UNIVERSIDADE D
COIMBRA

Carolina Maria Silva Marques

As aplicações móveis criadas no contexto da pandemia covid-19

A garantia do direito à liberdade e o tratamento de dados na Europa e nos países asiáticos

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses orientada pela Professora Doutora Suzana Tavares da Silva e apresentada à Faculdade de Direito da Universidade de Coimbra

Julho de 2021

Faculdade de Direito da Universidade de Coimbra

AS APLICAÇÕES MÓVEIS CRIADAS NO CONTEXTO DA PANDEMIA COVID-19:

A Garantia do Direito à Liberdade e o Tratamento de Dados na Europa e nos Países Asiáticos

NEW APP BORN IN THE COVID-19 CONTEXT:

The right to liberty guarantee and the Access to data in European and Asian Countries

Carolina Maria Silva Marques

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de Mestre)

Orientadora: Professora Doutora Suzana Tavares da Silva

Coimbra, 2021

FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Agradecimentos

À minha equipa maravilha, a minha família: aos meus pais, à minha irmã, tios, primos, avós e aos de coração por me acompanharem e celebrarem as minhas vitórias como se fossem deles. A vossa alegria e amor enchem-me o coração.

Aos meus amigos, desde a primária à faculdade. O vosso ombro amigo esteve sempre presente. Que tenhamos a oportunidade de festejar todos juntos esta etapa.

À minha orientadora, Doutora Suzana Tavares da Silva pela amizade e pela ajuda que me deu durante todo o processo. Numa conjuntura como esta, onde as inseguranças de um aluno são maiores, demonstrou-me que o papel de um orientador passa por motivar e ouvir. Fico-lhe muito grata pelas palavras e deixo a promessa de um dia nos podermos conhecer pessoalmente e não através de um ecrã.

Resumo

A presente investigação visa contribuir para uma visão comparada do enquadramento jurídico das aplicações móveis criadas no contexto da pandemia Covid-19 na Europa e nos Países Asiáticos. Estas ferramentas que surgiram como uma novidade no combate à propagação de contágios baseados no uso das tecnologias para o rastreio de contactos (suprindo as insuficiências e deficiências do rastreio mediante contacto pessoal), não corresponderam às expetativas por terem sido consideradas, na sua maioria, como instrumentos potencialmente restritivos dos direitos, liberdades e garantias.

Sabíamos que a Europa e os Países Asiáticos eram culturalmente diferentes, por isso não nos surpreendeu inteiramente o sucesso que estas ferramentas granjearam na Ásia, nem que as sociedades europeias acabassem por rejeitar o seu uso, apenas procurámos as explicações para estes factos.

Partimos da análise de todas as *APP*s existentes, procurámos compreender os critérios das aplicações móveis e os regimes de tratamento de dados pessoais nos diversos territórios, bem como a origem e a atualidade dos direitos fundamentais, em especial da proteção da privacidade e da liberdade pessoais. É esta a estrutura em que assenta o nosso estudo.

Palavras-Chave: Aplicações Móveis, *APP*s, Covid-19, Dados Pessoais, Direito à Liberdade, Direito à Privacidade, Europa, Países Asiáticos, Pandemia, Rastreio de Contactos.

Abstract

The present study aims to contribute to a broader view of the legal framework of mobile applications created in the context of the Covid-19 pandemic in Europe and in Asian countries. These tools that emerged as a novelty in the fight against the spread of contamination based on the use of technologies for contact tracing (supplying the insufficiencies of the trace based on personal contact) did not meet expectations as most of them were considered potential instruments to restrict rights.

We knew that Europe and Asian countries were culturally different, so it was not entirely surprising how successful these tools were in Asia, nor that European societies ended up rejecting their use. We looked for explanations for these facts.

We have started by analysing all existing *APP*s, we have sought to understand the criteria of mobile applications and the regimes for processing personal data in the different territories, as well as the origin and current status of fundamental rights, in particular the protection of privacy and personal freedom. This is the framework on which our study is based.

Key-words: *APP*s, Asian Countries, Contact Tracing, Covid-19, Europe, Mobile Applications, Pandemic, Personal Data, Right to Freedom, Right to Privacy.

Lista de Siglas e Abreviaturas

AEDP – Autoridade Europeia para a Proteção de Dados
API – Interface de programação de aplicações
APPs – Aplicações móveis
BLE – *Bluetooth Low Energy*
CDF – Carta dos Direitos Fundamentais da União Europeia
CEDH – Convenção Europeia dos Direitos do Homem
CEE – Comunidade Económica Europeia
CL – Código de legitimação
CNPD – Comissão Nacional de Proteção de Dados
COVID-19 – Doença por Coronavírus 2019
CRP – Constituição da República Portuguesa
DGS – Direção-Geral de Saúde
DUDH – Declaração dos Direitos do Homem e do Cidadão
EUA – Estados Unidos da América
GAEN – Notificação de Exposição Google-Apple
INCM – Imprensa Nacional-Casa da Moeda
INESC TEC – Instituto de Engenharia de Sistemas e Computadores, Ciência e Tecnologia
IP – Endereço de protocolo de internet
IPCV – Escola Superior de Tecnologia e Gestão do Politécnico de Viana do Castelo
MERS-CoV – Síndrome Respiratório do Médio Oriente
MFA – Movimento das Forças Armadas
MIT – Massachusetts Institute Technology
OCDE – Organização Europeia de Cooperação Económica
PIPA – Código de Proteção de Informações Pessoais
RGPD – Regulamento Geral sobre a Proteção de Dados
RPI – Chave de proximidade
SARS-CoV2 – Síndrome Respiratória Aguda-Grave – Coronavírus2
SIED – Serviço de Informações Estratégicas e de Defesa
SIS – Serviço de Informações de Segurança
SLD – Subsistema de gestão de códigos de legitimação de diagnóstico

SPD – Subsistema de avaliação de contactos de proximidade

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E

TC – Tribunal Constitucional

TEK – Chave de exposição temporária

TFUE – Tratado sobre o Funcionamento da União Europeia

TJUE – Tribunal de Justiça da União Europeia

UE – União Europeia

Índice

Introdução

As pandemias, encaradas como crises de saúde pública com um grande alcance e maiores consequências que uma epidemia, são fenómenos registados na história desde a Antiguidade, como é exemplo, da Peste Negra, Gripe Espanhola e, mais recentemente, a Covid-19.

Os milhares de óbitos registados levam a que os governos do mundo repensem estratégias de forma a combater a propagação destas doenças uma vez que se prevê, no futuro, que estes acontecimentos sejam mais frequentes atendendo à nossa forma de viver consumista. Assim sendo, com a evolução da tecnologia e as novas formas de comunicar, eclodem as aplicações móveis como novidade no abrandamento dos números assinalados.

