Proteção de dados pessoais *versus* proteção da Saúde em tempos de pandemia

ANA PAULA CABRAL*
ISCET

RESUMO

O direito à saúde é um direito fundamental consagrado na Constituição da República Portuguesa. O direito à proteção de dados não é um direito absoluto, pelo que pode ceder perante outros direitos, dependendo das circunstâncias. Este direito implica um cuidado com a segurança da informação, onde se integram os dados pessoais. Esta é uma tendência do presente que anuncia o futuro, a curto prazo. É um sinal do futuro no presente. Esta tendência reforçou-se com a intrusão abrupta na vida nacional, europeia e global do coronavírus, causador de uma pandemia, que urge combater. Neste artigo fazemos uma breve abordagem a alguns mecanismos e ferramentas utilizados neste combate, com implicações na proteção de dados pessoais. Apesar da imperatividade da defesa dos dados pessoais e respetiva proteção, terá sempre que haver cedência desta quando outros valores mais relevantes estiverem em causa, como é o caso da saúde de cada um individualmente considerado e saúde pública em geral, postas em causa pela pandemia.

PALAVRAS-CHAVE

Dados pessoais, proteção, saúde, pandemia

ABSTRACT

The right to health is a fundamental right enshrined in the Constitution of the Portuguese Republic. The right to data protection is not an absolute right, so it may give way to other rights, depending on the circumstances. This right implies a care with the security of information, where personal data are integrated. This is a trend of the present that announces the future, in the short term. It is a sign of the future in the present. This trend has been reinforced by the abrupt intrusion of the coronavirus into national, European and global life, which is causing a pandemic, that must be urgently combated. We have taken a brief look at some of the mechanisms and tools used in this fight, with implications for the protection of personal data. Despite the imperative of defending personal data and their protection, this will always have to be given up when more relevant values are at stake, such as the cause of the individual health and public health in general, called into question by the pandemic.

KEYWORDS

Personal data, protection, health, pandemic

INTRODUÇÃO

O presente artigo constitui uma reflexão pessoal, traduzindo igualmente o resultado da pesquisa desenvolvida no âmbito da temática da segurança da informação nos tempos de hoje.

Com efeito, trata-se de matéria com plena atualidade, portanto presente, sobre a qual recaem ou devem recair as nossas preocupações e, consequentemente, constituir objeto do Direito, que nos regula.

Se esta reflexão que tenho vindo a desenvolver há algum tempo, se antes nos parecia relevante, nos últimos meses passou a revestir-se de natureza fundamental, por força da pandemia que nos tem vindo a assolar e que veio redesenhar a vida de cada um de nós e do mundo em geral.

Várias questões se nos colocam buscando nós encontrar a adequada resposta no final da nossa reflexão. Concretamente, questionamo-nos sobre quais as tendências do presente, com caraterísticas muito específicas depois da chegada da pandemia.

Tentaremos encontrar uma resposta para a questão de como será o futuro, como se antevê que seja.

Para isso, para além de um enquadramento de análise e reflexão, propomo-nos ponderar sobre alguns aspetos de natureza jurídica, destacando-se a segurança da informação, a proteção da privacidade, concretamente dos

* Assistente, especialista em Direito.
Endereço eletrónico: acabral@iscet.pt

dados pessoais de cada sujeito *versus* a proteção da saúde de cada um dos sujeitos e a saúde pública em geral.

Esta reflexão, que em nosso entender é relevante, pelas consequências daqui decorrentes, passou a assumir contornos de suma importância por força da pandemia que estamos a atravessar, nunca antes por nós antecipados. Tempos em que cada sujeito se sente verdadeiramente inseguro, perante tudo e todos, sobretudo perante um inimigo poderoso e invisível, cuja defesa é muito difícil.

1. DESENVOLVIMENTO

1.1. Do direito à Saúde como direito fundamental

A Constituição da República Portuguesa (CRP), seguindo o modelo de diversas leis fundamentais de outros Estados Europeus, contém um catálogo de direitos fundamentais, onde se insere o direito à Saúde, no seu artigo 64.º.

Com efeito, o n.º 1 deste preceito consagra que "*Todos têm direito à proteção da saúde e o dever de a defender e promover*."

O direito à Saúde é um direito fundamental de natureza social, o que implica a respetiva concretização, nomeadamente através da publicação de legislação e subsequente execução.

