUTOMATIZADAS (ARTIGO 15.º)**

O artigo 15.º da Diretiva «Proteção de Dados» reconhece também ao titular dos dados o direito de não ficar sujeito a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, como por exemplo, a sua capacidade profissional, a menos que a decisão seja necessária para a celebração ou execução de um contrato, autorizada pelo direito da União ou do Estado-Membro, ou se baseie no consentimento explícito do titular dos dados.

## **3.2 Regulamento 2016/679 — Regulamento Geral sobre a Proteção de Dados («RGPD»)**

O Regulamento Geral sobre a Proteção de Dados inclui e reforça os requisitos na sequência da Diretiva «Proteção de Dados». Introduce também novas obrigações para todos os responsáveis pelo tratamento de dados, incluindo os empregadores.

### **3.2.1 PROTEÇÃO DE DADOS DESDE A CONCEÇÃO**

O artigo 25.º do Regulamento Geral sobre a Proteção de Dados exige que os responsáveis pelo tratamento de dados apliquem a proteção de dados desde a conceção e por defeito. A título de exemplo: caso um empregador entregue dispositivos aos empregados, as soluções mais respeitadoras da privacidade devem ser escolhidas se as tecnologias de acompanhamento estiverem envolvidas. A minimização dos dados deve também ser tida em conta.

### **3.2.2 AVALIAÇÕES DE IMPACTO SOBRE A PROTEÇÃO DE DADOS**

O artigo 35.º do Regulamento Geral sobre a Proteção de Dados sublinha os requisitos que o responsável pelo tratamento de dados deve realizar para proceder a uma avaliação de impacto sobre a proteção de dados («AIPD») quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. Um exemplo é o caso da avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar.

Nos casos em que a AIPD indique que os riscos identificados não podem ser suficientemente atenuados pelo responsável pelo tratamento de dados, ou seja, os riscos residuais permanecerem elevados, o responsável pelo tratamento de dados deve consultar a autoridade de controlo antes de proceder ao tratamento (artigo 36.º, n.º 1, tal como é esclarecido nas orientações do GT 29 em matéria de AIPD<sup>13</sup>).

### **3.2.2 «TRATAMENTO DE DADOS NO CONTEXTO LABORAL»**

O artigo 88.º do RGPD esclarece que os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a

---

<sup>13</sup> GT 29, *Orientações sobre a avaliação de impacto sobre a proteção de dados (AIPD) e determinar se o tratamento é suscetível de resultar em «risco elevado» para efeitos do Regulamento n.º 2016/679*, GT 248, 4 de abril de 2017, URL: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137), página 18.

defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral. Nomeadamente, estas normas podem ser estabelecidas para efeitos de:

- recrutamento;
- execução do contrato de trabalho (incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas);
- gestão, planeamento e organização do trabalho;
- igualdade e diversidade no local de trabalho;
- saúde e segurança no trabalho;
- proteção dos bens do empregador ou do cliente;
- exercício e gozo (individual) dos direitos e benefícios relacionados com o emprego; e
- cessação da relação de trabalho.

Em conformidade com o artigo 88.º, n.º 2, essas normas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para:

- a transparência do tratamento de dados;
- a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta; e
- os sistemas de controlo no local de trabalho.

No presente parecer, o Grupo de Trabalho apresentou orientações para a utilização legítima de novas tecnologias em várias situações específicas, descrevendo medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais dos empregados.

#### **4. Riscos**

As tecnologias modernas permitem que os empregados sejam objeto de um acompanhamento ao longo do tempo, nos seus locais de trabalho e nos seus domicílios, através de diversos dispositivos, tais como telemóveis inteligentes, computadores de secretária, *tablets*, veículos e tecnologia usável. Se não existirem limites ao tratamento e, se não for transparente, existe um risco elevado de que o interesse legítimo dos empregadores na melhoria da eficiência e da proteção do património de uma empresa se transforme numa monitorização intrusiva e injustificável.

As tecnologias que monitorizam as comunicações podem também ter um efeito dissuasor sobre os direitos fundamentais dos empregados na organização e preparação de reuniões de trabalhadores e na comunicação confidencial (incluindo o direito de procurar informações). A monitorização das comunicações e do comportamento exercerá pressão sobre os empregados para a conformidade, a fim de evitar a deteção daquilo que pode ser considerado como anomalia, de forma comparável ao modo como a utilização intensiva das câmaras de televisão em circuito fechado influenciou o comportamento dos cidadãos em espaços públicos. Além disso, devido às capacidades de tais tecnologias, os empregados podem não ter conhecimento de quais são os dados pessoais que estão a ser tratados e para que fins, embora seja também possível que nem sequer tenham conhecimento da existência da tecnologias de monitorização propriamente ditas.

A utilização de monitorização da TI difere também de outras e mais visíveis ferramentas de observação e de monitorização, como as câmaras de televisão em circuito fechado, na medida em que pode ser realizada de uma forma discreta. Na ausência de uma política de monitorização no local de trabalho de fácil compreensão e facilmente acessível, os empregados podem não ter conhecimento da existência e das consequências da monitorização que está a ser realizada e, por conseguinte, estão impossibilitados de exercer os seus direitos. Um outro risco advém da «recolha excessiva» de dados em tais sistemas, por exemplo, os que recolhem dados de localização *WiFi*.

O aumento da quantidade de dados gerados no local de trabalho, aliado às novas técnicas de análise e de cruzamento de dados, pode também criar riscos de tratamento posterior incompatível. Os exemplos de tratamento posterior ilegítimo são a utilização de sistemas legitimamente instalados para proteger o património para assim monitorizar a disponibilidade, o desempenho e a simpatia dos empregados para com os clientes. Outros exemplos são a utilização de dados recolhidos através de câmaras de televisão em circuito fechado para monitorizar regularmente o comportamento e o desempenho dos empregados, ou a utilização de um sistema de geolocalização (tal como, por exemplo, a localização por *WiFi* ou *Bluetooth*) para verificar constantemente os movimentos e o comportamento de um empregado.

Em consequência, tal localização pode infringir o direito de privacidade dos empregados, independentemente do facto de a monitorização ser realizada de forma sistemática ou ocasional. O risco não se limita à análise do conteúdo das comunicações. Assim, a análise de metadados sobre uma pessoa poderá permitir uma monitorização pormenorizada igualmente invasiva da vida privada e dos padrões de comportamento.

A utilização extensiva das tecnologias de monitorização pode também limitar a disponibilidade dos empregados para (e os canais através dos quais poderiam) informar os empregadores sobre irregularidades ou medidas ilícitas dos superiores e/ou outras ameaças aos empregados para prejudicar a empresa (em especial, os dados do cliente) ou o local de trabalho. O anonimato é muitas vezes necessário para um empregado em causa tomar medidas e comunicar tais situações. A monitorização que atente contra o direito de privacidade dos empregados pode impedir as comunicações necessárias aos responsáveis adequados. Em tal caso, os meios estabelecidos para os autores de denúncia internos podem tornar-se ineficazes<sup>14</sup>.