A nossa dissertação surge de dúvidas colocadas quanto à utilização destes instrumentos cujo objetivo principal é diminuir os contágios. Questionamos se a liberdade e a privacidade estão a ser restringidas? Como é que é feito o tratamento destes dados e por quem? E se estas *APP*s vão durar para sempre?

A comparação entre a Europa e os Países Asiáticos tem por base as diferenças que ressaltam e o facto de esta crise ter nascido, ao que tudo indica, na China. Posto isto, por um lado encontramos a União Europeia onde a dinâmica é feita entre os países aderentes e a proteção de dados tem por base o Regulamento Geral sobre a Proteção de Dados e, por outro lado deparamo-nos com os Países Asiáticos com uma política rígida e onde a matéria de dados pessoais é, ainda, prematura.

Deste modo, ao longo de três capítulos, analisamos as principais irregularidades destas ferramentas desde que a Organização Mundial de Saúde declarou a Covid-19 pandemia. O estudo de todas as aplicações móveis conhecidas, diplomas e diretrizes relativos à proteção de dados e as principais obras que se debruçam sobre estes temas, levou-nos a concluir que estes instrumentos violam o núcleo dos nossos direitos fundamentais e que, por isso, devem ser reformulados.

A prática de um sistema invasivo nos Países Asiáticos levou ao sucesso destas *APP*s mas violou a privacidade e a liberdade dos cidadãos. Já na União Europeia a escolha, e bem, de um sistema menos invasivo, levou ao insucesso pela falta de publicidade e incentivo ao uso.

Findamos com a certeza que estas conjunturas vão aumentar e que o mundo vai cada vez mais aceitar estas restrições como meio de sobrevivência.

I. As aplicações móveis criadas na Europa e nos Países Asiáticos no contexto da pandemia Covid-19 e os seus parâmetros

A Covid-19 (Doença por Coronavírus 2019), resultante da infeção causada pelo SARS-CoV2 (Síndrome Respiratória Aguda-Grave – Coronavírus 2[1]), foi registada, pela primeira vez, em Wuhan, província de Hubei, República Popular da China, no mês de dezembro de dois mil e dezanove, disseminando-se pelo mundo e chegando, também, a Portugal.

Declarada pandemia pela Organização Mundial de Saúde a onze de março de dois mil e vinte, este vírus, tanto quanto se sabe até ao momento, pode ser transmitido diretamente ou indiretamente, isto é, por contacto próximo entre pessoas ou através de objetos e superfícies[2]. Está em curso uma investigação epidemiológica, pelo que não foi ainda determinada a sua origem. Porém, os especialistas creem que os mercados abertos e os animais são as principais origens deste surto[3].

Num contexto de incertezas socioeconómicas, políticas e de saúde pública, os governos do mundo foram obrigados a tomar medidas com o intuito de minorar a propagação do vírus, que, ainda hoje, é responsável por um elevado risco de contágio e, como consequência, um elevado número de doenças graves e óbitos.

O uso obrigatório de máscara na via pública, os confinamentos domiciliários (impostos por deveres ou obrigações legais), a obrigatoriedade de medir a temperatura à entrada de determinados estabelecimentos públicos, o fecho de escolas e universidades ou a proibição de eventos culturais e desportivos foram, e continuam a ser, algumas das estratégias seguidas pelos governos europeus e asiáticos nas vagas pandémicas.

O nosso estudo centra-se na análise das aplicações móveis (*APP*s) de rastreio de proximidade criadas na Europa e nos Países Asiáticos, no âmbito do rastreio de contactos, e cujo principal objetivo é diminuir a incidência de contágios e o alastrar das infeções pandémicas. Observar cada uma das aplicações, nomeadamente, as suas políticas de privacidade e termos e condições, constitui uma tarefa indispensável não só para a devida comparação e para compreender como é que as mesmas funcionam, como também para

[1] O vírus SARS-CoV foi descoberto, pela primeira vez, em dois mil e dois. A junção do n.º2 deve-se à sua redescoberta em dois mil e vinte que desencadeou, posteriormente, a Covid-19. Direção-Geral da Saúde. (2021). *Perguntas Frequentes.* Acedido em 12 de janeiro de 2021, em: https://covid19.min-saude.pt/category/perguntas-frequentes/?t=retoma-das-atividades-e-agora#retoma-das-atividades-e-agora.
[2] *Ibid.*
[3] *Ibid.*

perceber em que critérios é que se baseiam, nomeadamente: a voluntariedade ou obrigatoriedade, o uso da tecnologia de baixo consumo energético *Bluetooth Low Energy* (*BLE*) ou geolocalização, a escolha entre o modelo descentralizado ou centralizado e, por fim, a interoperabilidade entre aplicações móveis.

O *conctact tracing* ou rastreio de contactos não é um conceito inovador no mundo. Através dele foi possível, em dois mil e catorze, controlar a epidemia Ébola, que assolou o continente africano[4]. A área da saúde pública, a criação das aplicações móveis e, recentemente, a Covid-19, permitiram que o conceito de "rastreio de proximidade" surgisse como tipologia do rastreio de contactos[5]. Desde então, as *APP*s são consideradas ferramentas de alerta importantes por acompanharem as pessoas que foram infetadas ou estiveram em contacto com outras, igualmente infetadas, de maneira a prevenir o contágio[6]. A avaliação da cadeia de transmissão pelas autoridades de saúde pública é imprescindível e decorre durante catorze dias desde a última exposição, evitando, ou procurando assim evitar, a transmissão comunitária[7]. Toda a população está abrangida neste rastreio, todavia a de risco constitui uma preocupação maior para a organização da despistagem[8].

Admitindo que estes instrumentos são essenciais, não os podemos considerar únicos, não só por poderem limitar as liberdades dos utilizadores, nomeadamente, no que diz respeito ao direito à liberdade e privacidade, como ainda por ser possível originarem ou potenciarem eventuais formas de discriminação[9]. Além disso, e por se tratar de aplicações móveis, estão sujeitas a consecutivas atualizações e falhas que são reportadas pelos utilizadores.

Os Ministérios de Saúde e as autoridades de saúde pública, na sua maioria, tomaram a iniciativa de desenvolverem, juntamente com empresas públicas e privadas, estas *APP*s.

---

[4] Organização Mundial de Saúde. (2014). *Contact tracing during an outbreak of Ebola virus disease.* Disease Surveillance and Response Programme Area Disease Prevention and Control Cluster. Genebra.

[5] Organização Mundial de Saúde. (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing.* Interim guidance. Genebra. p.1.

[6] European Commission. (2020). *Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection.* Communication from the commission. Bruxelas. p.1-2.

