VI.
Dados Pessoais

Glossário

CEPD

Comité Europeu para a Proteção de Dados

CNPD

Comissão Nacional de Proteção de Dados

Decreto-Lei n.º 20/2020

Decreto-Lei n.º 20/2020, de 1 de maio, altera as medidas excecionais e temporárias relativas à pandemia da doença COVID-19

Diretiva *E-Privacy*

Diretiva n.º 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas

Lei n.º 1-A/2020

Lei n.º 1-A/2020, de 19 de março, medidas excecionais e temporárias de resposta à situação epidemiológica provocada pelo coronavírus SARS-CoV-2 e da doença COVID-19

Lei n.º 58/2019

Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD (Regulamento (UE) 2016/679 do Parlamento 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)

Lei da Proteção de Dados e da Privacidade nas das Comunicações Eletrónicas

Lei n.º 41/2004, de 18 de agosto, que transpõe para a ordem jurídica nacional a **Diretiva E-Privacy** (Diretiva n.º 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas)

Lei de Bases da Saúde

Lei n.º 95/2019, de 4 de setembro

RGPD

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 Pessoais)

RJPSST

Regime Jurídico da Promoção da Segurança e Saúde no Trabalho (aprovado pela Lei n.º 102/2009, de 10 de setembro)

SST

Segurança e Saúde no Trabalho

VI. DADOS PESSOAIS

VI.A. Enquadramento prévio

Em matéria de proteção de dados pessoais, têm surgido questões sobre a forma como podem ser adotadas medidas preventivas e de mitigação do vírus, conformes com as previsões do RGPD, porquanto a perigosidade e a rapidez com que a pandemia tem evoluído requerem medidas rápidas e, em alguns casos, recolhas de dados pessoais que, numa situação de normalidade, não seriam necessárias. Em discussão encontram-se opções como as medições obrigatórias de temperatura no acesso a instalações (e, muito em particular, em contexto laboral), instalação de câmaras termográficas, utilização de dados de localização e monitorização de contactos entre pessoas singulares, entre outros temas.

No dia 16 de março, a Presidente do CEPD pronunciou-se sobre a proteção de dados pessoais no atual contexto[1]. De acordo com Andrea Jelinek, o RGPD não impede a adoção de medidas relacionadas com a prevenção e combate ao vírus que impliquem o tratamento de dados pessoais – sendo que este prevê, inclusivamente, o tratamento de dados em situações como a que agora vivemos –, mas que o mesmo deve continuar a ser cumprido. É, portanto, imperativo, que as medidas adotadas e a adotar estejam de acordo com a legislação na matéria, e que não haja, nesta fase e nas fases subsequentes, recolhas de dados excessivas, com prejuízo para os direitos dos titulares dos dados.

No final do mês de abril, o CEPD emitiu ainda orientações sobre o tratamento de dados relativos à saúde, para fins de investigação científica no contexto do surto da COVID-19[2].

VI.B. Tratamento de dados pessoais em contexto laboral: condição de licitude

IDENTIFICAÇÃO DO PROBLEMA

Várias questões têm sido suscitadas sobre o tratamento de dados pessoais de trabalhadores, no quadro das medidas de prevenção e combate à pandemia COVID-19 em contexto laboral, na medida em que parte das ações requer o tratamento de dados de saúde, o que reveste especial sensibilidade e está, consequentemente, sujeito a um regime particularmente exigente nos termos do RGPD. Desde o primeiro momento colocaram-se questões sobre práticas como as enumeradas de seguida:

- Questionários dirigidos a trabalhadores, visitantes e familiares sobre deslocações recentes e verificação de sintomas;
- Imposição aos trabalhadores da obrigatoriedade de informar o empregador sobre a existência de trabalhadores considerados "casos suspeitos" ou "confirmados" de infeção pelo vírus;
- Divulgação de informação a todos os trabalhadores a respeito da existência de "casos suspeitos" ou de pessoas infetadas entre os trabalhadores;
- Medição de temperatura de trabalhadores e visitantes, incluindo medição por recurso a câmaras termográficas.

ENQUADRAMENTO E POSSÍVEIS SOLUÇÕES

O tratamento de dados de saúde (*e.g.*, para efeitos de aferir se uma pessoa identificada ou identificável está infetada ou é um "caso suspeito") apenas pode ter lugar se estiver verificada uma das exceções taxativamente

(1) Disponível https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en.

