Declaração

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Declaração sobre o tratamento de dados pessoais no contexto do surto de COVID-19.

Adotada em 19 de março de 2020

O Comité Europeu para a Proteção de Dados adotou a seguinte declaração:

Os governos, assim como as organizações públicas e privadas de toda a Europa, têm estado a tomar medidas para conter e atenuar o surto de COVID-19, que podem implicar o tratamento de vários tipos de dados pessoais.

As normas em matéria de proteção de dados (como o Regulamento Geral sobre a Proteção de Dados) não obstam a que sejam adotadas medidas para combater a pandemia de coronavírus. A luta contra as doenças transmissíveis é um objetivo primordial partilhado por todas as nações, devendo ser apoiada da melhor forma possível. A humanidade tem interesse em travar a propagação de doenças e em utilizar técnicas modernas na luta contra os flagelos que afetam grande parte do mundo. Ainda assim, o Comité Europeu para a Proteção de Dados gostaria de sublinhar que, mesmo nestes tempos de exceção, os responsáveis pelo tratamento dos dados e os subcontratantes devem assegurar a proteção dos dados pessoais dos respetivos titulares. Por conseguinte, há que ter em conta uma série de considerações para garantir o tratamento lícito dos dados pessoais e ter sempre presente que qualquer medida tomada neste contexto deve respeitar os princípios gerais de direito, não podendo ser irreversível. Esta emergência pode legitimar a imposição de restrições às liberdades, desde que sejam proporcionadas e limitadas ao período de emergência.

1. Licitude do tratamento

O Regulamento Geral sobre a Proteção de Dados (RGPD) é um diploma legislativo genérico que prevê regras aplicáveis igualmente ao tratamento de dados pessoais num contexto como o do surto de COVID-19. **Permite que as autoridades competentes em matéria de saúde pública e os empregadores procedam ao tratamento de dados pessoais no contexto de uma epidemia, em conformidade com o direito nacional e nas condições nele estabelecidas**, por exemplo, se o

tratamento for necessário por motivos de interesse público importante no domínio da saúde pública. Nessas circunstâncias, não é necessário obter o consentimento dos particulares.

1.1 No que diz respeito ao tratamento de dados pessoais, incluindo das categorias especiais de dados, por parte das autoridades públicas competentes (por exemplo, as autoridades de saúde pública), o Comité Europeu para a Proteção de Dados considera que os artigos 6.º e 9.º do RGPD permitem o tratamento de dados pessoais, em especial quando esse tratamento se inserir no mandato legal das autoridades públicas, em conformidade com a legislação nacional e nas condições previstas no referido regulamento.

1.2 No contexto das relações laborais, o tratamento de dados pessoais pode ser necessário para cumprir obrigações legais a que o empregador esteja sujeito, nomeadamente obrigações em matéria de saúde e segurança no local de trabalho, ou por razões de interesse público, como o controlo de doenças e de outras ameaças à saúde. O RGPD prevê igualmente derrogações à proibição de tratamento de determinadas categorias especiais de dados pessoais, como os dados relativos à saúde, quando tal seja necessário por motivos de interesse público importante no domínio da saúde pública [artigo 9.º, n.º 2.º, alínea i)], com base no direito da União ou no direito nacional, ou quando seja necessário proteger os interesses vitais do titular dos dados [artigo 9.º, n.º 2.º, alínea c)], uma vez que o considerando 46 refere explicitamente o controlo de uma epidemia.

1.3 No que diz respeito ao tratamento de dados de telecomunicações, **tais como os dados de localização**, tem de ser igualmente cumprida a legislação nacional que aplica a Diretiva Privacidade Eletrónica. Em princípio, os dados de localização só podem ser utilizados pelo operador se forem tornados anónimos ou se tiver sido obtido o consentimento da pessoa em causa. No entanto, o artigo 15.º da **Diretiva Privacidade Eletrónica permite que os Estados-Membros introduzam medidas legislativas para salvaguardar a segurança pública**. Essa legislação excecional só é autorizada **se** constituir uma medida **necessária, adequada e proporcionada numa sociedade democrática**. Estas medidas devem ser conformes com a Carta dos Direitos Fundamentais e com a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Devem, além disso, ser **sujeitas ao controlo judicial do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos Humanos**. No caso de uma situação de emergência, devem também ser estritamente limitadas ao período que durar a emergência.