[7] Designam-se "transmissões comunitárias" as cadeias de transmissão cujas autoridades já não conseguem identificar o número de pessoas envolvidas. Direção-Geral da Saúde. (2021). *Perguntas Frequentes.* Acedido em 12 de janeiro de 2021, em: https://covid19.min-saude.pt/category/perguntas-frequentes/?t=retoma-das-atividades-e-agora#retoma-das-atividades-e-agora.

[8] Organização Mundial de Saúde. (2020). *Digital tools for COVID-19 contact tracing.* Annex: Contact tracing in the context of COVID-19. Genebra. p.4.

[9] European Commission. (2020*).* Ob.Cit. p.4.

Posteriormente, estariam disponíveis nos sistemas *Android* e *iOS*[10] e, em alguns casos, na *Huawei*[11]. As duas multinacionais norte-americanas Google e Apple criaram, em abril de dois mil e vinte, em parceria, a "Notificação de Exposição Google-Apple" (GAEN) com base no Bluetooth. Este projeto de auxílio no rastreio de contactos implica um interface de programação de aplicações (API), isto é, assegura uma interoperabilidade entre sistemas, permitindo que o utilizador mantenha os seus dados pseudonimizados[12] e haja uma maior segurança, privacidade e controlo. Para que uma aplicação seja criada com base nesta tecnologia, o país tem de considerar rigorosos critérios, atendendo a que o código-fonte[13] não é público. Entre os vários critérios, destaca-se o registo de uma aplicação por país que tem de ser aprovada e gerida, unicamente, pela autoridade de saúde pública[14].

O continente asiático foi o pioneiro no lançamento das *APP*s, com Singapura a lançar, a vinte de março de dois mil e vinte, a *TraceTogether* idealizada pelo Ministério da Saúde[15] e pela Agência da Tecnologia do Governo em apoio à SGUnited e cujos critérios se baseiam na voluntariedade e no uso da tecnologia *BLE*[16]. Foi com base neste modelo, em que o

[10] A Google e a Apple, ambas localizadas nos Estados Unidos da América, formam as principais empresas no ramo das telecomunicações. Enquanto rivais e de modo a potenciar as suas vendas no mundo, a Google adquiriu, em 2005, a "empresa" *Android* e, juntamente com a *Open Handset Alliance* (programa que junta empresas como a Motorola, Texas Instruments, Samsung, HTC, entre outras), criaram, em 2008, o sistema operacional *Android* com código aberto. A Apple, pelo contrário, utiliza o sistema *iOS* exclusivo em todos os seus equipamentos – telemóveis, iPods, Ipad e Apple TV. Filho, L. (2017). *Desenvolvendo o seu primeiro aplicativo Android*. 2ª edição, Novatec. Brasil. p.12-13 e Milani, A. (2014). *Programando para iPhone e iPad.* 2ª edição, Novatec. Brasil. p.14.

[11] Fundada em 1988 por Ren Zhengfei, a empresa chinesa utiliza o sistema operacional Huwai nos dispositivos da marca.

[12] A pseudonomização é o processo de tratamento de informação do usuário que encripta os seus dados pessoais. Através de um pseudónimo não será permitido identificar o indivíduo.

[13] Os programas de *software* têm por base um código fonte cujas informações permitem que o programa funcione. Consoante o seu sistema linguístico e as finalidades do projeto, a empresa autora pode, ou não, disponibilizá-los para outras companhias. Noleto, C. (2020, 31 de julho). Código-fonte: o que é e qual sua importância na programação. *Trybe*. Acedido a 11 de fevereiro de 2021, em: https://blog.betrybe.com/tecnologia/codigo-fonte/.

[14] O registo da aplicação oficial do país não invalida que existam outras secundárias. O estudo revelou que, tanto na Europa como na Ásia, atendendo à densidade populacional e ao território, a existência de mais do que uma aplicação móvel de rastreio de proximidade pode ser mais eficaz. Tanto a India como a Espanha, contam com quatro aplicações em código aberto. Coloca-se a questão de saber se estas seguem os mesmos trâmites ou se, pelo contrário, adotam uma tecnologia mais invasiva. Apple e Google. (2020). *Exposure Notifications, Frequently Asked Questions*. Preliminary – Subject to Modification and Extension. Estados Unidos da América. p.2-7.

[15] eHealth Network. (2020). *Mobile applications to support contact tracing in the EU's fight against COVID-19*. Common EU Toolbox for Member States. Bruxelas. p.9.

[16] O *Bluetooth Low Energy* ou Bluetooth 4.0 foi lançado em 2011 e surge como uma tecnologia de baixo consumo de bateria e troca de dados. Estima-se que um dispositivo com esta tecnologia dura de quatro a cinco anos, uma vez que quando não é utilizada entra em modo de hibernação. O Bluetooth, tal como o conhecemos, requer um maior consumo de bateria e consegue recolher um maior número de dados.

código-fonte é público, que surgiram as primeiras aplicações móveis e o modelo adotado acaba por não ser muito diferente de país para país.

O usuário que instala a *APP* recebe uma chave de exposição temporária (TEK), criada diariamente. Este código, posteriormente, será cruzado com a chave de proximidade (RPI) que, por sua vez, é gerada a cada dez/vinte minutos, conforme o contacto com outros *smartphones* próximos. No caso de este revelar uma grande intensidade, presume-se que existiu um "*handshake"*, ou seja, um *contacto relevante*, que justifica um cruzamento de dados que determinará se estiveram ou não durante quinze ou mais minutos, numa distância igual ou inferior a dois metros. Se assim for, então a pessoa será notificada para fazer um teste à Covid-19. As chaves mencionadas anteriormente ficarão armazenadas no telemóvel durante catorze dias e são produzidas aleatória e criptograficamente.

O controlo e a privacidade são, em grande medida, assegurados pelo sistema DP-3T. O seu propósito é minimizar a recolha e tratamento de dados, não permitindo que as pessoas, entre si, identifiquem as identidades dos titulares dos aparelhos ou os locais em que ocorreram os contactos de relevo[17].

O cálculo do risco de infeção pode exprimir-se através de uma cifra de cores à semelhança de um semáforo, onde o verde representa um perigo baixo e o vermelho, pelo contrário, um risco elevado. É pertinente explorarmos esta forma de comunicação, pois na China, por exemplo, a *APP Alipay Health Code*, desenvolvida pela *Ant Financial and Alipay – Alibaba*, funciona através de um *QR Code* diário que permite rastrear os cidadãos através de geolocalização[18]. Conforme o histórico de locais dos últimos quinze dias e as áreas visitadas, poderá ser atribuída uma cor verde (sem necessidade de isolamento), amarelo (sete dias de isolamento) ou vermelho (catorze dias de isolamento). A Comissão Nacional de

[17] Real Decreto n.º44, de 26 de junho de 2020. *Revista do Estado Belga* – Ed. 2. Monitor Belge. Ministério dos Assuntos Sociais e Saúde Pública. p.48432-48433.