(2) "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak", emitidas em 21-04-2020, disponíveis aqui (versão com pequenas correções feitas em 30-04-2020).

previstas no n.º 2 do artigo 9.º do RGPD, proibindo o n.º 1 o tratamento de dados de saúde (e de outras categorias especiais de dados), a não ser que alguma destas exceções (derrogações) se verifique. As derrogações previstas nas alíneas *b)* e *h)* do n.º 2 – dependendo das circunstâncias do caso concreto – podem ser, potencialmente, convocadas, legitimando o tratamento de dados de saúde no âmbito laboral.

Com efeito, nos termos da alínea *b)*, pode haver tratamento de dados de saúde "[s]e o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados".

Ora, a obrigação de assegurar um espaço de trabalho saudável recai sobre os empregadores, nos termos do RJPSST que prescreve que o empregador deve assegurar ao trabalhador condições de segurança e de saúde em todos os aspetos do seu trabalho. Logo, a recolha dos dados de saúde tendo em vista a adoção de medidas preventivas e de contenção (*e.g.*, monitorização de trabalhadores com sintomas de infeção), incluindo no contexto do gradual levantamento de medidas de confinamento no âmbito do combate à pandemia, tem respaldo no cumprimento daquela obrigação legal.

O tratamento de dados no âmbito laboral pode ainda ter fundamento, ainda que em menor número de casos, nos fins previstos na alínea *h)* (ou seja, "[p]ara efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social"). Nos termos do n.º 2 do artigo 29.º da Lei n.º 58/2019, "[n]os casos previstos nas alíneas *h)* e *i)* do n.º 2 do artigo 9.º do RGPD, o tratamento dos dados previstos no n.º 1 do mesmo artigo deve ser efetuado por um profissional obrigado a sigilo ou por outra pessoa sujeita a dever de confidencialidade, devendo ser garantidas medidas adequadas de segurança da informação".

Devemos, assim, ter em conta que: a par do CEPD, várias Autoridades de Controlo se pronunciaram sobre o tratamento de dados pessoais, à luz do RGPD, no atual contexto de pandemia. Analisando o referido por várias Autoridades de Controlo, como por exemplo, Espanha, Itália, Reino Unido, Irlanda, França e também Portugal, conclui-se que:

- As medidas a implementar devem ter em consideração – à luz dos princípios da necessidade e da proporcionalidade – as caraterísticas particulares de cada organização (*e.g.*, tipo de atividade, pessoas com fatores de risco) e devem ser escolhidas as medidas que impliquem o mínimo de intrusão possível, evitando, sempre que possível, a recolha de categorias especiais de dados;
- As medidas devem ser necessárias e proporcionais, sendo adotadas a fim de assegurar o respeito do princípio da minimização e mediante informação a todos os titulares dos dados, em cumprimento do princípio da transparência;
- Devem ser evitadas recolhas generalizadas e sistemáticas de dados pessoais, sem que as mesmas sejam justificadas (*e.g.*, medição obrigatória de temperatura e envio para os superiores hierárquicos), devendo seguir-se de perto as instruções das autoridades competentes;
- As medidas adotadas não devem exceder os limites indicados pelas autoridades competentes;
- Os dados devem permanecer, tanto quanto possível, confidenciais, não devendo, em

princípio, e a não ser que tal se revele estritamente necessário, ser identificados os trabalhadores infetados ou que constituam um caso suspeito junto de todos os trabalhadores ou devendo proceder-se a essa identificação perante o número de trabalhadores estritamente necessário para aferir o risco de contágio ou determinar medidas de quarentena;
- Deve haver canais específicos para que a informação possa circular no seio da empresa, apenas acedendo à mesma colaboradores vinculados a deveres de confidencialidade e na medida do estritamente necessário.

A CNPD emitiu orientações sobre o tratamento daqueles dados em contexto laboral[3] nas quais refere, concretamente que os empregadores não devem, eles próprios, proceder ao tratamento de dados relativos à saúde dos trabalhadores (incluindo a recolha e registo da temperatura corporal) ou relativos a eventuais situações ou comportamentos de risco destes (suscetíveis de indiciar infeção pelo novo coronavírus), indicando a CNPD que deve ser no contexto da medicina no trabalho que poderá proceder-se ao tratamento de dados desta natureza.

Nesse contexto, os profissionais de saúde podem:

(i) Avaliar o estado de saúde dos trabalhadores;
(ii) Obter as informações necessárias para avaliar a aptidão para o trabalho conforme com regras de SST; e
(iii) Adotar os procedimentos adequados a salvaguardar a saúde dos próprios e de terceiros, sempre que identifiquem trabalhadores com sintomas ou em outras situações que o justifiquem.