O presente direito fundamental está intrinsecamente ligado ao direito fundamental por excelência, que se insere no conjunto de direitos, liberdades e garantias e que é o direito à vida, consagrado no artigo 24.º da CRP.

Como direito de natureza social não goza da prerrogativa típica dos direitos, liberdades e garantias que é a sua aplicabilidade direta, nos termos do disposto no artigo 18.º da CRP. Porém, como direito fundamental que é, cabe ao Estado contribuir para a sua realização.

Se há momento em que o direito à Saúde está presente nas preocupações de cada sujeito, cada instituição, cada Estado, nomeadamente do Estado português, é o presente.

Isto porque agora a saúde de cada um é sentida como um bem de suma importância, dado que corre o risco de ser posta em causa da forma mais inacreditável possível, através da pandemia que atravessamos. Concomitantemente, o presente momento é um ótimo exemplo da necessidade e dependência de qualquer sujeito perante o Estado, por força da estrutura e mecanismos de que este dispõe. De facto, os momentos de crise servem para recentrar linhas de pensamento e até para alterar opiniões.

Exemplificando, no nosso caso, sempre fomos defensores dum Sistema de Saúde integrado pelos diversos elementos que o compõem, destacando-se o Serviço Nacional de Saúde (SNS) como fulcro do mesmo, mas colocando em pé de igualdade os prestadores, independentemente da sua natureza ser pública, privada, social ou cooperativa. Por força dos últimos tempos, alterei de algum modo a minha opinião, passando a defender um Sistema de Saúde fundamentalmente centrado no setor público, assumindo os prestadores não públicos como "complemento" no Sistema.

2. DOS DADOS PESSOAIS E RESPETIVA PROTEÇÃO. A PROTEÇÃO DA PRIVACIDADE

Afirmada a relevância do direito à Saúde, ponderemos agora sobre a importância da privacidade e da respetiva proteção.

A privacidade de cada sujeito constitui um direito respeitante à sua personalidade, protegida desde logo pela CRP, nomeadamente no seu artigo 26.º, que consagra a proteção genérica da personalidade, bem como pelas normas do Código Civil respeitantes aos direitos de personalidade.

Apesar da afirmação que acabámos de proferir, o foco da nossa análise é a privacidade, na perspetiva dos dados relativos a cada sujeito, pessoa singular. Dito de outro modo, o cerne da nossa reflexão são os dados pessoais, cuja proteção específica reside nas normas do Regulamento Geral de Proteção de Dados (RGPD), na Lei de Proteção de Dados e na relação entre a proteção destes dados e a de outros direitos, nomeadamente do direito à saúde.

O conflito entre estes dois tipos de direitos e a respetiva proteção pode assumir contornos diferentes em circunstâncias tão díspares da normalidade, como são as resultantes de um período como este que estamos a atravessar, por força da pandemia da COVID-19.

O 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, é uma fonte de direito comunitário derivado, que permite harmonizar os ordenamentos jurídicos dos Estados-membros, na medida em que é diretamente aplicável, não carecendo de ser transposto para os direitos nacionais, diferentemente das diretivas.

A União Europeia, ao definir o regime da proteção de dados num regulamento, pretendeu obter a harmonização dos regimes jurídicos correspondentes nos Estados-Membros e, mais do que isso, num âmbito geográfico muito mais alargado. Senão vejamos o disposto no artigo 3.º, sobre o seu âmbito de aplicação territorial. Por força desta norma, o regime constante do RGPD é aplicável bem mais além do âmbito geográfico dos Estados-Membros, podendo sê-lo em qualquer local onde sejam tratados dados de residentes em Estados da UE, aplicando-se mesmo ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

É compreensível que o âmbito de aplicação geográfico do RGPD seja tão amplo, pois só assim permite abranger alguns tratamentos de dados pessoais, que podem ocorrer fora do território dos Estados-Membros.

Globalmente, no que respeita ao regime constante do RGPD podemos afirmar tratar-se de um conjunto de normas jurídicas cujo objeto é a proteção dos dados pessoais, sem pôr em causa a liberdade de circulação no âmbito da União Europeia. Mais concretamente, conforme se dispõe no artigo 1.º, n.ºs 1 e 2 deste diploma (…) *estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.*

2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

Composto por 22 artigos e 173 considerandos, este instrumento de direito comunitário pretende estabelecer as regras em matéria de proteção de dados pessoais, de modo a acautelar da melhor forma a proteção deste tipo de dados.