[18] A tecnologia da geolocalização permite localizar e rastrear os movimentos das pessoas no seu quotidiano e, ainda, determinar a sua permanência nos locais. No caso em concreto, esta ferramenta de auxílio mais invasiva, em comparação com o *BLE*, permitirá identificar a linha de contágio do indivíduo. Os dados recolhidos são dados pessoais e o seu tratamento obriga a que seja criado um código de conduta pela sua particularidade. Pinheiro, A.S., Moura, C. (2016). Utilização de tecnologia de geolocalização e o tratamento de dados pessoais no regime jurídico português: a propósito da Deliberação n.º7680/2014 da Comissão Nacional de Proteção de Dados e jurisprudência posterior. *Fórum de Proteção de Dados*. n.º3:15-31.

Saúde da China, ao decretar que a entrada em qualquer espaço público exige um *QR Code* verde, torna a aplicação obrigatória[19].

Por último, importa referir que, no estudo de cada aplicação, rapidamente concluímos que as políticas de privacidade e termos e condições apresentadas na Europa são muito mais completas e transparentes do que na Ásia. Repare-se que, em alguns dos países não existe sequer transparência quanto à existência da própria *APP*. Serve de exemplo a aplicação do Irão, cuja única informação obtida é que a mesma não pode ser instalada na *App Store* ou *Google Play*[20]. Similarmente, a *APP Morchana* da Tailândia, apesar de estar disponível no sistema *Android* e *iOS*, não só os seus critérios não estão patentes, como não há informação da recolha e tratamento de dados.

1. O Modelo Centralizado e o Modelo Descentralizado

O primeiro requisito que nos propusemos analisar é a escolha entre o modelo centralizado e descentralizado na criação destas *APPs* e quais as implicações que daí decorrem para a vulnerabilidade da proteção da privacidade do utilizador[21]. Teoricamente, qualquer um é adequado à proteção da privacidade. Ambos permitem gerar "dados arbitrários" de maneira a que as pessoas não identifiquem o seu *hanshake*, ou seja, não reconheçam o seu contacto próximo.

A principal diferença está no local onde os dados são armazenados. O modelo central, preferido no continente asiático, armazena os dados num servidor único, cujo tratamento ficará à responsabilidade da autoridade sanitária[22]. Os governos que adotem este modelo

[19] Pequenino, K. (2020, 6 de março). China atribui código QR aos cidadãos para conter coronavírus [Versão eletrónica]. *Jornal Públic*o. Acedido em 23 de janeiro de 2021, em: https://www.publico.pt/2020/03/06/tecnologia/noticia/china-atribui-codigo-qr-cidadaos-conter-coronavirus-1906462 e Gillmor. D. K. (2020). *Principles For Technology-Assisted Contact-Tracing*. ACLU. Estados Unidos da América. p.4-5.

[20] Abdelkrim. (2020, 19 de abril). Covid-19, Mobile apps that preserve privacy. And the winner is… *Medium*. Acedido a 15 de janeiro de 2021, em: https://medium.com/@Abdelkrim/covid-19-mobile-apps-that-preserve-privacy-and-the-winner-is-68c72e098fca.

[21] Existem fontes que indicam existência de um modelo híbrido, isto é, a junção entre os dois modelos que permite o armazenamento de dados no dispositivo móvel e no servidor único. Todavia estas fontes não se revelaram fidedignas pelo que, para efeitos do estudo, não vamos analisar.

[22] European Commission. (2020). *Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection*. Communication from the commission. Bruxelas. p.9-10.

devem coletar o mínimo de dados possíveis ou necessários para cumprir a finalidade[23]. A título de exemplo, podemos referir o Governo das Filipinas, com a aplicação *StaySafePH*[24] ou ainda a *APP Pedulilindungi* (Indonésia), que embora não seja evidente o local onde os dados são armazenados, presume-se que respeitam estes parâmetros técnicos[25].

O modelo descentralizado armazena os seus dados no dispositivo móvel. A União Europeia recomenda[26] o uso deste plano, pois considera que o mesmo representa um menor risco para o cidadão e reflete um maior respeito pelo *princípio da minimização*[27]. No caso de um contacto próximo com alguém positivo, esta abordagem permite que o utilizador partilhe os seus dados de saúde com a autoridade competente. O consentimento é visto, neste contexto, como uma orientação ao usuário e, em certos casos, como partilha para fins estatísticos e de estudo da doença[28]. Veja-se o caso da Alemanha, que além da *APP* de rastreio de contacto próximo (*Corona-Warn-APP),* criou uma aplicação móvel (*Corona-Datenspende*) que se destina à doação de dados, de forma consentida e anónima[29].

Em resumo, os Governos podem adotar um ou outro modelo, conquanto respeitem o princípio da minimização. Não obstante o controlo e segurança como princípios basilares, ambas as abordagens têm vulnerabilidades.

[23] Organização Mundial de Saúde. (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing.* Interim guidance. Genebra. p.4.
[24] Stay Safe Philippines. (2020). *Data Privacy*. Acedido em 25 de janeiro de 2021, em: https://www.staysafe.ph/data-privacy.
[25] Norton Rose Fulbright. (2020). *Contact Tracing apps in Indonesia: A new world for data privacy*. Estados Unidos da América. p.2.
[26] Tal como referimos, a União Europeia recomenda o uso e não obriga. O governo francês adotou o modelo centralizado na sua *APP – TousAntiCovid.* Já países como a Bélgica (*Corona Alert*) e a Dinamarca (*Smittestop*), adotaram o modelo descentralizado. Ministère des Solidarités et de la Santé. (2020). *TousAntiCovid: Respostas às suas perguntas*. Acedido em 25 de janeiro de 2021, em: https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/tousanticovid, Cf. Art 14.º, §3, 1º. Real Decreto n.º44, de 26 de junho de 2020. *Revista do Estado Belga* – Ed. 2. Monitor Belge. Ministério dos Assuntos Sociais e Saúde Pública. p.48447 e Sundheds-Og Aeldreministeriet. (2020). *Aftale om frivilling smittesporingsapp for Covid-19.* Dinamarca. p.1.
[27] eHealth Network. (2020). *Mobile applications to support contact tracing in the EU's fight against COVID-19*, Common EU Toolbox for Member States. Bruxelas. p.14-15 e European Commission. (2020). Ob.Cit. p.10.
[28] Organização Mundial de Saúde. (2020). Ob.Cit. p.4.
[29] Institut, R. K. (2020, 1 de maio). Wie funktioniert die Corona-Datenspende?. *Corona-Datenspende*. Acedido a 25 de janeiro de 2021, em: https://corona-datenspende.de/science/reports/how/.