A **frequência** e o **tipo de avaliação** deve ser determinada por aqueles profissionais de saúde, de acordo com: (*i*) critérios científicos que presidem às suas decisões clínicas; e (*ii*) orientações da autoridade nacional de saúde.

A CNPD sublinha que os empregadores se devem limitar a atuar de acordo com as orientações da autoridade nacional de saúde para a prevenção de contágio pelo novo coronavírus no contexto laboral e que se devem abster de adotar iniciativas que impliquem a recolha de dados pessoais de saúde dos seus trabalhadores quando as mesmas não tenham base legal, nem tenham sido ordenadas pelas autoridades administrativas competentes.

Posteriormente, e contrariando as orientações da CNPD, o Decreto-Lei n.º 20/2020, que altera as medidas excecionais e temporárias relativas à pandemia provocada pela doença COVID-19, veio admitir, nos termos previstos no seu artigo 13.º-C, a medição de temperatura corporal de trabalhadores.

De acordo com o n.º 1 da disposição "[n]o atual contexto da doença COVID-19, e exclusivamente por motivos de proteção da saúde do próprio e de terceiros, podem ser realizadas medições de temperatura corporal a trabalhadores para efeitos de acesso e permanência no local de trabalho". Prevê, todavia, o n.º 2 da disposição que é "expressamente proibido o registo da temperatura corporal associado à identidade da pessoa, salvo com expressa autorização da mesma", sendo que, de acordo com o n.º 3, "[c]aso haja medições de temperatura superiores à normal temperatura corporal, pode ser impedido o acesso dessa pessoa ao local de trabalho".

Em suma: pode haver medições de temperatura, impedindo o trabalhador de entrar no local de trabalho, porém, não pode haver registo, a não ser que haja consentimento do trabalhador. Questiona-se, no entanto, de que forma pode ser documentado o impedimento em aceder ao local de trabalho, porquanto não poderá ser feito sem que haja a indicação de que o trabalhador tinha,

[3] Orientações da CNPD emitidas em 23-04-2020, sobre recolha de dados de saúde e da vida privada de trabalhadores no contexto da pandemia (disponíveis aqui).

no dia em questão, uma temperatura corporal superior ao normal, sendo assim necessário que se mantenha um registo de que nesse dia o trabalhador não foi autorizado a entrar nas instalações por esse motivo. Salientamos que, pedir consentimento aos trabalhadores para que os seus dados sejam registados – e não vemos que a expressão "salvo expressa autorização da mesma" possa ter diferente interpretação – não nos parece legitimar o tratamento, na medida em que, em virtude da existência de uma relação de subordinação e desigualdade congénita no binómio "empregador-trabalhador", o consentimento assim obtido dificilmente poderá ter-se como válido.

Sem prejuízo de não se aplicar o previsto no n.º 3 do artigo 28.º da Lei n.º 58/2019, que elenca dois casos em que o consentimento não pode fundamentar o tratamento de dados pessoais de trabalhadores, parece que também no caso em análise não poderia este registo de dados (temperatura corporal do trabalhador) assentar no consentimento deste, enquanto fundamento de licitude (ou derrogação da proibição) para o tratamento, na medida em que dificilmente constituirá consentimento conforme com o exigido pelo RGPD, de acordo com o qual o consentimento deve ser uma "manifestação de vontade, livre, específica, informada e explícita (inequívoca), pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[4]. Nesse sentido, admite-se que, caso a temperatura seja superior ao normal, para que o trabalhador seja impedido de aceder ao seu local de trabalho, possa ter de haver intervenção dos serviços de STT.

Por outro lado, deveria o legislador ter indicado quais os métodos através dos quais pode ser feita a medição de temperatura; *e.g.* a medição através de câmaras termográficas pode integrar a previsão da norma?

[4] *Cf.* artigo 4.º, 11), do RGPD.

VI.C. Interesse público e interesse vital

IDENTIFICAÇÃO DO PROBLEMA

Para além do tratamento de dados pessoais no âmbito laboral, há tratamentos de dados de saúde que não podem sustentar-se no consentimento dos titulares dos dados, quer por este não ser viável, quer por não ser a condição de licitude mais adequada. Em algumas circunstâncias, o interesse público e o interesse vital, presentes na necessidade de combate à pandemia COVID-19, poderão assumir-se como condições de licitude do tratamento de dados, para lá do consentimento dos titulares dos dados.

ENQUADRAMENTO E POSSÍVEIS SOLUÇÕES

O interesse público e o interesse vital são, em abstrato, condições que podem legitimar o tratamento de dados pessoais, designadamente, por entidades públicas (artigo 23.º da Lei n.º 58/2019), para efeitos, por exemplo, de monitorização de epidemias e da prevenção da sua propagação (*i.e.* fins humanitários).