Em boa verdade, o regime aqui inserto não traz novidades muito significativas relativamente ao até aí vigente nos diferentes estados, como é o caso do Estado português, procedendo-se fundamentalmente, como já pudemos referir a uma intenção de harmonização de regimes e atualização dos mesmos.

Não podemos, porém, deixar de mencionar alguns pontos como sejam a alteração do paradigma de proteção, que passa a ser de natureza autorregulatória. Dito de outro modo, cada responsável pelo tratamento de dados tem a obrigação de os tratar cumprindo as regras e imprimindo todo o necessário cuidado devendo, sempre que necessário, evidenciar a forma como esse tratamento se efetua.

Após a consagração de 26 conceitos, desde logo o de dados pessoais e de tratamento de dados, que, no fundo, corresponde a toda e qualquer atividade sobre dados pessoais, estabelece o RGPD um conjunto de princípios base em matéria de tratamento.

Sumariamente integram esses princípios: o da licitude, lealdade e transparência; a recolha de dados com finalidades determinadas, explícitas e legítimas; a minimização exatidão e atualização dos dados; a limitação da conservação e o tratamento de forma que garanta a sua segurança.

A licitude do tratamento dos dados depende da presença de uma das condições de legitimidade descritas no artigo 6.º deste diploma, seja o consentimento (expresso, positivo, o que não é o mesmo que escrito) do respetivo titular, o cumprimento de um contrato ou de uma obrigação jurídica, a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, o exercício de funções de interesse público ou da autoridade pública, como responsável pelo tratamento de dados; a necessidade para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros.

É de realçar igualmente a afirmação de que, à partida, os dados pessoais especiais não podem ser objeto de tratamento, embora o RGPD estabeleça as exceções a este princípio.

Chamamos a atenção também para a consagração de um conjunto de contraordenações nesta matéria, cujas coimas são de tal modo elevadas que se tornam inexequíveis na prática.

Apesar do RGPD ser, conforme já aqui afirmámos, diretamente aplicável nos Estados-Membros, impunha-se uma lei de execução deste regime, o que aconteceu, no que ao Estado português respeita, com algum atraso.

A Lei n.º 58/2019, de 08 de agosto (Lei de Proteção de Dados – LPD), que veio revogar a lei até aí vigente, vem assegurar a execução do RGPD na ordem jurídica nacional.

Não consagra vários esclarecimentos relativamente a dúvidas de execução resultantes do RGPD necessários, mas estabelece alguns aspetos dignos de destaque como sejam:

- A consagração da Comissão Nacional de Proteção de Dados (CNPD) como autoridade de controlo nacional e respetiva caraterização;
- O estabelecimento de normas relativas à figura do encarregado de proteção de dados;
- A definição dum quadro sancionatório de natureza contraordenacional e criminal, em matéria de dados pessoais, inserido num conjunto de normas em matéria de tutela administrativa e jurisdicional;
- A previsão de um conjunto de disposições especiais sobre o consentimento de menores; proteção de dados pessoais de pessoas já falecidas; portabilidade e interoperabilidade dos dados; videovigilância; o dever de segredo; o prazo de conservação de dados e a sua transferência, e ainda o tratamento de dados por entidades públicas para finalidades diferentes.

Atendendo à relevância da matéria para a restante reflexão que nos encontramos a fazer, destaca-se o capítulo onde se consagram situações especiais de tratamento de dados pessoais, centrando-me no tratamento de dados de saúde e dados genéticos, consagrado no artigo 29.º da LPD.

Realçamos a preocupação do legislador nacional em prever, nos dois primeiros números deste artigo, que: "1 – *Nos tratamentos de dados de saúde e de dados genéticos, o acesso a dados pessoais rege-se pelo princípio da necessidade de conhecer a informação; e que (…) 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*."

3. DA SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

A proteção de dados pessoais está intrinsecamente ligada à segurança de informação em geral. Com efeito, nem toda a informação se reconduz a dados pessoais, mas estes dados são indubitavelmente informação.

Como, na atualidade, a informação é maioritariamente tratada com recurso às tecnologias de natureza informática, a proteção de dados pessoais e a segurança da informação em geral estão intimamente ligadas à cibersegurança.

A Lei n.º 46/2018 de 13 de agosto estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Apesar da segurança do ciberespaço consagrada no presente diploma, aí mesmo se estabelece a necessidade de não serem salvaguardadas as funções essenciais do Estado, incluindo medidas de proteção da informação cuja divulgação seja contrária aos interesses de segurança nacional, à manutenção de ordem pública ou a permitir a investigação, a deteção e a repressão de infrações penais.