2. *Bluetooth Low Energy* e Geolocalização

O continente europeu e o continente asiático divergem, na preferência entre *Bluetooth Low Energy* ou Geolocalização para o rastreio de contactos. Atente-se que este critério é o que define a *APP* e o que permite perceber de que forma é que os direitos, liberdades e garantias, mais concretamente, o direito à liberdade e à vida privada são afetados.

A Comissão Europeia recomenda o uso do *Bluetooth Low Energy*. No documento emitido por esta instituição europeia, com o título "Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados", frisa-se que esta tecnologia é mais precisa e adequada à finalidade[30]. As aplicações móveis da Europa seguiram esta recomendação, mas existem exceções. A Bulgária (*Corona Alert*) utiliza um sistema híbrido. Um cidadão búlgaro pode voluntariamente partilhar a sua localização para que, no caso de emergência, possa ser encontrado[31]. Também, a *APP* cipriota, patrocinada pela *Safe Paths do Massachusetts Institute Technology* (MIT), opta pela geolocalização[32].

O processamento de dados por localização não parece a solução mais adequada à luz da legislação europeia e do nosso ordenamento jurídico. A recolha dos locais e da hora do contacto próximo não aparenta ser significativo quando comparado com a data dos primeiros sintomas para se determinar o isolamento da pessoa[33]. Poderíamos admitir que a localização facilitaria a identificação das cadeias de transmissão, no entanto, este tipo de abordagem requer cuidado pela extrema invasão na vida da população.

No seio destes instrumentos pode existir discriminação, no sentido de que nem todos têm acesso a *smartphones* atualizados[34] ou porque não têm estes equipamentos. Singapura, diminuiu este défice ao desenvolver o "*Token*", um objeto que se assemelha a um *pager* fornecido pelo governo, gratuita e voluntariamente. O *Token* utiliza a tecnologia *Bluetooth*

---

[30] Comissão Europeia. (2020). *Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados*. Jornal oficial da União Europeia. Bruxelas. p.6.

[31] Virusafe. (2020). *Termos e Condições*. Acedido em 27 de janeiro de 2021, em https://virusafe.io/information/terms-of-use.html.

[32] CovTracer. (2020). *CovTracer Privacy Policy.* Chipre. p. 3-4.

[33] European Commission. (2020*). Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection.* Communication from the commission. Bruxelas. p.8-9.

[34] As aplicações móveis só estão disponíveis em *smartphones* com *Android* 6 e Iphones *iOS* 13.5 impossibilitando qualquer utilizador com equipamento inferior de fazer *download*.

Low Energy e reserva os dados no próprio equipamento durante vinte e cinco dias[35]. A União Europeia, neste aspeto, considera que deve haver uma maior acessibilidade e inclusão, porém nenhuma *APP* utiliza estes *wearables*[36].

No Barém (*BeAware Baharin*) e no Kuwait (ك ل ون ش, *How Are you?*), com o intuito de circunscrever os casos positivos, foram criadas pulseiras eletrónicas capazes de monitorizar os indivíduos que estão em casa. Num estudo recente, a Amnistia Internacional acusou estas *APP*s, juntamente com a Noruega, de serem as mais invasivas no mundo[37]. Arriscamo-nos a fazer uma analogia com os meios técnicos de controlo à distância (vigilância eletrónica)[38] que impõem ao arguido a obrigação de não se ausentar, ou de não se ausentar sem autorização, da habitação própria ou de outra em que de momento resida (artigo 201.º do Código de Processo Penal). Nesta condição, o doente que sair da sua residência pode enfrentar pena de prisão e/ou multa.

No nosso entender, como veremos melhor mais adiante, as aplicações de localização violam o princípio da proporcionalidade, subprincípio do princípio do estado de direito democrático. Assim sendo, devemos privilegiar a tecnologia *Bluetooth Low Energy* mesmo que esta possa apresentar defeitos: erros de leitura na distância entre as pessoas, falsos positivos, falhas nos alarmes de contágio, entre outros.

3. A obrigatoriedade e voluntariedade

Ao longo do estudo das medidas adotadas para controlar e minorar os efeitos perversos da pandemia Covid-19, percebemos que as aplicações móveis podem ser uma vantagem, desde a testagem da população à comunicação dos sintomas a ter em conta. Todavia, estes

[35] TraceTogether. (2020). *TraceTogetherToken*. Acedido em 27 de janeiro de 2021, em: https://www.tracetogether.gov.sg/common/token/index.html.

[36] Cit. "Inclusiveness is all the more important for those, like children, vulnerable groups, and elderly persons, who often do not have smartphone and/or connected device, or may not be digital-savvy enough to install and properly use the tracing app.". eHealth Network. (2020). *Mobile applications to support contact tracing in the EU's fight again COVID-19, Common EU Toolbox for Member States*. Bruxelas. p.19-20.

[37] Amnistia Internacional. (2020, 16 de junho). Aplicações de rastreio de contactos de Noruega, Bahrein e Kuwait entre as mais perigosas para a privacidade. Acedido a 27 de janeiro de 2021, em: https://www.amnistia.pt/aplicacoes-de-rastreio-de-contactos-de-noruega-bahrein-e-kuwait-entre-as-mais-perigosas-para-a-privacidade/.

[38] Cf. Lei n.º 33/2010, de 2 de setembro. *Diário da República n.º171/2010 – 1ª Série*. Assembleia da República. Lisboa.

não são os únicos meios disponíveis para executar aquelas tarefas e, por essa razão, devemos refletir sobre o seguinte ponto: a obrigatoriedade e a voluntariedade.

A Europa, atualmente, não tem nenhuma *APP* obrigatória, não obstante terem existido propostas nesse sentido, como sucedeu na Eslovénia (*#Ostanizdrav*). Em contrapartida, na Ásia, além dos exemplos enunciados anteriormente, tem ainda aplicações obrigatórias na Turquia (*Hayat Eve Sigar*)[39] e no Qatar (*EHTERAZ*), desde vinte e dois de maio de dois mil e vinte[40].

A Diretiva 2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (*Eprivacy Directive*), permite a utilização obrigatória quando seja necessário, adequado ou proporcionado para salvaguardar, neste caso, a saúde pública[41]. A Organização Mundial de Saúde e a Comissão Europeia recomendam o regime da voluntariedade e acrescentam que uma pessoa que não descarregue a aplicação não deve ser punida.

Em suma, parece-nos desproporcionado limitar o livre-arbítrio da população. As *APP*s devem ser vistas como utensílios do quotidiano que transmitam confiança no seu serviço e, por isso, a sua utilização deve provir dessa confiança e não de uma norma coativa.