No contexto atual de pandemia, sem prejuízo da existência de outras fontes de licitude, o tratamento de dados pessoais (*e.g.*, o tratamento de declarações ou certificados, por parte de agentes de segurança pública, para efeitos de circulação para o trabalho) poderá vir a ter como fonte de licitude o interesse público e o interesse vital, tal como estabelecido nas alíneas *d)* e *e)* do artigo 6.º, n.º 1, do RGPD, que consagram, respetivamente: (*i*) a licitude do tratamento "necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular"; e (*ii*) a licitude do tratamento "necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento".

Caso o tratamento de dados incida sobre categorias especiais de dados[5], deverá também

[5] Dados "que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa" (artigo 9.º, n.º 1, do RGPD).

ter-se em consideração as derrogações ínsitas nas alíneas *c)*, *g)* e *i)* do n.º 2 do artigo 9.º do RGPD, que determinam a inaplicabilidade da proibição geral de tratamento de categorias especiais de dados, respetivamente, nos seguintes casos: (*i*) necessidade do tratamento "para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento" (cremos que o campo de aplicação desta fonte de licitude no contexto em análise será bastante limitado); (*ii*) necessidade do tratamento "por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados"; e (*iii*) necessidade do tratamento "por motivos de interesse público no domínio da saúde pública, tais como assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, também com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional".

No que toca à obrigação de o responsável pelo tratamento atuar com base no direito do Estado-Membro (neste caso, Portugal), cumpre realçar o estabelecido na Base 35, n.º 2, da Lei de Bases da Saúde, na qual se determina que: "[c]abe, em especial, aos organismos competentes estudar, propor, executar e fiscalizar as medidas necessárias para prevenir a importação ou exportação das doenças submetidas ao Regulamento Sanitário Internacional, enfrentar a ameaça de expansão das doenças transmissíveis e promover todas as operações sanitárias exigidas pela defesa da saúde da comunidade internacional". Deste modo, à semelhança do que sucede, por exemplo, em Espanha, as entidades administrativas competentes podem propor medidas urgentes que visem combater a ameaça de expansão da COVID-19 e proteger a saúde pública, para salvaguarda dos interesses públicos essenciais, devendo os responsáveis pelo tratamento visados cooperar e cumprir as medidas que forem preconizadas pela Administração Pública.

De notar que o interesse vital apenas deve ser convocado quando o tratamento não puder basear-se manifestamente noutro fundamento jurídico (Considerando 46, do RGPD).

Os dados pessoais tratados ao abrigo das referidas fontes de licitude devem ser limitados ao mínimo necessário relativamente às finalidades para as quais são tratados ("minimização dos dados"), sendo que, embora possa estar em causa uma situação de emergência para a proteção da saúde pública essencial e/ou interesses vitais, o direito fundamental à proteção de dados deve continuar a ser respeitado (Considerando 54 do RGPD).

Assim, os responsáveis pelo tratamento deverão identificar os tratamentos de dados pessoais que realizam ou que pretendem realizar no contexto da pandemia COVID-19, avaliar quais as fontes de licitude que legitimam os referidos tratamentos e estar atentos às eventuais recomendações que a CNPD emitiu e ainda venha a emitir a este respeito.

VI.D. CNPD: suspensão de prazos

IDENTIFICAÇÃO DO PROBLEMA

No contexto atual, e em resultado de se tratar de uma situação de exceção, cumpre ter atenção ao regime: (*i*) dos prazos processuais e procedimentais em curso; (*ii*) dos prazos de prescrição e caducidade; e (*iii*) dos prazos para cumprimento de obrigações previstas na legislação aplicável pelos responsáveis pelo tratamento (em especial, "*data breaches*" e exercício de direitos pelos titulares dos dados).

ENQUADRAMENTO E POSSÍVEIS SOLUÇÕES

Os prazos referentes a atos processuais e procedimentais a praticar em processos civis, criminais e contraordenacionais em curso encontram-se suspensos, até à cessação do regime excecional atualmente em vigor, introduzido pelo artigo 7.º da Lei n.º 1-A/2020 (subsequentemente alterado). A suspensão dos prazos para prática dos referidos atos implica, igualmente, a suspensão dos prazos de prescrição e de caducidade que se encontrem em curso, incluindo no que respeita aos prazos máximos imperativos previstos na lei. A suspensão dos prazos para a prática de atos processuais e procedimentais determina, assim, também a suspensão dos prazos de prescrição relativos a eventuais contraordenações praticadas pelos responsáveis pelo tratamento[6].