## 5. Cenários

A presente secção aborda um certo número de tratamento de dados no local de trabalho em que as novas tecnologias e/ou o desenvolvimento das tecnologias existentes têm ou podem ter o potencial de resultar em riscos elevados para a privacidade dos empregados. Em todos esses casos, os empregadores devem ter em consideração, se:

---

<sup>14</sup> Ver, por exemplo, o GT 29, *Parecer 1/2006 sobre a aplicação das regras europeias em matéria de proteção de dados aos sistemas internos de denúncia de infrações nos domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro*, GT 117, 1 de fevereiro de 2006, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_pt.pdf)

- a atividade de tratamento é necessária e, em caso afirmativo, os fundamentos jurídicos que se aplicam;
- a proposta do tratamento de dados pessoais é equitativa para os empregados;
- a atividade de tratamento é proporcional às preocupações suscitadas; e
- a atividade de tratamento é transparente.

### 5.1 Operações de tratamento durante o processo de recrutamento

A utilização dos meios sociais pelas pessoas é generalizada e relativamente comum para que os perfis de utilizador sejam acessíveis ao público, dependendo das definições escolhidas pelo titular da conta. Em consequência, os empregadores podem considerar que a inspeção dos perfis sociais de possíveis candidatos possa ser justificada durante o seu processo de recrutamento. Isto pode também ser o caso de outras informações publicamente disponíveis sobre o potencial empregado.

No entanto, os empregadores não devem pressupor que o simples facto do perfil de um utilizador estar publicamente disponível num meio social lhes permita proceder ao tratamento desses dados para os seus próprios fins. É necessário um fundamento jurídico para este tratamento, tal como um interesse legítimo. Neste contexto, o empregador deve, antes da inspeção do perfil no meio social, ter em conta se o perfil no meio social do candidato diz respeito a fins profissionais ou privados, uma vez que isto pode ser uma indicação importante para a admissibilidade jurídica da inspeção dos dados. Além disso, os empregadores apenas estão autorizados à recolha e ao tratamento de dados pessoais respeitantes aos candidatos a emprego, na medida em que a recolha desses dados é necessária e pertinente para o desempenho da função à qual estão a candidatar-se.

Os dados recolhidos durante o processo de recrutamento devem, em geral, ser eliminados, assim que se torne claro que uma oferta de emprego não será realizada ou não for aceite pela pessoa em causa<sup>15</sup>. A pessoa tem também de ser corretamente informada de qualquer tratamento antes de iniciar o processo de recrutamento.

Não existe qualquer fundamento jurídico para um empregador exigir ao potencial empregado «ser amigo» do potencial empregador, ou por outras vias, facultar o acesso ao conteúdo dos seus perfis.

#### **Exemplo**

Durante o processo de recrutamento de pessoal, um empregador verifica os perfis dos candidatos em várias redes sociais e inclui informações provenientes destas redes (e quaisquer outras informações disponíveis na *Internet*) no processo de verificação.

Apenas se for necessário para o emprego em questão a análise das informações sobre um candidato nos meios sociais, por exemplo, a fim de poder avaliar os riscos específicos em relação a candidatos para uma função específica, e os candidatos serem corretamente informados (por exemplo, no texto do anúncio de emprego), o empregador pode ter uma base

<sup>15</sup> Ver também o Conselho da Europa, *Recomendação CM/Rec (2015) 5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral*, ponto 13.2 (1 de abril de 2015, URL: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805c3f7a](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a)). Nos casos em que o empregador pretenda conservar os dados com vista a uma nova oportunidade de emprego, o titular dos dados deverá ser informado desse facto e de lhe ser dada a possibilidade de se opor a esse tratamento posterior, caso em que deverá ser eliminado (Id.).

jurídica nos termos do artigo 7.º, alínea f), para analisar as informações publicamente disponíveis sobre os candidatos.

## 5.2 Operações de tratamento decorrentes da verificação dos antecedentes laborais

Através da existência de perfis nos meios sociais, e o desenvolvimento de novas tecnologias de análise, os empregadores têm (ou podem obter) a capacidade técnica da verificação, de forma permanente, dos empregados através da recolha de informações sobre os seus amigos, opiniões, crenças, interesses, costumes, paradeiro, atitudes e comportamentos e, por conseguinte, da captação de dados, incluindo os dados sensíveis relativos à vida privada e familiar do empregado.

A verificação dos antecedentes laborais nos perfis dos meios sociais dos empregados não deve ser realizada numa base generalizada.

Além disso, os empregadores devem abster-se de exigir a um empregado ou a um candidato a emprego o acesso a informações que partilha com outros através das redes sociais.

### **Exemplo**

Um empregador monitoriza os perfis de antigos empregados no *LinkedIn* que estão envolvidos durante a vigência das cláusulas de não concorrência. A finalidade desta monitorização consiste em controlar a conformidade com essas cláusulas. A monitorização é limitada a estes antigos empregados.

Enquanto o empregador puder provar que tal monitorização é necessária para proteger os seus interesses legítimos, que não existem outros meios menos invasivos disponíveis e que os antigos empregados tenham sido devidamente informados da extensão da observação regular das suas comunicações públicas, o empregador pode invocar o fundamento jurídico do artigo 7.º, alínea f), da Diretiva «Proteção de Dados».

Além disso, os empregados não devem ser obrigados a utilizar um perfil nos meios sociais que seja fornecido pelo seu empregador. Mesmo quando tal seja especificamente previsto à luz das suas tarefas (por exemplo, porta-voz de uma organização), devem conservar a opção de um perfil «não laboral» não público que possam utilizar em vez do perfil «oficial» relacionado com o empregador e, tal deverá ser especificado nos termos e condições do contrato de trabalho.

## 5.3 Operações de tratamento decorrentes da utilização de monitorização das TIC no local de trabalho

Tradicionalmente, a monitorização das comunicações eletrónicas no local de trabalho (por exemplo, telefone, navegação na *Internet*, correio eletrónico, mensagens instantâneas, VOIP, etc.) era considerada a principal ameaça contra a privacidade dos empregados. Em 2001, no seu *documento de trabalho sobre a vigilância das comunicações eletrónicas no local de trabalho*, o GT 29 retirou várias conclusões relativamente à monitorização do correio eletrónico e da utilização da *Internet*. Embora essas conclusões se mantenham válidas, é necessário ter em conta os mais recentes desenvolvimentos tecnológicos que permitiram novas formas de monitorização potencialmente mais invasivas e difusas. Tais desenvolvimentos incluem, nomeadamente:

- as ferramentas de prevenção de perda de dados (PPD), que realizam a monitorização das comunicações enviadas, a fim de detetar potenciais violações de dados;