4. A Interoperabilidade

Apesar de a conjuntura atual apresentar o distanciamento social como uma das medidas mais eficazes no combate à propagação do vírus e onde, por essa razão, as viagens pelo mundo são feitas em menor número, ainda assim há sempre deslocações necessárias (para assistência a familiares, para assegurar as relações económicas, para os trabalhadores transfronteiriços e internacionais, etc…). Por isso, a Comissão Europeia determinou que estes programas de rastreio automatizado de contactos devem ser interoperáveis, ou seja, as aplicações devem ser capazes de trocar informações entre si para que o cidadão continue atualizado, em caso de deslocamento além-fronteiras.

[39] Norton Rose Fulbright. (2020). *Contact Tracing apps in Turkey: A new world for data privacy*. Estados Unidos da América. p.1.
[40] Government Communications Office. (2021). *Preventive Measures*. State of Qatar. Acedido em 28 de janeiro de 2021, em: https://www.gco.gov.qa/en/preventative-measures/.
[41] Cf. Artigos 5.º e 15.º, n.º1. Diretiva 2002/58/CE, de 12 de julho. *Jornal Oficial das Comunidades Europeias.* Parlamento Europeu e do Conselho.

Hodiernamente, a interoperabilidade não está presente no mundo, nem em toda a União Europeia[42]. A comunicação e a cooperação entre os Estados-Membros e outros países na transmissão de dados mínimos, requer protocolos entre as autoridades de saúde públicas e a Organização Mundial de Saúde. No entanto, entende-se que neste serviço devem ser definidos critérios iguais para todos, de modo a não existir, futuramente, nenhuma incongruência nas interrupções das cadeias de transmissão transfronteiriças – a definição do contacto próximo (distância e duração da exposição), o método utilizado pela *APP* para registar a ligação e, por fim, o armazenamento de dados (período necessário)[43].

A Irlanda (*Covid Tracker*) desenhou um modelo de interoperabilidade interna com a Irlanda do Norte (*StopCovid NI*) de maneira a abranger um maior número de habitantes e podemos questionar se o mesmo não deveria ter sido adotado entre Portugal e Espanha. Atente-se que, em caso de deslocação, o utilizador não deve utilizar a *APP* do seu país de origem, mas desconectá-la para descarregar a do país estrangeiro.

Em síntese, a liberdade de circulação das pessoas, para qualquer finalidade, pode ter a interoperabilidade como solução.

5. A aplicação STAYAWAY COVID em Portugal

Em Portugal, o Instituto de Engenharia de Sistemas e Computadores, Ciência e Tecnologia (INESC TEC), o Instituto de Saúde Pública da Universidade do Porto e as empresas Keyruptive e Ubirider[44], desenvolveram a *APP* STAYAWAY COVID, aprovada pelo Decreto-Lei n.º 52/2020, de 11 de agosto. Este diploma, aprovado após pronúncia da Comissão Nacional de Proteção de Dados (CNPD)[45], baseia-se nas recomendações da

[42] Cit. «"Portal Federativo", um portal de acesso à rede gerido pela Comissão através de uma ferramenta informática segura que recebe, armazena e disponibiliza um conjunto mínimo de dados pessoais entre os servidores de suporte dos Estados-Membros para efeitos de assegurar a interoperabilidade das aplicações móveis nacionais de rastreio de contactos e de alerta;». Cf. Artigo 1.º, n.º1, alínea j). Decisão de Execução (UE) 2020/1023, de 15 de julho. *Jornal Oficial da União Europeia.*

[43] eHealth Network. (2020). *Interoperability guidelines for approved contact tracing mobile applications in the EU*. Bruxelas. p.4-5.

[44] Desenvolvido no âmbito do programa "Iniciativa Nacional Competência Digitais e.2030, Portugal INcoDe.2030", um programa desenvolvido pelo Governo em 2017, visa promover as competências digitais e o desenvolvimento tecnológico de Portugal investindo em jovens qualificados e requalificando os recursos humanos portugueses. Programa INCoDe.2030. *INCoDe.2030*. Acedido em 16 de janeiro de 2021, em: https://www.incode2030.gov.pt/incode2030.

[45] Presidida por Filipa Calvão, a Comissão Nacional de Proteção de Dados, entidade administrativa independente, funciona junto da Assembleia da República. A este órgão compete controlar e fiscalizar a recolha

Comissão Europeia e no Regulamento Geral sobre a Proteção de Dados (RGPD), e estabelece a voluntariedade e o uso da tecnologia *Bluetooth Low Energy*[46], como na generalidade das aplicações da Europa.

A entidade responsável pelo tratamento de dados é a Direção-Geral de Saúde (DGS). Esta responsabilidade inclui, tal como o artigo 3.º enumera, "*a geração, comunicação, armazenamento e processamento de dados, bem como a articulação entre os intervenientes no sistema (...)"*[47]. Os intervenientes aqui enunciados, contratados pela DGS, são os Serviços Partilhados do Ministério da Saúde, E.P.E (SPMS) e meios técnicos necessários[48] para que a aplicação tenha êxito e logre os seus objetivos.

Entre os modelos centralizado e descentralizado, descritos anteriormente, a STAYAWAY COVID insere-se num modelo descentralizado, por se entender adequado à privacidade e ao anonimato do utilizador. Além deste plano, adota ainda um método de "arquitetura semi-descentralizada", ou seja, junta o dispositivo móvel pessoal com um sistema que se subdivide entre: o subsistema de avaliação de contactos de proximidade (SPD), controlado pela Imprensa Nacional-Casa da Moeda (INCM), e o subsistema de gestão de códigos de legitimação de diagnóstico (SLD), controlado pelo SPMS[49]. Ambos estão ligados ao funcionamento da aplicação.

Sabemos, desde logo, que as *APP*s geram duas chaves – as TEK e as RPI. Quando o utilizador faz o *download* da aplicação, o sistema SPD será o responsável por armazenar as TEK e, no caso de haver contacto próximo com alguém infetado, será necessário cruzar as chaves TEK com as RPI, atendendo à distância e à duração do contacto, de modo a calcular o risco de contágio e determinar o estado do utilizador: "sem risco", "alerta de potencial contacto de risco" ou "diagnosticado com covid". Se o utilizador testar positivo à Covid-19, nesse caso, o sistema SLD será responsável por colocar em contacto o doente e o profissional de saúde, que fará o devido diagnóstico através de um código de legitimação (CL) cedido

e o tratamento de dados pessoais, combinado com o respeito dos direitos fundamentais. Comissão Nacional de Proteção de Dados. (2021). *O que somos e quem somos*. Acedido em 16 de janeiro de 2021, em: https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/.