Por outro lado, a referida suspensão de prazos não prejudica a necessidade de cumprir, nos prazos fixados, as obrigações que impendem sobre os responsáveis pelo tratamento nos termos do RGPD e de outra legislação aplicável, de entre as quais se destacam a necessidade de notificação de violações de dados pessoais ("*data breach*") e as respostas ao exercício de direitos pelos titulares dos dados.

VI.E. Teletrabalho, confidencialidade e medidas de segurança

IDENTIFICAÇÃO DO PROBLEMA

Um dos temas prementes, resultado da obrigatoriedade da primazia do teletrabalho atualmente verificada, prende-se com a necessidade do cumprimento de medidas técnicas e organizativas de segurança no tratamento de dados pessoais.

ENQUADRAMENTO E POSSÍVEIS SOLUÇÕES

A obrigatoriedade do teletrabalho, sempre que o mesmo se coadune com as funções exercidas pelo trabalhador, gera a necessidade de o empregador se adaptar, criando condições para o exercício de funções através dos meios tecnológicos adequados. Tal necessidade implicará não só a concessão de meios que permitam esse teletrabalho (preferencialmente, meios tecnológicos pertencentes ao próprio empregador), mas também a criação de medidas adicionais de segurança em matéria de proteção de dados. Deverão ser reforçadas as políticas internas no que respeita à privacidade e à segurança dos dados, bem como a estrutura destinada a permitir o trabalho remoto.

O reforço dos sistemas de acesso remoto deve incluir, entre o mais, a implementação das aplicações necessárias a permitir o acesso remoto (como sejam aplicações destinadas à autenticação dos utilizadores, extensão do prazo de duração de *passwords*, VPN e *firewalls*) e a constante atualização e monitorização da segurança dessas aplicações. A crise gerada pela pandemia COVID-19 deu já origem a um aumento do cibercrime, pelo que os responsáveis pelo tratamento de dados devem estar ao corrente deste tipo de atividades ilícitas, alertando constantemente os seus trabalhadores para os riscos que vão surgindo e criando um canal eficaz de troca de informação com os profissionais internos de tecnologias de informação.

Sempre que os trabalhadores usem os seus próprios meios – o que será frequente –, será conveniente a implementação (sempre que estas não existam) de políticas de *Bring Your Own Device*.

Naquele âmbito, a CNPD emitiu orientações destinadas a garantir a conformidade dos tratamentos de dados pessoais dos trabalhadores

---

(6) Acrescente-se ainda que a CNPD por deliberação de 16-03-2020 – Deliberação 2020/170 – havia determinado, no seguimento, então, da declaração de situação de alerta declarada pelo Governo no Despacho n.º 3298-B/2020 de 13 de março, que "os prazos de resposta aos projetos de deliberação se encontram interrompidos até à declaração, pelo órgão de soberania competente, do fim do período excecional que o País atravessa por causa da pandemia" indicando ainda que "os prazos fixados nos projetos começam a ser contados, de novo, no dia útil seguinte à publicação oficial de tal declaração".

em teletrabalho com o regime jurídico de proteção de dados e a minimizar o impacto sobre a privacidade em regime de teletrabalho[7].

A CNPD considera que o recurso, pelos empregadores, a ferramentas (*e.g.*, *TimeDoctor*; *Hubstaff, Timing, ManicTime, TimeCamp, Toggl, Harvest*) que façam um controlo detalhado da atividade no equipamento informático usado pelos trabalhadores e que procedam a uma recolha sistemática de informação sobre a atividade e inatividade do trabalhador constitui tratamento excessivo de dados pessoais, violador do princípio da minimização[8] dos dados pessoais que não é, por isso, admissível[9].

No que toca ao registo do tempo de trabalho, a CNPD admite que, em regime de teletrabalho, o registo possa ser feito com recurso a soluções tecnológicas específicas, lembrando que as ferramentas usadas para o efeito terão de estar "desenhadas de acordo com os princípios da privacidade desde a conceção e por defeito, não recolhendo mais informação do que a necessária para a prossecução daquela finalidade"[10].

[7] Disponíveis em https://www.cnpd.pt/home/orientacoes/Orientacoes_controlo_a_distancia_em_regime_de_teletrabalho.pdf.

[8] *Cfr*. alínea *c*) do n.º 1 do artigo 5.º do RGPD. O responsável pelo tratamento, que neste contexto é o empregador, só deve tratar os dados adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.