A proteção jurídica específica contra violações de direitos e interesses através dos meios informáticos pode concretizar-se na consagração de normas de natureza criminal – veja-se a tipificação de crimes na lei do cibercrime.

A Lei n.º 109/2009 de 15 de setembro aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

4. DA PROTEÇÃO DO DIREITO À SAÚDE *VERSUS* PROTEÇÃO DOS DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO EM TEMPOS DE PANDEMIA

Feita a referência a aspetos que vão influenciar a nossa reflexão focada no cerne deste trabalho e que é a relação entre a proteção do direito à saúde e a dos dados pessoais,

que se complexificou no momento corrente determinado pela pandemia do COVID-19, trataremos agora de conjugar as diferentes variáveis de uma equação complexa.

A nossa cogitação conjuga concretamente fatores como: o direito fundamental à saúde; o direito e liberdade fundamental das pessoas singulares de proteção dos dados pessoais ou, de forma mais lata, a proteção da privacidade e o direito à segurança da informação.

A ponderação destes elementos tem que ser combinada com algumas mudanças determinadas pelo surgimento de um novo que veio baralhar tudo quanto era considerado certo e seguro, complexificando o que já era complicado. Este novo elemento é a pandemia provocada pelo coronavírus causador da doença de COVID-19.

Para combater esta pandemia foi necessário reinventar situações e tomar um conjunto de medidas que podem pôr em causa os direitos que se pretende defender, como é o direito à proteção dos dados pessoais.

A situação vivida foi (é) de tal forma difícil que chegou a ser declarado pelo Presidente da República estado de emergência.

Previsto na CRP, o estado de emergência só em situações muito excecionais pode ser decretado, de acordo com o regime, consagrado na Lei n.º 44/86, de 30 de setembro.

Com efeito, a sua vigência determina consequências gravosas para o funcionamento do Estado, mais especificamente para os cidadãos. É que, por força da sua declaração, ficam suspensos alguns direitos, com a exclusiva finalidade de adotar as medidas necessárias para a proteção da saúde pública, no âmbito da pandemia COVID-19.

Trata-se de um regime excecional, previsto na Constituição (artigo 19.º).

Uma vez declarado pelo Presidente da República, cabe ao Governo executar a declaração do estado de emergência nos termos declarados pelo Presidente da República e autorizados pela Assembleia da República. O Governo deve manter estas instituições informadas da execução da declaração do estado de emergência.

Conforme previsto no artigo 1.º deste diploma legal, "*o estado de sítio ou o estado de emergência só podem ser declarados nos casos (…) de calamidade pública*".

A suspensão dos direitos, liberdades e garantias determinada pela declaração de estado de emergência tem que ser limitada "*quanto à sua extensão, à sua duração e aos meios utilizados, ao estritamente necessário ao pronto restabelecimento da normalidade*".

É de referir que a violação da declaração de estado de emergência constitui crime de desobediência.

É ao Presidente da República que cabe declarar (através de um Decreto, sujeito a referenda do Governo) o estado de emergência, dependendo da audição do Governo e da autorização da Assembleia da República.

Uma vez cessando as "*circunstâncias que tiverem determinado a declaração (…) do estado de emergência, será esta imediatamente revogada, mediante decreto do Presidente da República referendado pelo Governo*."

O estado de emergência cessa automaticamente pelo decurso do prazo fixado na respetiva declaração.

A caraterização e fundamentação do estado declarado, respetivo âmbito territorial, a duração e a especificação dos direitos, liberdades e garantias cujo exercício fica suspenso ou restringido por força da declaração de estado de emergência são alguns dos elementos que obrigatoriamente integram o conteúdo desta declaração.

É ao Governo que cabe a execução da declaração do estado de emergência, tendo que manter informados o Presidente da República e a Assembleia da República dos atos que praticar neste âmbito.

Procedemos, de seguida, a uma brevíssima referência a três ferramentas concebidas pela necessidade de combater a pandemia e que têm implicações em dados pessoais, sendo legítima a dúvida quanto à possibilidade de violarem as normas que regulam a sua proteção.

Smart Crowd

O sistema denominado *Smart Crowd* visa, a partir da recolha de fotografias tiradas a um conjunto de praias (cerca de 70), uma indicação qualitativa quanto à sua taxa de ocupação.