2. Princípios fundamentais em matéria de tratamento de dados pessoais

Os dados pessoais necessários para atingir os objetivos visados devem ser tratados para finalidades específicas e explícitas.

Além disso, os titulares dos dados devem receber informações transparentes sobre as atividades de tratamento levadas a cabo e as suas principais características, incluindo o período de conservação dos dados recolhidos e as finalidades do tratamento. As informações fornecidas devem ser facilmente acessíveis e redigidas numa linguagem clara e simples.

É importante adotar medidas de segurança adequadas e políticas de confidencialidade que garantam que os dados pessoais não são divulgados a pessoas não autorizadas. As medidas adotadas para gerir a situação de emergência atual e o processo decisório subjacente devem ser devidamente documentados.

3. Utilização de dados de localização dos dispositivos móveis

- **Podem os governos dos Estados-Membros utilizar os dados pessoais relativos aos telemóveis particulares para monitorizar, conter ou atenuar a propagação da COVID-19?**

Em alguns Estados-Membros, os governos pretendem utilizar os dados de localização dos dispositivos móveis como forma de monitorizar, conter ou atenuar a propagação da COVID-19. Isto poderá implicar, por exemplo, a possibilidade de geolocalização das pessoas ou o envio de mensagens de saúde pública às pessoas que se encontrem numa determinada área, por telefone ou mensagem de texto. **As autoridades públicas devem, em primeiro lugar, procurar tratar os dados de localização de forma anónima (ou seja, tratá-los agregados, de forma a que as pessoas não possam ser identificadas), o que permitiria obter relatórios sobre a concentração de dispositivos móveis num determinado local («cartografia»).**

As regras de proteção dos dados pessoais não se aplicam aos dados que tenham sido adequadamente anonimizados.

Se **não for possível tratar apenas dados anónimos, a** Diretiva Privacidade Eletrónica **permite aos Estados-Membros adotar medidas legislativas para salvaguardar a segurança pública** (artigo 15.º)**.**

Se forem adotadas medidas que permitam tratar dados de localização não anonimizados, o Estado-Membro deverá estabelecer as **salvaguardas adequadas**, nomeadamente proporcionar aos consumidores dos serviços de comunicações eletrónicas o **direito de recorrer aos tribunais**.

O princípio da proporcionalidade é igualmente aplicável. Dado o objetivo específico a atingir, devem ser sempre preferidas as soluções menos intrusivas. As medidas mais invasivas, como o «rastreio» de indivíduos (ou seja, o tratamento de dados históricos de localização não anonimizados), poderão ser consideradas proporcionais em determinadas circunstâncias e em função das modalidades concretas do tratamento dos dados. No entanto, devem ser objeto de maior escrutínio e prever salvaguardas para assegurar o respeito dos princípios de proteção de dados (proporcionalidade da medida em termos de duração e âmbito, conservação dos dados por um período limitado e restrição da finalidade).

4. Relações laborais

- **Pode um empregador exigir que os visitantes ou empregados forneçam informações específicas em matéria de saúde no contexto do surto de COVID-19?**

A aplicação do princípio da proporcionalidade e da minimização dos dados é particularmente relevante neste contexto. O empregador só deve exigir informações sanitárias na medida em que o direito nacional o permita.

- **Pode um empregador realizar exames médicos aos seus empregados?**

A resposta reside nas legislações nacionais em matéria de emprego ou de saúde e segurança. Os empregadores só devem ter acesso e tratar dados relativos à saúde dos seus empregados se alguma obrigação legal o impuser.

- **Pode um empregador revelar que um trabalhador está infetado com a COVID-19 aos seus colegas ou a outras pessoas?**

Os empregadores devem informar o pessoal sobre os casos de COVID-19 e tomar medidas de proteção, mas não devem comunicar mais informações do que aquelas que se mostrem necessárias. Nos casos em que seja necessário revelar os nomes dos trabalhadores que contraíram o vírus (por exemplo, num contexto preventivo) e a legislação nacional o permitir, os trabalhadores em causa devem ser antecipadamente informados e a sua dignidade e integridade protegidas.

- **Que informações tratadas no contexto do surto de COVID-19 podem ser obtidas pelos empregadores?**

Os empregadores podem obter informações pessoais para cumprir as respetivas obrigações e organizar o trabalho em conformidade com a legislação nacional.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)