[9] Para uma indicação sobre o modo como, nestas orientações, a CNPD preconiza a possibilidade de o empregador exercer o seu poder de controlar a atividade do trabalhador *vd.* capítulo IV.D, "Controlo à distância em regime de teletrabalho" *supra*.

[10] Por referência aos princípios de "*data protection by design*" e "*by default*" constantes do artigo 25.º do RGPD.

Para uma indicação sobre algumas formas alternativas de o empregador conseguir esse registo de tempo de trabalho que a CNPD considerou expressamente nas orientações emitidas *vd.* capítulo IV.D "Controlo à distância em regime de teletrabalho" *supra*.

VI.F. Tratamento de dados de localização

IDENTIFICAÇÃO DO PROBLEMA

Em resultado da necessidade de cumprir quarentenas e manter o isolamento social, a par de outros benefícios (*e.g.*, detetar focos da doença), têm sido discutidos os benefícios da partilha de dados – desejavelmente anonimizados e agregados – por parte das operadoras de telecomunicações, com as autoridades, tendo em vista a monitorização de zonas onde se verifiquem "ajuntamentos" e onde não estejam a ser cumpridas as obrigações de isolamento ou distanciamento social. Adicionalmente, têm surgido projetos e iniciativas privadas com o objetivo de monitorizar a doença e ajudar ao seu controlo. Não sendo estes dados considerados – ao contrário dos dados relativos à saúde – categorias especiais de dados nos termos e para os efeitos do disposto no artigo 9.º do RGPD, ainda assim, o seu tratamento está sujeito ao regime especial consagrado na Lei da Proteção de Dados e da Privacidade nas Comunicações Eletrónicas, lei especial em face do RGPD.

ENQUADRAMENTO E POSSÍVEIS SOLUÇÕES

Numa entrevista de 19 de março[11], o presidente da Autoridade de Supervisão Italiana (*Garante*) demonstrou preocupação ao referir que o estado de emergência e a consequente compressão das liberdades individuais não podem justificar a tomada de medidas excessivas, dando como exemplo a existência de propostas para rastreios digitais em massa, que não devem ser irrefletidamente adotadas. Nesse sentido, a recolha de dados de localização e de outros que permitam rastrear hábitos e movimentos, devem ser objeto de ponderada análise, devendo optar-se sempre pela medida menos restritiva.

Em Itália, na Alemanha e na Áustria foram já partilhados, por parte de operadoras de telecomunicações, dados de localização, anonimizados e agregados, com autoridades de

[11] Disponível em: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9292565.

saúde, para ajudar a monitorizar o cumprimento dos períodos de quarentena e isolamento social, permitindo a identificação de concentrações e movimentações pelas autoridades. Tratando-se de dados anonimizados, *i.e.*, que não permitam, de forma irreversível, identificar os seus titulares, não estaremos no âmbito do RGPD. Contudo, havendo a intenção de tratar dados pessoais de localização e dados auxiliares a estes controlos e análises (*e.g.*, controlo e movimento de quem se encontra em quarentena), o RGPD deverá ser observado, a par da legislação especial aplicável.

Em Portugal, de acordo com o n.º 1 do artigo 7.º da Lei da Proteção de Dados e da Privacidade nas Comunicações Eletrónicas, "[n]os casos em que sejam processados dados de localização, para além dos dados de tráfego, relativos a assinantes ou utilizadores das redes públicas de comunicações ou de serviços de comunicações eletrónicas acessíveis ao público, o tratamento destes dados é permitido apenas se os mesmos forem tornados anónimos".

Em termos simplificados, podem ser partilhados dados de localização, desde que estes sejam anónimos; havendo a intenção de processar dados de localização de titulares identificados ou de forma a que os mesmos titulares sejam identificáveis, deve este tratamento ser precedido de consentimento.

De todo o modo, importa – mesmo no atual contexto – reduzir ao máximo o grau de intrusão que a recolha massiva dos tipos de dados que representa, devendo ser feita de forma proporcional e na medida do estritamente necessário.

Uma vez que este tema tem sido objeto de ampla discussão, e que se antevê que as tecnologias que têm por base a utilização de dados de localização possam ser um auxílio relevante no combate à pandemia, o CEPD pronunciou-se[12], de forma sucinta, sobre o tratamento de dados de localização, tendo em vista analisar a disseminação da COVID-19 e a eficácia das medidas de confinamento e sobre a utilização de aplicações de *contact tracing* (rastreamento de contacto).

O CEPD pugna por uma abordagem comum no seio da União Europeia, salientando que a eficiência da utilização desta tecnologia dependerá da coordenação com as autoridades de saúde.