Estas imagens são recolhidas periodicamente por uma câmara da praia e alimentam um sistema autónomo de análise inteligente, instalado em cada câmara que processa a informação de forma autónoma (sem qualquer intervenção humana nem disponibilização). O sistema inteligente é utilizado para processar a informação e efetua

uma análise local dessa. Utiliza as imagens apenas durante o tempo estritamente necessário para o cálculo da taxa de ocupação e de seguida, envia informação alfanumérica (n.º de pessoas e área útil), em formato anónimo e agregado, para disponibilizar em forma de dado qualitativo – ocupação baixa, elevada ou plena.

Não há dúvida quanto ao facto de que esta aplicação procede a tratamento de dados pessoais, pois a captação de imagens pelas câmaras a instalar nas praias implica recolha, processamento e conservação de informação relativa a pessoas singulares identificáveis.

Ora, a captação sistemática de imagens de pessoas num espaço público corresponde a uma das situações em que o RGPD impõe a realização de uma avaliação de impacto sobre a proteção de dados, o que efetivamente aconteceu.

A recolha de dados pessoais através do presente sistema serve duas aplicações (App "Info Praia" e App "Praia em Direto").

A presente descrição serve para proceder ao enquadramento da eventual violação de dados pessoais através deste mecanismo.

Podemos concluir que os dados pessoais aqui tratados, cujo objetivo é garantir o controlo da pandemia da Covid-19, são-no de forma legítima, desde que sejam tomadas as medidas de minimização do risco possíveis, nomeadamente o seu funcionamento apenas durante o período de tempo em que é necessária para atingir o objetivo estabelecido, cumprindo assim as normas a que está sujeita. Seguimos de perto a posição da CNPD na sua Deliberação 2020/251 .

Trace COVID-19

A ferramenta Trace COVID-19 serve para proceder ao acompanhamento *contact tracing* de doentes com esta doença em vigilância e autocuidados.

A utilização desta ferramenta levanta dúvidas relativamente à possibilidade de pôr em causa as normas que regulam o tratamento de dados pessoais.

Questiona-se a eventual violação da privacidade e confidencialidade dos dados pessoais objeto de tratamento através desta ferramenta, na medida em que permite a consulta, sem aparente limitação, no universo disponível, bem como a exportação, sem qualquer controlo, de listagens de dados pessoais para tabelas de Excel.

Quando estamos perante uma ferramenta desta natureza, algumas questões se nos colocam para podermos defender uma posição quanto à bondade do seu funcionamento, no que respeita ao tratamento de dados pessoais.

As questões que se nos afiguram como relevantes são muitas, destacando-se: o que faz esta aplicação; se trata dados pessoais e, em caso afirmativo, quais são esses dados; quem tem acesso a essa aplicação e, consequentemente, aos dados eventualmente aí tratados; como se procede a esse acesso; se comunica com outras aplicações e, em caso afirmativo, de que forma, etc..

Na impossibilidade de nos pronunciarmos em profundidade sobre todos estes aspetos, seguimos de perto os elementos a que pudemos aceder através da análise da Deliberação 2020/262 da CNPD.

Desde logo podemos apontar uma falha a esta aplicação, que se traduz no facto de não ter sido precedida de uma avaliação do impacto em matéria de dados pessoais, dado que se trata de uma das situações em que esta é obrigatória, nos termos do artigo 35.º do RGPD. Esta obrigatoriedade existe mesmo, tratando-se de uma ferramenta concebida para atuar numa situação de emergência de saúde pública, correspondendo-lhe o objetivo de acompanhar, da melhor forma, os doentes com esta patologia, bem como os sujeitos suspeitos de estarem infetados.

No entanto, o legislador europeu, quando ponderou sobre as normas do RGPD, não excluiu esta obrigação numa situação destas, nem tão pouco a inseriu no conjunto de situações suscetíveis de serem afastadas *in genere* pelo legislador nacional (cf. artigo 23.º do RGPD).

Apesar do que acabámos de referir, a situação de emergência de saúde pública, a necessidade de satisfação do interesse público em presença e a possibilidade de administrativamente ter sido acautelada a avaliação do impacto das medidas que suportam a aplicação em apreço, legitimam, em nosso entender, esta intervenção, mesmo sem a avaliação do impacto suprarreferida.

Chamamos a atenção para o facto de que o princípio da limitação da conservação dos dados determina que, não sendo estes necessários, após a extinção da pande-

mia, devem ser eliminados e não aproveitados para outras finalidades para além da que presidiu à sua recolha.