- as barreiras de segurança de próxima geração («Next-Generation Firewalls - NGFWs») e os sistemas de gestão unificada de ameaças («Unified Threat Management - UTM»), que podem proporcionar várias tecnologias de monitorização, incluindo a inspeção profunda de pacotes de dados, a interceção de TLS, a filtragem de sítios *Web*, a filtragem de conteúdos, a comunicação integrada de soluções de segurança, as informações da identidade do utilizador (como descrito supra) e a prevenção de perda de dados. Tais tecnologias podem também ser implantadas individualmente, dependendo do empregador;
- as aplicações e as medidas de segurança que envolvem o acesso do empregado para a entrada nos sistemas do empregador;
- a tecnologia *eDiscovery*, que se refere a qualquer processo em que os dados eletrónicos são pesquisados com o objetivo de os utilizar como prova;
- o acompanhamento da aplicação e a utilização do dispositivo através de *software* invisível, quer no computador de secretária, quer na computação em nuvem;
- a utilização de aplicações de escritório no local de trabalho fornecidas como um serviço de computação em nuvem, o que, em teoria, permite a entrada bastante pormenorizada das atividades dos empregados;
- a monitorização de dispositivos pessoais (por exemplo, computadores pessoais, telemóveis, *tablets*), que os empregados fornecem para os seus trabalhos, em conformidade com uma política de utilização específica, tal como a «Bring-Your-Own-Device (BYOD)» (Traga o seu próprio dispositivo), bem como a tecnologia «Mobile Device Management (MDM)» (gestão de dispositivos móveis), que permite a distribuição de aplicações, dados e definições de configuração e correções para dispositivos móveis; e
- a utilização de tecnologia usável (por exemplo, dispositivos relacionados com a saúde e a condição física).

É possível que um empregador venha a aplicar uma solução de monitorização «multifuncional», tal como uma série de pacotes de segurança que lhe permite acompanhar qualquer utilização das TIC no local de trabalho, em vez de apenas a monitorização do endereço de correio eletrónico e/ou dos sítios *Web*, como foi o caso anteriormente. As conclusões adotadas no GT 55 aplicar-se-iam a qualquer sistema que permita a realização de tal monitorização<sup>16</sup>.

### Exemplo

Um empregador tenciona implantar um aparelho de inspeção TLS para decifrar e inspecionar o tráfego seguro, com a finalidade de detetar qualquer ato mal-intencionado. O aparelho é também capaz de registar e analisar toda a atividade em linha de um empregado na rede da organização.

A utilização de protocolos de comunicações cifradas está cada vez mais a ser aplicada para proteger os fluxos de dados em linha que envolvam dados pessoais contra a interceção. No

<sup>16</sup> Ver também o processo *Copland contra o Reino Unido*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (URL: <http://www.bailii.org/eu/cases/ECHR/2007/253.html>), no qual o Tribunal declarou que as mensagens de correio eletrónico enviadas a partir de estabelecimentos comerciais e as informações resultantes da monitorização de utilização da *Internet* poderiam constituir parte da vida privada e da correspondência de um empregado e, que a recolha e o armazenamento dessas informações sem o conhecimento do empregado, representariam uma interferência com os direitos do empregado, embora o Tribunal não decidisse que essa monitorização não deveria nunca ser necessária numa sociedade democrática.

entanto, esta possibilidade pode também colocar problemas, uma vez que a cifragem torna impossível a monitorização da receção e do envio de dados. O equipamento de inspeção TLS decifra o fluxo de dados, analisa o conteúdo para fins de segurança e depois volta a proceder à cifragem do fluxo posteriormente.

Neste exemplo, o empregador invoca o interesse legítimo, a necessidade de proteger a rede e os dados pessoais dos empregados e os clientes mantidos nessa rede, contra o acesso não autorizado ou a fuga de dados. No entanto, a monitorização de cada atividade em linha dos empregados é uma resposta desproporcional e uma interferência com o direito à confidencialidade das comunicações. O empregador deve, em primeiro lugar, investigar outros meios menos invasivos, para proteger a confidencialidade dos dados dos clientes e da segurança da rede.

Na medida em que alguma interceção de tráfego de TLS possa ser qualificada como estritamente necessária, o aparelho deve ser configurado de forma a evitar a entrada permanente dos empregados, por exemplo, através do bloqueio de tráfego suspeito de receção e de envio e do redirecionamento do utilizador para um portal de informação onde pode solicitar a análise de uma decisão automatizada. Se, algumas entradas gerais fossem, no entanto, consideradas estritamente necessárias, o aparelho poderia ser também configurado de forma a não armazenar dados de entrada, a menos que o aparelho assinalasse a ocorrência de um incidente, com minimização das informações recolhidas.

Como exemplo de boas práticas, o empregador poderá oferecer alternativas de acesso sem monitorização aos empregados. Tal poderá ser feito através da oferta gratuita de *WiFi*, ou dos dispositivos autónomos ou terminais (com garantias adequadas para assegurar a confidencialidade das comunicações), sempre que os empregados possam exercer o seu direito legítimo de recorrer a instalações de trabalho para qualquer utilização privada<sup>17</sup>. Além disso, os empregadores devem considerar determinados tipos de tráfego cuja interceção põe em perigo o bom equilíbrio entre os seus interesses legítimos e a privacidade do empregado, tal como a utilização do correio eletrónico, das visitas a serviços bancários em linha e dos sítios *Web* relacionados com a saúde, a fim de, adequadamente, configurar o aparelho, de modo a não prosseguir com a interceção das comunicações em circunstâncias que não são conformes com o princípio da proporcionalidade. As informações sobre o tipo de comunicações cuja monitorização o aparelho realiza devem ser especificadas aos empregados.

Uma política relativa aos efeitos de quando e por quem podem ser acedidos dados de entrada suspeitos deve ser desenvolvida e tornada acessível, de forma fácil e permanente a todos os empregados, a fim de os orientar também sobre a utilização aceitável e não aceitável da rede e das instalações. Tal permite aos empregados adaptar o seu comportamento para evitarem ser controlados quando legitimamente utilizem as instalações de trabalho de TI para utilização privada. Como exemplo de boas práticas, tal política deve ser avaliada, pelo menos, anualmente, a fim de se apreciar se a solução de monitorização escolhida apresenta os

---

<sup>17</sup> Ver o processo *Halford contra o Reino Unido*, [1997] CEDH 32, URL: <http://www.bailii.org/eu/cases/ECHR/1997/32.html>, no qual o Tribunal declarou que as «chamadas telefónicas feitas a partir de estabelecimentos comerciais, bem como de residências podem ser abrangidas pelo conceito de «vida privada» e de «correspondência», na aceção do artigo 8.º, ponto 1 [da Convenção]»; e o processo *Barbulescu contra a Roménia*, [2016] ECHR 61, (URL: <http://www.bailii.org/eu/cases/ECHR/2016/61.html>), relativo à utilização de uma conta pessoal de correio instantâneo profissional para a correspondência, no qual o Tribunal declarou que a monitorização da conta pelo seu empregador foi limitada e proporcional; a opinião dissidente do juiz Pinto de Albuquerque que defendeu que um equilíbrio cuidadoso deveria ser encontrado.

resultados pretendidos, e se existem outras ferramentas ou meios menos invasivos para alcançar a mesma finalidade.