Quanto ao tratamento de dados de localização, reitera o CEPD que deve ser dada primazia à utilização de dados anonimizados, recordando a necessidade de garantir uma anonimização que, de facto, não permita a (re)identificação dos titulares dos dados. De acordo com o CEPD "[o] conceito de anonimização é propenso a ser mal compreendido e muitas vezes é confundido com pseudonimização. Enquanto a anonimização permite usar os dados sem qualquer restrição, os dados pseudonimizados ainda estão no âmbito do RGPD", assinalando, de igual modo, a dificuldade em efetivamente anonimizar os dados de localização. Por outro lado, e à luz do princípio da transparência, o CEPD refere que as técnicas de anonimização utilizadas devem ser tornadas públicas.

No que respeita às aplicações de *contact tracing*, *grosso modo*, e não entrando em detalhe quanto aos vários modelos em discussão, estas têm o objetivo de informar os utilizadores caso estes tenham tido contactado com alguém que, posteriormente, se confirme estar infetado.

Para o CEPD é essencial que a utilização destas aplicações seja voluntária, assinalando o seu caráter intrusivo.

---

(12) Diretrizes n.º 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19 disponíveis em https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf .

O CEPD refere que, idealmente, caso estas aplicações sejam utilizadas, devem fazer parte de uma estratégia concertada em matéria de saúde pública, coordenando as respetivas funcionalidades com testes e verificação manual dos contactos, analisando eventuais cadeias de contágio e evitando *falsos positivos* e dados errados.

O CEPD apela à necessidade de ter em conta o princípio da minimização, recordando que as aplicações de *tracing:*

(i) Não exigem o rastreamento de localizações precisas dos utilizadores individuais, sendo suficiente a utilização de dados de proximidade;
(ii) Podem funcionar sem identificar diretamente os titulares, devendo implementar medidas que evitem essa identificação;
(iii) Devem evitar a extração de informação, que deve manter-se, sempre que possível, no equipamento terminal do utilizador, recolhendo apenas a informação estritamente necessária.

Sempre que a estas aplicações de monitorização de contactos seja de aplicar o previsto no artigo 5.º, n.º 3, da Diretiva *E-Privacy* (transposto pelo artigo 5.º da Lei da Proteção de Dados e da Privacidade nas Comunicações Eletrónicas) – *i.e.* quando impliquem o acesso a informação armazenada no dispositivo, que não se qualifique como dados de tráfego –, deve ser previamente obtido o consentimento do utilizador[13].

Por outro lado, refere o CEPD que devem ser definidos prazos de conservação curtos, devendo ser tida em conta a efetiva necessidade de tratar os dados, ao invés, naturalmente, da mera conveniência de os armazenar.

Relativamente à condição de licitude que deve estar verificada, nos termos do RGPD, sempre que haja tratamento de dados pessoais, esta não tem necessariamente de ser o consentimento, podendo, por exemplo, aplicar-se o previsto no artigo 6, n.º 1, alínea *e)*. Melhor dizendo: a instalação da aplicação deve ser voluntária, mas o subsequente tratamento de dados pessoais poderá ter por fundamento outra condição de licitude, desde que o Estado-Membro em causa haja legislado sobre essa matéria.

Não desconsiderando o relevo desta tecnologia no combate à atual situação de pandemia, é essencial que a sua utilização não se torne um hábito, e que cesse em absoluto no fim desta crise pandémica, em virtude do potencial intrusivo que acarreta.

Também a Comissão Europeia adotou uma recomendação, em 08-04-2020, para **apoiar as medidas de contenção do coronavírus através de dados e aplicações móveis**[14] **na qual estabeleceu** um processo para o desenvolvimento de uma abordagem comum que foi designada por "conjunto de instrumentos" (*common toolbox*), para a utilização de meios digitais no combate à crise provocada pela COVID-19.

Em causa está um conjunto de medidas práticas para uma utilização eficaz das tecnologias e dos dados, com particular incidência nos dois domínios a seguir indicados:

"(1) Uma abordagem pan-europeia, coordenada a nível da União, com vista à utilização de aplicações móveis que permitam aos cidadãos tomarem medidas eficazes e

(13) Damos nota de que, neste caso, deverá ser obtido consentimento, independentemente de estarem ou não em causa dados pessoais. As únicas exceções à necessidade de obter consentimento são as que se encontram previstas nas alíneas *a)* e *b)*, do n.º 2 do artigo 5.º da Lei da Proteção de Dados e da Privacidade nas Comunicações Eletrónicas.