[46] Cf. Artigo 1.º. Decreto-Lei n.º52/2020, de 11 de agosto. *Diário da República n.º155/2020 – 1ª Série*. Ministério da Economia e da Transição Digital. Lisboa.

[47] Cf. Artigo 3.º. *Ibid.*

[48] Cf. Sumário. *Ibid.*

[49] Deliberação/2020/277, de 29 de junho. *Processo PRE/2020/6.* Comissão Nacional de Proteção de Dados. Lisboa. p.3. e STAYAWAY COVID. (2020). *Política de Privacidade.* Acedido em 16 de janeiro de 2021, em: https://stayawaycovid.pt/politica-de-privacidade/.

por via telefónica e submetido na aplicação móvel pelo doente. A este diagnóstico acrescenta-se um acompanhamento dos sintomas (no caso de existirem)[50].

A CNPD admite que este é o melhor modelo para proteger os dados dos utilizadores. O facto de a *APP* STAYAWAY COVID ter, igualmente, o código-fonte público, isto é, estar acessível a qualquer pessoa que pretenda ver quais os trâmites que a aplicação segue, permite entender quais os perigos associados ao seu uso, bem como as suas limitações no que concerne aos direitos, liberdades e garantias[51].

A transparência é um princípio basilar na construção destas aplicações, assim como, veremos mais tarde, o consentimento. Entende-se que o utilizador tem o *poder de escolha* desde que instala a aplicação até ao momento em que decide partilhar o seu estado de saúde com o profissional que o acompanhará[52]. No fundo, o usuário deverá ter o controlo da sua informação, tendo o direito de retificar[53] ou mesmo de a excluir[54] no caso de apagar a *APP*.

Em Portugal, a falta de confiança ressentiu-se nos números dos *downloads* realizados pelos portugueses. A eficácia destes instrumentos reflete-se na quantidade de pessoas que os instalam e usam para mitigar o contágio. Recentemente, em Portugal o INESC TEC deu a conhecer que dos três milhões de portugueses que instalaram a *APP,* 1,8 milhões deixaram de usar a *STAYAWAY COVID*[55], o que em termos percentuais, corresponde a 60%. As razões apontadas foram a ausência de códigos gerados, a falta de conhecimento no uso da aplicação por parte dos médicos[56] e a falta de recomendação por parte do executivo e autoridades de saúde[57].

---

[50] Deliberação/2020/277, de 29 de junho. *Processo PRE/2020/6.* Comissão Nacional de Proteção de Dados. Lisboa. p.4-5.
[51] *Ibid.* p.11.
[52] *Ibid.* p. 22.
[53] Cf. Artigo 16.º. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas.
[54] Cf. Artigo 17.º. *Ibid.*
[55] Séneca, H. (2021, 26 de janeiro). StayAway Covid já está disponível para iPhones mais antigos. [Versão eletrónica]. *Jornal Expresso*. Acedido em 11 de fevereiro de 2021, em: https://expresso.pt/sociedade/2021-01-26-StayAway-Covid-ja-esta-disponivel-para-iPhones-mais-antigos.
[56] A Associação D3- Defesa dos Direitos Digitais, associação portuguesa sem fins lucrativos, em comunicado à imprensa, repudiou a falta de conhecimento no uso da aplicação por parte dos médicos mencionada pelo INESC TEC e frisa que esta aplicação nunca cumpriu os seus objetivos. Como tal, o encerramento do projeto, na sua opinião, seria a solução. Associação D3-Defesa dos Direitos Digitais. (2021). *D3 condena ataque aos médicos e exige o fim da app Stayaway Covid*. Acedido em 20 de janeiro de 2021, em: https://www.direitosdigitais.pt/comunicacao/comunicados/114-d3-condena-ataque-aos-medicos-e-exige-fim-da-app-stayaway-covid.
[57] Pequenino, K. (2021, 15 de janeiro). 60% já apagaram a StayAwayCovid: são 1,8 milhões de portugueses [Versão eletrónica]. *Jornal Público.* Acedido em 18 de janeiro de 2021, em:

O Governo, no dia catorze de outubro de dois mil e vinte, data em que foi decretado o estado de calamidade, apresentou a Proposta de Lei n.º 62/XIV ao abrigo do artigo 197.º, número 1.º, alínea d) da Constituição da República Portuguesa (CRP). Este diploma, não só pretendia estabelecer a obrigatoriedade das máscaras na via pública quando não fosse possível assegurar o distanciamento social, como também a obrigatoriedade do uso da *APP* STAYAWAY COVID "*no contexto laboral ou equiparado, escolar, académico*", onde se incluem, Forças Armadas e de Segurança e Administração Pública[58]. A fiscalização destas disposições competiria à Guarda Nacional Republicana, à Polícia de Segurança Pública, à Polícia Marítima e às Polícias Municipais, que, em caso de incumprimento, aplicariam o artigo 3.º do Decreto-Lei n.º 28-B/2020, de 26 de junho, que estabelece o regime contraordenacional, no âmbito da situação de calamidade, contingência e alerta.

Face a esta proposta, constitucionalistas portugueses, nomeadamente Vital Moreira e Jorge Reis Novais, a Associação D3-Defesa dos Direitos Digitais[59], os vários partidos com assento na Assembleia da República[60] e a CNPD pronunciaram-se sobre a sua inconstitucionalidade. No global, destaca-se a falta de uma obrigação legal ao uso diário do telemóvel, o que desde logo, criaria uma lacuna para quem não tem este tipo de equipamentos e, ainda, se acrescenta o perigo que constituiria para a defesa dos direitos, liberdades e garantias dos cidadãos.

A CNPD, no Parecer/2020/129, emitido ao abrigo das suas competências[61], desconstrói a proposta legislativa antes mencionada, concluindo que este tipo de medidas "*representaria*

https://www.publico.pt/2021/01/15/tecnologia/noticia/60-ja-apagaram-stayaway-covid-sao-18-milhoes-portugueses-1946366.

[58] Proposta de Lei n.º 62/XIV, de 14 de outubro. Presidência do Conselho de Ministros. Lisboa, em especial os n.ºs 1 e 3 do artigo 1.º.

[59] Cit. "*A obrigação de instalação de uma app, qualquer que seja, é uma intrusão inédita e anti-democrática digna de autoritarismo chinês e não do modelo europeu de sociedade.".* Associação D3-Defesa dos Direitos Digitais. (2020). *Comunicado sobre Stayaway Covid*. Acedido em 20 de janeiro de 2021, em: https://www.direitosdigitais.pt/comunicacao/comunicados/106-comunicado-sobre-stayaway.