Independentemente da tecnologia em causa ou das capacidades de que dispõe, a base jurídica do artigo 7.º, alínea f) só está disponível se o tratamento satisfizer determinadas condições. Em primeiro lugar, os empregadores que utilizam estes produtos e aplicações devem considerar a proporcionalidade das medidas que estão a aplicar, bem como eventuais medidas adicionais que podem ser tomadas para atenuar ou reduzir a dimensão e o impacto do tratamento de dados. Como exemplo de boas práticas, esta consideração pode ser realizada através de uma AIPD antes da introdução de qualquer tecnologia de monitorização. Em segundo lugar, os empregadores devem aplicar e comunicar políticas de utilização aceitável juntamente com políticas de proteção da privacidade, sublinhando a utilização permissível da rede e do equipamento da organização, e descrevendo com rigor o momento em que o tratamento é realizado.

Em alguns países, a criação de uma tal política iria exigir, do ponto de vista jurídico, a aprovação de uma comissão de trabalhadores ou representação similar dos empregados. Na prática, tais políticas são muitas vezes redigidas pelo pessoal de manutenção das TI. Uma vez que o seu principal objetivo será, na sua maioria, em matéria de segurança, e não sobre a expectativa legítima de privacidade dos empregados, o GT 29 recomenda que em todos os casos uma amostra representativa dos empregados participe na avaliação da necessidade da monitorização, bem como da lógica e da acessibilidade da política.

## **Exemplo**

Um empregador implanta uma ferramenta de prevenção de perda de dados para monitorizar automaticamente o correio eletrónico enviado, a fim de prevenir a transmissão não autorizada de dados de propriedade industrial (por exemplo, dados pessoais do cliente), independentemente de tal ação ser intencional ou não. Quando um correio eletrónico é considerado a fonte potencial de uma violação de dados, é realizada uma investigação aprofundada.

Mais uma vez, o empregador invoca a necessidade do seu interesse legítimo de proteger os dados pessoais dos clientes, bem como o seu património contra o acesso não autorizado ou a fuga de dados. No entanto, tais ferramentas de prevenção de perda de dados podem envolver um tratamento de dados pessoais desnecessário, por exemplo, um alerta de «falsos positivos» pode resultar em acesso não autorizado de correio eletrónico legítimo que tenha sido enviado pelos empregados (que pode ser, por exemplo, correio eletrónico pessoal).

Por conseguinte, a necessidade de as ferramentas de prevenção de perda de dados e a sua implantação devem ser plenamente justificadas, de modo a encontrar o equilíbrio adequado entre os seus interesses legítimos e o direito fundamental à proteção de dados pessoais dos empregados. Para que os interesses legítimos do empregador possam ser invocados, devem ser adotadas determinadas medidas para atenuar os riscos. Por exemplo, as regras que o sistema segue para caracterizar um correio eletrónico como potencial violação de dados devem ser totalmente transparentes para os utilizadores e, nos casos em que a ferramenta reconhece um correio eletrónico que será enviado como uma possível violação de dados, uma mensagem de advertência deve informar o remetente da mensagem de correio eletrónico antes da transmissão por correio eletrónico, de modo a que seja dada ao remetente a possibilidade de cancelar essa transmissão.

Em alguns casos, é possível a monitorização dos empregados, não tanto devido à implantação de tecnologias específicas, mas simplesmente porque os empregados deverão utilizar aplicações em linha que lhes são disponibilizadas pelo empregador que procede ao tratamento de dados pessoais. A utilização de aplicações de escritório baseadas na computação em nuvem (por exemplo, editores de documentos, calendários, redes sociais) constitui um exemplo. Deve garantir-se que os empregados podem designar determinados espaços privados, para os quais o empregador não pode obter acesso, salvo em circunstâncias excecionais. Isto é, por exemplo, pertinente para os calendários, que muitas vezes são também utilizados para nomeações privadas. Se o empregado estabelece uma nomeação para «privado» ou assinala isso na própria nomeação, os empregadores (e outros empregados) não devem ser autorizados a analisar o conteúdo da nomeação.

O requisito da subsidiariedade neste contexto significa, por vezes, que a monitorização não pode ser realizada em caso algum. É o caso, por exemplo, quando a proibição da utilização dos serviços de comunicações pode ser evitada através do bloqueio de determinados sítios *Web*. Se for possível o bloqueio de sítios *Web*, em vez de a monitorização contínua de todas as comunicações, o bloqueio deve ser escolhido, a fim de cumprir este requisito da subsidiariedade.

De um modo mais geral, a prevenção deve ter muito mais peso do que a deteção: os interesses do empregador são mais bem servidos ao prevenir a utilização abusiva da *Internet* através de meios técnicos, do que ao despender de recursos em matéria de deteção de abusos.

## **5.4 Operações de tratamento decorrentes da utilização de monitorização das TIC fora do local de trabalho**

A utilização das TIC fora do local de trabalho tornou-se mais frequente com o crescimento das políticas em matéria de trabalho no domicílio, trabalho à distância e do «Bring-Your-Own-Device» (Traga o seu próprio dispositivo). As capacidades de tais tecnologias podem representar um risco para a vida privada dos empregados, visto que, em muitos casos, os sistemas de monitorização existentes no local de trabalho são efetivamente alargados à esfera doméstica dos empregados quando utilizam estes equipamentos. .

### **5.4.1 MONITORIZAÇÃO DE DOMICÍLIO E TRABALHO À DISTÂNCIA**

Tornou-se mais comum para os empregadores oferecerem aos empregados a possibilidade de trabalhar à distância, por exemplo, a partir de casa e/ou em movimento. Com efeito, este é um fator central subjacente à distinção reduzida entre o local de trabalho e o domicílio. Tal envolve, em geral, para o empregador a entrega de equipamento de TIC ou *software* aos empregados que, uma vez instalados no seu domicílio/nos seus próprios dispositivos, lhes permite ter o mesmo nível de acesso à rede, aos sistemas e aos recursos do empregador que teriam, se estivessem no local de trabalho, dependendo da aplicação.

Ao mesmo tempo, o trabalho à distância pode ter um desenvolvimento positivo, mas apresenta igualmente uma área de risco adicional para o empregador. Por exemplo, os empregados que tenham acesso remoto a infraestruturas do empregador não estão vinculados pelas medidas de segurança física existentes no local das instalações do empregador. Dito claramente: sem a aplicação de medidas técnicas adequadas, o risco de acesso não autorizado aumenta e pode resultar na perda ou destruição das informações, incluindo os dados pessoais dos empregados ou clientes, que o empregador pode deter.

A fim de atenuar esta área de risco, os empregadores podem pensar que existe uma justificação para a implantação de pacotes de *software* (quer nas instalações de trabalho, quer na nuvem) que tenham a capacidade de, por exemplo, registar a digitação no teclado ou os movimentos do rato, as capturas de ecrã (quer de forma aleatória, quer em intervalos fixos), registar as aplicações utilizadas (e durante quanto tempo foram utilizadas) e, mediante dispositivos compatíveis, que permitam imagens de câmaras *Web* e a recolha das mesmas. Estas tecnologias estão amplamente disponíveis, incluindo as provenientes de terceiros, como de prestadores de serviços de computação em nuvem.