(14) Recomendação (UE) 2020/518 da Comissão de 8 de abril de 2020, relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a crise da COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32020H0518&from=PT.

mais específicas de distanciamento social e que alertem, previnam e rastreiem os contactos, a fim de limitar a propagação da COVID-19 [...] abordagem [que] incluirá um método de acompanhamento e partilha das avaliações da eficácia das aplicações, da sua interoperabilidade e das implicações transfronteiriças, bem como do modo como as aplicações garantem o respeito pela segurança, pela privacidade e pela proteção dos dados; e

(2) Um sistema comum de utilização de dados anonimizados e agregados sobre a mobilidade das populações destinado a i) modelizar e prever a evolução da doença, ii) monitorizar a eficácia da tomada de decisões pelas autoridades dos Estados-Membros no que respeita a medidas como o distanciamento social e o confinamento, e iii) contribuir para uma estratégia coordenada de saída da crise da COVID-19."

No seguimento dessa recomendação, foi desenvolvido o mencionado "conjunto de instrumentos" europeu, para propiciar a utilização de aplicações móveis de alerta e rastreio de contactos para responder à pandemia da COVID-19[(15)] tendo esse conjunto de instrumentos sido acompanhado, no dia imediato, pela emissão de um conjunto de orientações da Comissão Europeia referentes às aplicações móveis em causa (e seu desenvolvimento) na perspetiva da proteção de dados[(16)].

Estas são orientações que incidem apenas sobre aplicações móveis "descarregadas, instaladas e utilizadas voluntariamente pelos cidadãos) com uma ou várias das seguintes funcionalidades:

- fornecimento de informações exatas aos cidadãos sobre a pandemia de COVID-19;
- fornecimento de questionários para autoavaliação e orientação dos cidadãos (funcionalidade de controlo de sintomas) (...);
- alerta das pessoas que tenham estado na proximidade de uma pessoa infetada durante determinado período de tempo, de modo a fornecer informações como a recomendação de autoquarentena ou a indicação dos locais de realização de testes de diagnóstico (funcionalidades de rastreio de contactos e alerta);
- criação de um fórum de comunicação para médicos e pacientes em situação de autoisolamento e para os casos em que é prestado aconselhamento ulterior em matéria de diagnóstico e de tratamento (...)".

---

(15) Mobile applications to support contact tracing in the EU's fight against COVID-19 - *Common EU Toolbox for Member States* emitidas em 15-04-2020 pela Rede de Saúde em Linha (EHealth), rede de autoridades nacionais responsáveis pela saúde em linha, disponíveis em https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

(16) Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados (2020/C 124 I/01) disponíveis em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN.

AUTORES

Francisca Robalo Cordeiro
Associada

Helena Tapp Barroso
Sócia

Maria da Assunção da Cunha Reis
Associada

Marta Salgado Areias
Associada

Tiago Félix da Costa
Sócio

Member
Lex Mundi
World Ready

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Com o cliente, em qualquer lugar, em qualquer momento.

MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

LISBOA
Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTO
Avenida da Boavista, 3265 – 4.2
Edifício Oceanvs
4100-137 Porto
T +351 226 166 950 - 226 052 380
F +351 226 163 810 - 226 052 399
mlgtsporto@mlgts.pt

FUNCHAL
Av. Arriaga, n.º 73, 1.º, Sala 113
Edifício Marina Club
9000-060 Funchal – Portugal
T +351 291 200 040
F +351 291 200 049
mlgtsmadeira@mlgts.pt

mlgts.pt

ALC ADVOGADOS

LUANDA
Masuika Office Plaza
Edifício MKO A, Piso 5, Escritório A/B
Talatona, Município de Belas
Luanda – Angola
T +244 926 877 476/8/9
T +244 926 877 481
geral@alcadvogados.com

alcadvogados.com

HRA ADVOGADOS

MAPUTO
Avenida Marginal, 141, Torres Rani
Torre de Escritórios, 8.º piso
Maputo – Moçambique
T +258 21 344000
F +258 21 344099
geral@hrlegalcircle.com

hrlegalcircle.com

MdME LAWYERS

MACAU
Avenida da Praia Grande, 409
China Law Building
21/F and 23/F A-B, Macau
T +853 2833 3332
F +853 2833 3331
mdme@mdme.com.mo

HONG KONG
Unit 2503 B
25F Golden Centre
188 Des Voeux Road
Central, Hong Kong
T +852 3619 1180
F +853 2833 3331
mdme@mdme.com.mo

Foreign Law Firm

mdme.com.mo