Assim, a utilização desta aplicação deve ter lugar através de utilizadores que sejam profissionais de saúde, sujeitos ao dever de sigilo profissional, o acesso aos dados dos utentes.

Stayway COVID

STAYWAY COVID para rastreio da propagação da COVID – trata-se de uma aplicação de utilização voluntária em dispositivos móveis.

Esta aplicação, cujo objetivo é contribuir para quebrar rapidamente cadeias de transmissão, consiste num sistema digital de rastreio de proximidade (*contact tracing*). Mais concretamente, esta ferramenta procede à notificação da exposição individual a fatores de risco de contágio.

Pretende-se que o portador do telemóvel onde esteja instalada a aplicação seja notificado sempre que o seu aparelho tenha estado a uma distância de menos de 2 metros, durante mais de 15 minutos, de uma pessoa, igualmente utilizadora da aplicação e a quem veio a ser diagnosticada a COVID-19. Isto porque existe o risco de o sujeito portador do equipamento móvel ter sido contaminado, atendendo à distância e ao período de tempo de contacto.

Aspeto muito relevante caraterizador desta ferramenta é que assenta na vontade do utilizador do equipamento onde está instalada. Só descarrega a aplicação no seu equipamento porque voluntariamente o quer; para além dos dados pessoais objeto de tratamento serem pseudonimizados, pode não comunicar sempre que recebe a notificação de ter estado em contacto com alguém infetado. Além do mais, pode desativar esta aplicação em determinados períodos, ou melhor, pode simplesmente desligar o *bluetooth*, deixando de receber notificações, ligando-o novamente quando entender.

Alguns riscos para os dados pessoais sempre poderão existir, como é o caso do risco de poder, eventualmente, haver lugar à identificação do utilizador da aplicação mas, como já foi dito, os dados pessoais estão pseudonimizados.

Outro risco que pode ser imputado a esta ferramenta reside no facto de recorrer ao *interface* de dois gigantes que são a Google e a Apple.

Porém, apreciada globalmente parece-nos que esta aplicação tenta minimizar ao máximo os riscos de violação da privacidade, sendo sempre defensável a manutenção do seu cariz voluntário, a vários níveis, conforme aqui já foi por nós referido.

Outros aspetos específicos podem ser identificados, neste período da pandemia, que colocam em confronto a necessidade de combatê-la com a defesa dos dados pessoais, aos quais apenas faremos referência.

É o que se passa: com o ensino à distância, através da utilização de plataformas informáticas; com o controlo da temperatura corporal dos alunos ou dos trabalhadores, como forma de rastreio de sintomas considerados como típicos da COVID-19.

Relativamente ao controlo à distância em regime de teletrabalho, há que notar que, por força da pandemia, grande parte dos trabalhadores passou a trabalhar em teletrabalho.

Algumas entidades empregadoras, pretendendo controlar os seus trabalhadores, adotaram *softwares* intrusivos no que toca aos direitos pessoais destes últimos, para além de lhes imporem a obrigação de manterem as câmaras de vídeo permanentemente ligadas.

A CNPD já se pronunciou nesta matéria, considerando que estas ferramentas são desproporcionadas e violadoras de diversos princípios de proteção de dados.

Além do mais, a situação anómala da pandemia não justifica uma derrogação das normas laborais na matéria.

Outra situação típica desde que surgiu a pandemia e que pode ter implicações relativamente à proteção de dados pessoais é a utilização de tecnologias de suporte ao ensino à distância. Com efeito, uma das consequências da pandemia, no que ao ensino diz respeito, traduziu-se na utilização de plataformas eletrónicas que têm permitido um ensino à distância ou não presencial.

Estes mecanismos de suma importância têm, por um lado, que ser utilizados com algum cuidado, porque têm que acautelar os dados pessoais utilizados, sejam eles dos estudantes sejam dos docentes, e, por outro lado, têm que revestir das garantias necessárias a acautelar a segurança da informação através dessas plataformas veiculadas.

CONCLUSÕES

O direito à saúde é um direito fundamental de natureza social que, como tal, carece da execução em termos legislativos e, subsequentemente, de natureza administrativa.

A proteção dos dados pessoais concretiza um direito e liberdade de proteção da privacidade de cada sujeito que, apesar de tudo, não é um direito absoluto, podendo ter que ceder perante outro direito, desde logo o direito à saúde.