No entanto, o tratamento envolvido nessas tecnologias é desproporcional e é muito pouco provável que o empregador tenha um fundamento jurídico na aceção do interesse legítimo, por exemplo, o registo da digitação no teclado ou os movimentos do rato de um empregado.

A solução passa por abordar o risco colocado pelo domicílio e o trabalho à distância, de forma proporcional e não excessiva, seja qual for a opção oferecida e a tecnologia proposta, nomeadamente se as fronteiras entre a utilização privada e a utilização profissional forem fluidas.

### **5.4.2 «BRING-YOUR-OWN-DEVICE - BYOD» (TRAGA O SEU PRÓPRIO DISPOSITIVO)**

Devido ao aumento da popularidade, das características e da capacidade dos dispositivos eletrónicos de consumo, os empregadores podem ser confrontados com pedidos dos empregados para utilizar os seus próprios dispositivos no local de trabalho com vista à

realização do seu trabalho. Esta situação é conhecida como «Traga o seu próprio dispositivo» ou «BYOD».

A aplicação eficaz do «BYOD» pode conduzir a uma série de vantagens para os empregados, incluindo a melhoria da satisfação dos empregados em relação ao emprego, a motivação acrescida em geral, o aumento da eficiência no emprego e uma maior flexibilidade. No entanto, por definição, a utilização de um dispositivo do empregado será de natureza pessoal, e isso é mais suscetível de ser o caso em determinados períodos do dia (por exemplo, à noite e aos fins de semana). Há, por conseguinte, uma possibilidade distinta de que a utilização pelos empregados dos seus próprios dispositivos venha a implicar o tratamento de informações pessoais sobre os empregados pelos empregadores e, eventualmente, sobre os familiares que também utilizam os dispositivos em questão.

No contexto laboral, os riscos para a privacidade do «BYOD» são comumente associados a tecnologias de monitorização que recolhem identificadores como os endereços MAC, ou nos casos em que um empregador acede a um dispositivo do empregado com a justificação de realizar uma análise de segurança, ou seja, de *software* mal-intencionado. No que diz respeito a este último, existem várias soluções comerciais que permitem a análise de dispositivos particulares. No entanto, a sua utilização poderá resultar no acesso a todos os dados armazenados nesse dispositivo e, por conseguinte, tem de ser gerida cuidadosamente. Por exemplo, as partes de um dispositivo que se presumem ser apenas utilizadas para fins privados (por exemplo, a pasta de armazenamento de fotografias do dispositivo) não podem, em princípio, ser acedidas.

A monitorização da localização e do tráfego de tais dispositivos pode ser considerada como servindo um interesse legítimo para proteger os dados pessoais pelos quais o empregador é responsável, tal como o responsável pelo tratamento de dados; No entanto, esta monitorização a um dispositivo pessoal do empregado pode ser ilícita, se tal monitorização também incluir dados relativos à vida privada e familiar do empregado. A fim de evitar a monitorização das informações privadas, devem ser postas em prática medidas adequadas para estabelecer uma distinção entre a utilização privada e a utilização profissional do dispositivo.

Os empregadores devem também aplicar métodos pelos quais os seus próprios dados armazenados no dispositivo são transferidos de forma segura entre esse dispositivo e a respetiva rede. Pode acontecer que o dispositivo seja, por conseguinte, configurado para encaminhar todo o tráfego através de uma rede privada virtual («VPN») para a rede das empresas, de modo a oferecer um determinado nível de segurança; No entanto, se uma medida deste tipo é aplicada, o empregador deve também ter em conta que o *software* instalado, para efeitos de monitorização, apresenta um risco para a privacidade durante os períodos de utilização pessoal pelo empregado. Os dispositivos que oferecem proteção adicional como o isolamento de processos ou «sandboxing» (conservação dos dados contidos numa aplicação específica) poderiam ser utilizados.

Em contrapartida, o empregador deve também considerar a proibição da utilização de dispositivos de trabalhos específicos para utilização privada, se não existir forma de evitar que a utilização privada seja monitorizada, por exemplo, se o dispositivo disponibilizar acesso remoto aos dados pessoais para os quais o empregador é o responsável pelo tratamento de dados.

### **5.4.3 GESTÃO DE DISPOSITIVOS MÓVEIS («MOBILE DEVICE MANAGEMENT — MDM»)**

A gestão de dispositivos móveis permite aos empregadores localizar dispositivos à distância, implantar configurações e/ou aplicações específicas e eliminar dados mediante pedido. O próprio empregador pode utilizar esta funcionalidade, ou recorrer a um terceiro para fazer isso. Os serviços de gestão de dispositivos móveis permitem também aos empregadores registar ou acompanhar o dispositivo em tempo real, caso não seja comunicado o seu furto.

Uma AIPD deve ser realizada antes da implantação dessas tecnologias quando é nova, ou é nova para o responsável pelo tratamento de dados. Se o resultado da AIPD concluir que a tecnologia de gestão de dispositivos móveis é necessária em circunstâncias específicas, ainda assim deve ser realizada uma avaliação para verificar se o tratamento de dados resultante está conforme com os princípios da proporcionalidade e da subsidiariedade. Os empregadores devem garantir que os dados, recolhidos no âmbito desta capacidade de localização remota, são tratados para um fim específico e não podem ou não poderão fazer parte de um programa mais alargado que permita uma monitorização permanente dos empregados. Mesmo para fins específicos, a funcionalidade de acompanhamento deve ser atenuada. Os sistemas de acompanhamento podem ser concebidos para registar os dados de localização sem os apresentar ao empregador. Em tais circunstâncias, os dados de localização devem ficar disponíveis apenas em situações em que o dispositivo seja comunicado ou perdido.

Os empregados cujos dispositivos estejam inscritos nos serviços de gestão de dispositivos móveis também devem ser plenamente informados sobre que acompanhamento está a ser realizado e que consequências isso lhes traz.

### **5.4.4 TECNOLOGIA USÁVEL**

Os empregadores estão cada vez mais tentados a fornecer aos seus empregados tecnologia usável, a fim de acompanhar e monitorizar a sua saúde e atividade no local de trabalho e, por vezes, mesmo fora do local de trabalho. No entanto, este tratamento de dados envolve o tratamento de dados relativos à saúde, e, por conseguinte, é proibido, com base no artigo 8.º da Diretiva «Proteção de Dados».

Tendo em conta a desigualdade na relação entre os empregadores e os empregados, ou seja, a dependência financeira do empregado relativamente ao empregador, e o caráter sensível dos dados relativos à saúde, é muito improvável que o consentimento juridicamente explícito e válido possa ser dado para efeitos de acompanhamento ou monitorização de tais dados, uma vez que os empregados não são, na sua essência, «livres» para dar tal consentimento de antemão. Mesmo que o empregador utilize um terceiro para recolher os dados relativos à saúde, o qual só forneceria informações agregadas sobre a evolução da saúde geral ao empregador, o tratamento poderá ainda ser ilícito.

Por outro lado, como referido no *Parecer 5/2014 sobre as técnicas de anonimização*<sup>18</sup>, é tecnicamente muito difícil de garantir a completa a anonimização dos dados. Mesmo num ambiente com mais de mil empregados, dada a disponibilidade de outros dados sobre os empregados, o empregador poderá continuar a destacar cada empregado com indicações de saúde específicas, tais como a pressão arterial elevada ou a obesidade.

---

<sup>18</sup> GT 29, *Parecer 5/2014 sobre as técnicas de anonimização*, GT 216, 10 de abril de 2014, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf)

**Exemplo:**

Uma organização dá como oferta generalizada dispositivos de monitorização de condição física aos seus empregados. Os dispositivos realizam a contagem do número de passos que os empregados dão e registam os seus batimentos cardíacos, bem como os padrões de sono ao longo do tempo.

Os dados relativos à saúde daí resultantes só devem ser acessíveis ao empregado e não ao empregador. Todos os dados transferidos entre o empregado (como titular dos dados) e o prestador de serviços/dispositivos (como responsável pelo tratamento de dados) são de grande importância para essas partes.

Como os dados relativos à saúde podem também ser tratados pela entidade comercial responsável pelo fabrico dos dispositivos ou pela oferta de um serviço aos empregadores, ao escolher o dispositivo ou o serviço, o empregador deverá avaliar a política de privacidade do fabricante e/ou do prestador de serviços, a fim de garantir que a mesma não implique um tratamento ilícito dos dados relativos à saúde dos empregados.

### **5.5 Operações de tratamento relacionadas com a pontualidade e a assiduidade**

Os sistemas que permitem a monitorização pelos empregadores a quem entra nas suas instalações e/ou em determinadas áreas das suas instalações, podem também permitir o acompanhamento das atividades dos empregados. Embora tais sistemas tenham existido durante vários anos, as novas tecnologias destinadas a acompanhar a pontualidade e a assiduidade dos empregados estão a ser cada vez mais amplamente implantadas, nomeadamente as que se referem ao tratamento de dados biométricos, assim como outras, como o acompanhamento por dispositivos móveis.

Embora tais sistemas possam constituir uma importante componente de uma pista de auditoria de um empregador, colocam também o risco de proporcionar um nível de conhecimento e controlo invasivo das atividades do empregado no local de trabalho.

**Exemplo:**

Um empregador mantém uma sala com servidores onde os dados empresariais sensíveis, os dados pessoais relativos aos empregados e os dados pessoais relativos aos clientes são armazenados em formato digital. A fim de cumprir as obrigações jurídicas para proteger os dados contra o acesso não autorizado, o empregador tinha instalado um sistema de controlo de acesso que regista a entrada e a saída dos empregados que têm a devida autorização para entrar na sala. Caso qualquer peça de equipamento venha a desaparecer ou os dados sejam suscetíveis de acesso não autorizado, perda ou furto, os registos mantidos pelo empregador não lhe permite determinar quem teve acesso à sala nessa altura.

Dado que o tratamento é necessário e não prevalece o direito ao respeito da vida privada dos empregados, pode ser no interesse legítimo na aceção do artigo 7.º, alínea f), se os empregados foram adequadamente informados sobre a operação do tratamento. No entanto, a monitorização contínua da frequência e da entrada e da saída exatas dos empregados não pode ser justificada, se esses dados forem também utilizados para outros fins, como, por exemplo, a avaliação do desempenho dos empregados.

## 5.6 Operações de tratamento que utilizam sistemas de vídeo de monitorização

Os sistemas de monitorização e vigilância por vídeo continuam a colocar problemas semelhantes em matéria de privacidade dos empregados, como anteriormente: a capacidade de captar de forma contínua o comportamento do trabalhador<sup>19</sup>. As alterações mais relevantes relativas à aplicação desta tecnologia no contexto laboral são a capacidade de acesso a dados recolhidos facilmente à distância (por exemplo, através de um telemóvel inteligente); a redução da dimensão das câmaras (juntamente com o aumento das suas capacidades, por exemplo, a alta definição); e o tratamento que pode ser realizado mediante novas análises de vídeo.

Com as capacidades dadas pelas análises de vídeo, é possível que um empregador monitorize as expressões faciais do trabalhador por meios automatizados, a fim de identificar desvios de padrões de circulação predefinidos (por exemplo, em contexto fabril), e mais. Tal seria desproporcional em relação a direitos e liberdades dos empregados e, por conseguinte, ilícito, de um modo geral. O tratamento também é suscetível de envolver, eventualmente, os perfis e a tomada de decisões automatizadas. Por conseguinte, os empregadores devem abster-se de utilizar tecnologias de reconhecimento facial. Pode haver alguma margem de exceção a esta regra, mas estes cenários não podem ser utilizados para invocar uma legitimação geral da utilização de tal tecnologia<sup>20</sup>.

## 5.7 Operações de tratamento que envolvem veículos utilizados pelos empregados

As tecnologias que permitem aos empregadores a monitorização dos seus veículos passaram a ser amplamente adotadas, nomeadamente entre organizações cujas atividades envolvem o transporte ou têm frotas de veículos significativas.

Qualquer empregador que utilize telemática para veículos estará a recolher dados sobre o veículo e sobre cada empregado que o conduz. Estes dados podem incluir não só a localização do veículo (e, portanto, do empregado) recolhida pelos sistemas de localização GPS básicos, mas também, dependendo da tecnologia, uma grande quantidade de informações, que incluem o comportamento de condução. Existem determinadas tecnologias que também podem permitir uma monitorização contínua tanto do veículo como do condutor (por exemplo, os aparelhos de registo de ocorrências).

Um empregador poderá ser obrigado a instalar tecnologia de localização nos veículos para demonstrar o cumprimento de outras obrigações jurídicas como, por exemplo, garantir a segurança dos empregados que conduzem esses veículos. O empregador pode também ter um interesse legítimo em poder localizar os veículos a qualquer momento. Ainda que os empregadores tivessem um interesse legítimo para atingir estes fins, em primeiro lugar, deve ser apreciada a questão de saber se o tratamento é necessário para esses fins, e se a aplicação atual está em conformidade com os princípios da proporcionalidade e da subsidiariedade. Quando a utilização de um veículo privado profissional é autorizada, a medida mais importante que um empregador pode tomar para garantir o cumprimento destes princípios é

---

<sup>19</sup> Ver supra o processo em referência de *Köpke contra a Alemanha*; além disso, há ainda a assinalar que, em determinadas jurisdições, a instalação de sistemas, como as câmaras de televisão em circuito fechado para comprovar a existência de um comportamento ilícito, teve a respetiva autorização; ver o processo *Bershka* no Tribunal Constitucional de Espanha.

<sup>20</sup> Além disso, nos termos do RGPD, o tratamento de dados biométricos para efeitos de identificação deve basear-se numa exceção prevista pelo artigo 9.º, n.º 2.

oferecer uma opção de exclusão: o empregado deverá, em princípio, ter a possibilidade de, temporariamente, desligar o sistema de localização quando circunstâncias especiais o justificarem desligar, tais como uma consulta médica. Deste modo, o empregado pode, por sua própria iniciativa, proteger determinados dados de localização como privados. O empregador deve garantir que os dados recolhidos não são utilizados para tratamento posterior ilegítimo, tal como o acompanhamento e a avaliação dos empregados.