A proteção dos dados pessoais está intrinsecamente ligada à segurança da informação, porque esta engloba dados de diferente natureza, nomeadamente dados pessoais.

Tendências do presente que anunciam o futuro a curto, médio e longo prazo perfilavam-se no sentido de haver situações em que o direito à proteção de dados pessoais surgia a ter que ceder perante outros direitos, de que se pode destacar o direito à saúde.

Toda esta estrutura e organização foi abalada com o surgimento e disseminar do coronavírus e com a correspondente infeção.

A situação pandémica determinou a declaração de estado de emergência e, consequentemente, a tomada de decisões com contornos diferentes das tomadas em situação normal.

É que não só valores mais altos se levantaram e levantam, como estamos perante sinais do futuro no presente.

Não é necessário fazer futurologia, para perceber que nada é como era e nada vai voltar a ser como era antes desta pandemia.

Porém, a presente situação não pode servir de justificação para a instalação de uma mentalidade que não atenda certos valores e direitos relevantes, como é o caso da privacidade e à respetiva proteção.

Por isso, situações comuns como a recolha de dados de saúde dos trabalhadores, concretamente a temperatura corporal, deve ser feita sempre com a garantia de que essa informação de saúde dos trabalhadores é tratada com respeito pela proteção de dados pessoais.

Relativamente aos indivíduos com o diagnóstico de Covid-19, importa realçar a necessidade de que os seus dados pessoais, de identificação e contacto não sejam divulgados, nem seja prestada informação que permita a fácil identificação dessas pessoas. Numa palavra, esta informação, sempre que tenha que ser prestada tem que o ser de modo a respeitar a proteção dos dados pessoais.

Os sistemas de videovigilância, ainda que em tempo de pandemia, têm que continuar a cumprir as normas a que estão legalmente sujeitos. Mesmo durante o estado de emergência continuou a ser proibida a captação de imagens e sons, violando as imposições legais.

Assim, concluímos que, até mesmo em estado de emergência, os direitos não deixam de existir. Por isso, as soluções que eventualmente possam pôr em causa dados pessoais devem respeitar, tanto quanto possível, os princípios de tratamento consagrados no quadro normativo aplicável e as condições de legitimidade previstas para esse tratamento.

É que direitos como o direito à liberdade podem ser suspensos em caso de estado de sítio ou de estado de emergência, que apenas pode ser declarado em situações muito restritas e excecionais, como é o caso da calamidade pública e foi o caso despoletado por esta pandemia.

Ora, se assim é, pode acontecer que a proteção do direito à saúde prevaleça sobre a proteção dos dados pessoais, embora esta solução só possa ocorrer em situações pontuais legitimadas na sua excecionalidade.

Perante este cenário, ponderámos quanto à bondade de algumas soluções adotadas e implementadas nesta pandemia, respeitantes à proteção de dados pessoais, como é o caso de algumas aplicações de rastreamento de situações (sistema de *contact tracing STAYAWAY*; *sistema Trace COVID19*).

Em jeito de síntese conclusiva, afirmamos que, apesar da nossa vontade de acérrima defesa dos dados pessoais e respetiva proteção, terá sempre que haver cedência desta quando outros valores mais relevantes estiverem em causa, como é o causa da saúde de cada um individualmente considerado e saúde pública em geral, postas em causa pela pandemia.

NOTAS

[1] No título II (Direitos, liberdades e garantias) da CRP consagram-se na lei fundamental os direitos, liberdades e garantias pessoais – capítulo I; direitos, liberdades e garantias de participação política – capítulo II; direitos, liberdades e garantias dos trabalhadores – capítulo III.

[2] Artigo 18.º, n.º 1 da CRP:

1. *Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são diretamente aplicáveis e vinculam as entidades públicas e privadas.*

[3] Cf. Artigo 1º, n.º 3 do RGPD:

3 – A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

[4] Cf. artigo 4.º, 1) e 2).

[5] Cf. artigo 5.º.

[6] Note-se que o conceito de consentimento é um dos exemplos de alterações introduzidas pelo regime do RGPD, pois este consentimento, para ser válido, tem que ser expresso, positivo e nunca implícito.

[7] Cf. artigo 9.º do RGPD.

[8] Cf. artigo A da LPD.

[9] Cf. artigos 24.º a 31.º da LPD.

[10] Lei que aprova o regime do estado de sítio e do estado de emergência.