O empregador deve também informar claramente os empregados de que um dispositivo de localização foi instalado num veículo de empresa que conduzem, e que os seus movimentos são registados, durante todo o período de utilização do referido veículo (e que, dependendo da tecnologia em causa, o seu comportamento de condução pode também ser registado). De preferência, tais informações devem ser apresentadas de forma muito visível em todos os veículos, ao alcance da visão do condutor.

É possível que os empregados utilizem os veículos de empresa fora do horário de trabalho, por exemplo, para utilização pessoal, dependendo das políticas específicas que regem a utilização desses veículos. Dado o carácter sensível dos dados de localização, é pouco provável que exista uma base jurídica para a monitorização da localização dos veículos dos empregados fora do horário de trabalho acordado. No entanto, na existência dessa necessidade, deve ser considerada uma aplicação que seja proporcional aos riscos. Por exemplo, tal pode significar que, para prevenir o furto de veículos, a localização do referido veículo não deve estar registada fora do horário de trabalho, a menos que o veículo saia para um percurso mais longo definido (região ou mesmo país). Além disso, a localização só poderá ser indicada em forma de «plano de emergência»: o empregador apenas pode ativar a «visibilidade» da localização, acedendo a dados já armazenados pelo sistema, quando o veículo sai para uma região predefinida.

Tal como referido no *Parecer 13/2011 do GT 29 sobre serviços de geolocalização em dispositivos móveis inteligentes*<sup>21</sup>:

«Os dispositivos de localização de veículos não são dispositivos de localização do pessoal. A sua função é determinar ou monitorizar a localização dos veículos em que são instalados. Os empregadores não devem considerá-los como dispositivos de localização ou monitorização do comportamento ou do paradeiro dos condutores ou outros empregados, nomeadamente enviando alertas relacionados com a velocidade do veículo.»

Além disso, tal como afirmado no *Parecer 5/2005 do GT 29 sobre a utilização de dados de localização para criar serviços de valor acrescentado*<sup>22</sup>:

«O tratamento de dados de localização pode justificar-se se for efetuado para monitorizar o transporte de pessoas ou bens ou para melhorar a distribuição de recursos com vista à prestação de serviços em locais isolados (por exemplo, para planificar operações em tempo real), ou quando exista um objetivo de segurança relacionado com o próprio empregado ou com os bens ou veículos a seu cargo. Em contrapartida, o Grupo de Trabalho considera o

<sup>21</sup> GT 29, *Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes*, GT 185, 16 de maio de 2011, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_pt.pdf)

<sup>22</sup> GT 29, *Parecer 5/2005 sobre a utilização de dados de localização para criar serviços de valor acrescentado*, GT 115, 25 de novembro de 2005, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115\\_pt.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_pt.pdf)

tratamento de dados excessivo sempre que os empregados sejam livres de organizar a sua viagem ou quando este seja efetuado com o objetivo único de vigiar o trabalho de um empregado e esse desempenho possa ser aferido por outros meios.»

### **5.7.1 APARELHOS DE REGISTO DE OCORRÊNCIAS**

Os aparelhos de registo de ocorrências dotam o empregador com a capacidade técnica de tratamento de uma quantidade significativa de dados pessoais sobre os empregados que conduzem veículos de empresa. Tais dispositivos são cada vez mais instalados em veículos com o objetivo de registar ocorrências de vídeo, incluindo, eventualmente, som, em caso de acidente. Estes sistemas estão em condições de registar em determinadas alturas, por exemplo, em resposta a travagem brusca, mudanças bruscas de direção ou acidentes, sempre que os momentos imediatamente anteriores ao incidente sejam armazenados, mas também podem ser definidos para uma monitorização contínua. Estas informações podem ser utilizadas posteriormente para observar e analisar o comportamento de condução de uma pessoa com o objetivo de o melhorar. Além disso, muitos destes sistemas integram GPS para acompanhar a localização do veículo em tempo real e outros dados correspondentes à condução (tais como a velocidade do veículo) podem ser igualmente armazenados para tratamento posterior.

Estes dispositivos tornaram-se particularmente frequentes entre organizações cujas atividades envolvem transporte ou têm frotas de veículos significativas. No entanto, a implantação de aparelhos de registo de ocorrências só pode ser lícita, se existir uma necessidade de tratar os dados pessoais sobre os empregados, decorrente de uma finalidade legítima e se o tratamento estiver conforme com os princípios da proporcionalidade e da subsidiariedade.

#### **Exemplo**

Uma empresa de transportes equipa todos os seus veículos com uma câmara de vídeo no interior da cabina, que regista som e vídeo. O objetivo do tratamento destes dados é melhorar as competências de condução dos empregados. As câmaras são configuradas para conservar registos sempre que ocorram incidentes, como a travagem brusca ou as mudanças bruscas de direção. A empresa assume que dispõe de um fundamento jurídico para o tratamento, no seu interesse legítimo, nos termos do artigo 7.º, alínea f), da diretiva, para proteger a segurança dos seus empregados e a de outros condutores.

No entanto, o interesse legítimo da empresa para monitorizar os condutores não prevalece sobre os direitos dos referidos condutores para a proteção dos seus dados pessoais. A monitorização contínua dos empregados com estas câmaras constitui uma grave interferência com o direito à privacidade. Existem outros métodos (por exemplo, a instalação de equipamentos que impedem a utilização de telemóveis), bem como outros sistemas de segurança, como o sistema avançado de travagem de emergência ou o sistema de aviso de afastamento da faixa de rodagem, que podem ser utilizados para efeitos de prevenção de acidentes rodoviários, que poderão ser mais adequados. Além disso, tal registo de vídeo tem uma elevada probabilidade de resultar no tratamento de dados pessoais de terceiros (tais como os peões) e, para esse tratamento, o interesse legítimo da empresa não é suficiente para justificar o tratamento.

### **5.8 Operações de tratamento que envolvem a divulgação de dados dos empregados a terceiros**

Tem-se tornado cada vez mais comum para as empresas transmitir os dados dos seus empregados, para efeitos de garantia da prestação fiável dos serviços. Estes dados podem ser bastante excessivos, dependendo do âmbito dos serviços prestados (por exemplo, a fotografia de um empregado pode ser incluída). No entanto, os empregados não estão em posição de, dado o desequilíbrio de poderes, dar o seu livre consentimento para o tratamento dos seus dados pessoais pelo seu empregador e, se o tratamento de dados não é proporcional, o empregador não tem fundamento jurídico.

**Exemplo:**

Uma empresa de entregas envia aos seus clientes uma mensagem de correio eletrónico com uma ligação para o nome e a localização da pessoa que faz a entrega (empregado). A empresa também pretendeu fornecer uma fotografia do passaporte da pessoa que faz a entrega. A empresa partiu do princípio de que teria um fundamento jurídico para o tratamento, no seu interesse legítimo (artigo 7.º, alínea f), da Diretiva), permitindo ao cliente verificar se a pessoa que faz a entrega é efetivamente a pessoa certa.