[11] Cf. artigo 3.º, n.º 1 da Lei n.º 44/86, de 30 de setembro.

[12] Cf. artigo 7.º da Lei n.º 44/86, de 30 de setembro.

[13] Cf. artigo 11.º da Lei n.º 44/86, de 30 e setembro.

[14] Cf. artigo 10.º da Lei n.º 44/86, de 30 de setembro.

[15] Cf. artigo 13.º, n.º 1 da Lei n.º 44/86, de 30 de setembro.

[16] Cf. artigo 14.º, alíneas a) a d) da Lei n.º 44/86, de 30 de setembro.

[17] Cf. artigo 17.º da Lei n.º 44/86, de 30 de setembro.

[18] Artigo 4.º, alíneas 1) e 2) do RGPD.

[19] Artigo 35.º n.º 1 e n.º 3, alínea c) do RGPD.

[20] *"O recurso a câmaras incidentes sobre cerca de 70 praias nacionais, que tiram fotografias para cálculo da taxa de ocupação das mesmas, tem em vista garantir o controlo da pandemia da Covid-19.*

Considerando que em causa está a captação de imagens de pessoas em elevadíssimo número que se encontram no espaço público e em condições de especial exposição num local destinado a ser vivido de forma descontraída, o tratamento de dados pessoais só se justifica pela necessidade de exercício de funções do interesse público de prevenção de risco e de proteção da saúde pública, a cargo, no contexto do acesso, ocupação e utilização das praias para a época balnear de 2020, da APA, nos termos do Decreto-Lei n.º 24/2020, de 25 de maio. Assim, o tratamento está limitado temporalmente à época balnear de 2020, para controlo da pandemia da Covid-19."

[21] Nome, data de nascimento, morada, contacto telefónico, *email*, número de utente ou número e identificação fiscal (NIF) e/ou documento de identificação, estado de vigilância, estado de exame, data de início e fim de vigilância, origem do utente, localização (domicílio, hospital ou outra), *link* epidemiológico / contacto, registo de óbito; outros dados, como informações recolhidas nas vigilâncias, como, por exemplo, o resumo dos sintomas.

[22] Cf. as Diretrizes n.º 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19, aprovadas pelo Comité Europeu para a Proteção de Dados.

[23] Cf. artigo 19.º, n.º da CRP.

[24] Seguimos de perto a declaração de Ana Sofia Carvalho, do Conselho Nacional de Ética para as Ciências da Vida de 2 de julho de 2020.

BIBLIOGRAFIA

Andrade, José Carlos Vieira de (2019), *Os Direitos Fundamentais Na Constituição Portuguesa de 1976*, 6.ª edição, Coimbra: Almedina.

Calvão, Filipa Urbano (2018), *Direito da Proteção de Dados Pessoais*, Porto: Universidade Católica.

Canotilho, J. J. Gomes; Moreira, Vital (2014), *Constituição da República Portuguesa Anotada*, vol. I, 4.ª ed. revista – reimpressão, Coimbra: Coimbra Editora.

Canotilho, J. J. Gomes (2018, Reimpressão 2019), *Direito Constitucional e Teoria da Constituição*, 7.ª ed., Coimbra: Almedina.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (ed.) (2007), *Tratamento de dados de saúde: estudos e ensaios clínicos*, 1.ª ed., Lisboa: Comissão Nacional de Proteção de Dados, D.L. 2007.

Cordeiro, A. Barreto Menezes (2020), *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*, Coimbra: Almedina.

EUROPEAN COMMISSION (2020), *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation*, Communication from the Commission to the European Parliament and the Council, Brussels: European Commission.

Galvão, Filipa (2015), *Fórum De Proteção de Dados*, n.º 1, julho 2015, Lisboa: Comissão Nacional de Proteção de Dados.

Leal, Cristina (2016), *O acórdão Schrems do Tribunal de Justiça da União Europeia: repercussões na esfera de ação das autoridades nacionais de proteção de dados*, s.l.: Comissão Nacional de Proteção de Dados.

Miranda, Jorge (2017), *Direitos Fundamentais*, Coimbra: Almedina.

Pinheiro, Alexandre Sousa *et al*. (2018), *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra: Almedina.

LEGISLAÇÃO

Constituição da República Portuguesa

Lei n.º 44/86, de 30 de setembro

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados)

Lei n.º 46/2018 de 13 de agosto

Lei n.º 58/2019, de 08 de agosto