No entanto, não é necessário fornecer o nome e a fotografia da pessoa que faz a entrega aos clientes. Uma vez que não existe outro fundamento legítimo para este tratamento, a empresa de entregas não está autorizada a fornecer esses dados pessoais aos clientes.

## **5.9 Operações de tratamento que envolvem transferências internacionais de dados de RH e de outros empregados**

Os empregadores estão a utilizar cada vez mais aplicações e serviços baseados na computação em nuvem, tais como os que são concebidos para o tratamento de dados de RH e as aplicações de escritório em linha. A utilização da maior parte destas aplicações terá como resultado a transferência internacional de dados relativos aos empregados. Como já foi sublinhado no Parecer 8/2001, o artigo 25.º da referida diretiva precisa que as transferências de dados pessoais para um país terceiro só podem realizar-se se esse país assegurar um nível de proteção adequado. Seja a que título for, a transferência deve satisfazer as disposições da diretiva.

Deverá, assim, garantir-se que estas disposições relativas à transferência internacional de dados são conformes. O GT 29 reitera a sua posição anterior de que é preferível invocar uma proteção adequada, em vez de as derrogações enumeradas no artigo 26.º da Diretiva «Proteção de Dados»; Nos casos em que o consentimento é invocado, deve ser específico, inequívoco e de livre vontade. No entanto, deve também ser garantido que os dados partilhados fora da UE/EEE e o posterior acesso por outras entidades dentro do grupo continuem a ser limitados ao mínimo estritamente necessário para os fins previstos.

## **6. Conclusões e recomendações**

### **6.1 Direitos fundamentais**

O conteúdo das comunicações supra e os dados de tráfego relativos a essas comunicações gozam da mesma proteção dos direitos fundamentais como comunicações «análogas».

As comunicações eletrónicas efetuadas a partir de estabelecimentos comerciais podem ser abrangidas pelos conceitos de «vida privada» e de «correspondência», na aceção do artigo

8.º, ponto 1, da Convenção Europeia. Com base na atual Diretiva «Proteção de Dados», os empregadores apenas podem recolher dados para finalidades legítimas, com o tratamento a ser realizado em condições adequadas (por exemplo, proporcionais e necessárias, de interesse real e atual, de uma forma lícita, articulada e transparente), com uma base jurídica para o tratamento de dados pessoais recolhidos ou gerados através de comunicações eletrónicas.

O facto de um empregador ter a titularidade dos meios eletrónicos não exclui o direito dos empregados à confidencialidade das suas comunicações e dos dados relacionados com a localização e a correspondência. O acompanhamento da localização dos empregados através dos seus próprios dispositivos ou daqueles entregues pela empresa deve ser limitado nos casos em que tal seja estritamente necessário para uma finalidade legítima. É certo que, no caso do «BYOD», é importante que os empregados tenham a possibilidade de proteger as suas comunicações privadas de qualquer monitorização relacionada com o trabalho.

## **6.2 Consentimento; interesse legítimo**

Os empregados raramente estão em posição de dar, recusar ou revogar livremente o consentimento, dada a dependência que resulta da relação entre empregador e empregado. Tendo em conta o desequilíbrio de poderes, os empregados só podem dar o seu livre consentimento em circunstâncias excecionais, quando as consequências não tiverem qualquer tipo de relação com a aceitação ou a rejeição de uma oferta.

O interesse legítimo dos empregadores pode, por vezes, ser invocado como fundamento jurídico, mas apenas se o tratamento for estritamente necessário para uma finalidade legítima e estiver conforme com os princípios da proporcionalidade e da subsidiariedade. Um teste de proporcionalidade deve ser efetuado antes da implantação de qualquer ferramenta de monitorização, a fim de verificar se todos os dados são necessários, se esse tratamento excede os direitos de privacidade gerais que os empregados têm também no local de trabalho e quais as medidas que devem ser tomadas para garantir que as violações do direito à vida privada e do direito à confidencialidade das comunicações são limitadas ao mínimo estritamente necessário.

## **6.3 Transparência**

Deve ser feita uma comunicação eficaz aos empregados em relação a qualquer monitorização realizada, à finalidade e às circunstâncias desta monitorização, bem como às possibilidades de impedirem que os seus dados sejam recolhidos por tecnologias de monitorização. As políticas e as regras em matéria de monitorização legítima devem ser claras e facilmente acessíveis. O Grupo de Trabalho recomenda o envolvimento de uma amostra representativa dos empregados na criação e na avaliação dessas regras e políticas, uma vez que a maior parte da monitorização pode atentar contra a vida privada dos empregados.

## **6.4 Proporcionalidade e minimização dos dados**

O tratamento de dados no local de trabalho deve ser uma resposta proporcional aos riscos enfrentados por um empregador. Por exemplo, a utilização abusiva da *Internet* pode ser detetada sem a necessidade de analisar o conteúdo do sítio *Web*. Se a utilização abusiva pode ser impedida (por exemplo, mediante a utilização de filtros de *Internet*), o empregador não tem qualquer direito geral à monitorização.

Além disso, uma proibição generalizada da comunicação é impraticável, por razões pessoais, e a execução pode exigir um nível de monitorização que pode ser desproporcional. A prevenção deve ter muito mais peso do que a deteção: os interesses do empregador são mais bem servidos ao prevenir a utilização abusiva da *Internet* através de meios técnicos, do que ao despende recursos em matéria de deteção de abusos.

As informações registadas a partir da monitorização contínua e as informações que são apresentadas ao empregador devem ser reduzidas ao mínimo possível. Os empregados devem ter a possibilidade de, temporariamente, desligar o sistema de localização quando circunstâncias especiais o justificarem. As soluções que, por exemplo, permitem a localização de veículos, podem ser concebidas para registar os dados relativos à posição sem os apresentar ao empregador.

Os empregadores devem ter em conta o princípio da minimização de dados no momento da decisão sobre a implantação de novas tecnologias. As informações devem ser conservadas durante o prazo mínimo e necessário com um período de retenção especificado. Sempre que as informações deixem de ser necessárias, devem ser eliminadas.

### **6.5 Serviços de computação em nuvem, aplicações em linha e transferências internacionais**

Sempre que os empregados devam utilizar as aplicações em linha que tratam dados pessoais (tais como as aplicações de escritório), os empregadores devem considerar permitir aos empregados a designação de determinados espaços privados, aos quais o empregador não pode ter acesso em nenhuma circunstância, tal como uma mensagem de correio eletrónico privada ou uma pasta com documentos.

A utilização da maior parte das aplicações em nuvem irá resultar na transferência internacional de dados dos empregados. Deve garantir-se que os dados pessoais transferidos para um país terceiro fora da UE só se realiza nos casos em que seja garantido um nível de proteção adequado e que os dados partilhados fora da UE/EEE e o posterior acesso por outras entidades dentro do grupo continuem a ser limitados ao mínimo necessário para os fins previstos.

\* \* \*

Feito em Bruxelas, em 8 de junho de 2017

*Pelo Grupo de Trabalho,  
A Presidente  
Isabelle FALQUE-PIERROTIN*