[60] Diário de Notícias. (2020, 15 de outubro). O que dizem os partidos sobre a obrigatoriedade da app StayAway Covid. [Versão eletrónica]. *Diário de Noticias*. Acedido em 20 de janeiro de 2021, em: https://www.dn.pt/poder/o-que-dizem-os-partidos-sobre-a-proposta-de-obrigatoriedade-da-app-stayaway-covid-12924386.html.

[61] Cf. Artigo 57.º, n.º1, alínea c) e artigo 36.º, n.º4 do Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados.* Parlamento Europeu e do Conselho da União Europeia. Bruxelas e Artigo 3.º, Artigo 4.º, n.º2 e artigo 6.º, n.º1, alínea a) da Lei n.º 58/2019, de 8 de agosto. *Diário da República n.º151/2019 – 1ª Série.* Assembleia da República. Lisboa.

abrir a porta a restrições futuras do mesmo tipo, em circunstâncias diferenciadas, mesmo que sob a inovação do bem comum"[62].

A CNPD, no seu parecer, subscreve essencialmente o que a doutrina vem afirmando a propósito das exigências constitucionais em matéria de restrição de direito, liberdades e garantias. Todavia, acrescenta que não é a única questão a apontar ao regime da obrigatoriedade da *APP*. A fiscalização das entidades policiais, regulada no artigo 5.º da Proposta de Lei n.º 62/XIV, não foi bem delineada. O modo de como esta é feita pelas entidades entra em contradição com a reserva da vida privada[63] e com o artigo 34.º, número 4.º da CRP que regula a "Inviolabilidade do domicílio e da correspondência", desde ter de exibir à polícia o seu telemóvel quando solicitado, até provar que descarregou a aplicação. Tal como a Comissão Nacional de Proteção de Dados afirma, a vida privada de cada um está "*(…) em muitos aspetos e dimensões, espelhada no seu telemóvel, sobretudo quando este corresponde a um smartphone*"[64]. Em suma, o acesso quase livre destas entidades policiais representaria uma violação do direito à vida privada e liberdade e, como tal, a CNPD concluiu pela inconstitucionalidade da proposta do Governo. A medida acabaria por não ser adotada, tendo sido aprovada apenas, pela Lei n.º 62-A/2020, de 27 de outubro, a obrigatoriedade de uso de máscara em espaços públicos[65].

Note-se que, ainda no parecer, é acentuada a ideia de que este tipo de instrumentos não são únicos, mas sim complementares e que, como tal, não devem substituir-se aos direitos fundamentais presentes na nossa legislação e na legislação europeia.

Por fim, a aplicação STAYWAY COVID, tal como as restantes aplicações conhecidas no mundo, é temporária e apagar-se-á assim que a pandemia terminar e a mesma cumprir a sua finalidade[66]. Não se exclui, porém, a possibilidade de que esta possa ser apagada antes.

[62] Parecer/2020/129, de 27 de outubro. *Processo PAR/2020/92*. Comissão Nacional de Proteção de Dados. Lisboa. p.19.
[63] Cf. Artigo 26.º da Constituição da República Portuguesa.
[64] Parecer/2020/129, de 27 de outubro. Ob. Cit. p.9-10.
[65] *Ibid.* p.8-10.
[66] Cf. Artigo 5.º. Decreto-Lei n.º52/2020, de 11 de agosto. *Diário da República n.º155/2020 – 1ª Série*. Ministério da Economia e da Transição Digital. Lisboa.

II. O tratamento de dados pessoais em contexto pandémico: o *standard* europeu

O ápice do mundo digital e da transferência de informação pessoal foi atingido durante a pandemia Covid-19 com a criação de plataformas *online*, entre elas as aplicações móveis como ferramenta de auxílio na diminuição de contágios e infeções pandémicas. Consequentemente, a proteção do direito à vida privada, enquanto meio de garantia da liberdade do ser humano, ressurtiu pelo ceticismo existente face a estas aplicações e pelo seu mau funcionamento, como já comprovamos no ponto anterior.

Para efeitos deste capítulo, importa perceber em que consiste o conceito de dados pessoais e o seu tratamento no continente europeu e asiático, analisando as legislações existentes. Observaremos, também, o género de dados que são pedidos nas aplicações e quem são as entidades responsáveis (públicas e privadas), os seus limites, os modelos de consentimento requeridos e o direito ao esquecimento do usuário.

Os dados pessoais, atualmente, podem ser requeridos em qualquer local que visitemos – *sites*, empresas, inquéritos, companhias de telecomunicações, entre outros. Estas informações permitirão identificar qualquer pessoa e, como tal, o seu tratamento terá de ser refletido. O Regulamento Geral sobre a Proteção de Dados[67], publicado na União Europeia em dois mil e dezasseis como resposta ao aumento de dados no mercado interno e a livre circulação no mercado externo[68], regula alguns exemplos destas informações - "*um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, psicológica, genética, mental, económica, cultural ou social*"[69] -, todavia podemos acrescentar outros: *email*, endereço de protocolo de internet (*IP*)[70], matrícula de um automóvel, um *curriculum vitae* ou um som de uma voz registada.

A proteção de dados pessoais, nomeadamente, o seu tratamento constitui um direito fundamental regulado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia,

[67] O Regulamento Geral sobre a Proteção de Dados revogou a Diretiva 95/45/CE, 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.
[68] Castro, C.S. "Art8.º - Proteção de dados pessoais" em Silveira, A. e Canotilho, M. (2013). *Carta dos Direitos Fundamentais da União Europeia: comentada*. Almedina. Coimbra. p.121.
[69] Cf. Artigo 4.º, n.º 1. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas.
[70] O endereço IP serve para identificar uma rede ou um dispositivo que navegue na Internet.

no artigo 16.º, número 1.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e, na legislação portuguesa, no artigo 35.º da CRP[71]. Não obstante, não é um direito absoluto e pode entrar em colisão com outros direitos fundamentais regulados e bens jurídicos. Assim, em caso de conflito é necessário limitar o seu exercício de forma a chegar a uma concordância prática.

O tratamento de dados diz respeito a um conjunto de ações automatizadas ou não automatizadas que, uma vez desconstruídas, explicam os diferentes momentos deste procedimento. Para o nosso estudo importa referir, a sua recolha, organização, conservação, utilização, limitação e a destruição[72]. Os responsáveis por este processo devem assegurar a confidencialidade dos dados dos sujeitos, respeitar a pertinência para a qual foram recolhidos e a sua finalidade. Desta maneira, evitar-se-á que as pessoas não autorizadas acedam a estas referências e as disponibilizem sem autorização. A esta função adita-se, ainda, a clareza e a transparência com que estas entidades se devem governar.

Desde dois mil e quinze que cento e nove países adotaram leis desta matéria no mundo, mais trinta e três do que em dois mil e onze[73]. A "*decisão de adequação*" da União Europeia tem vindo a facilitar este processo ao permitir que um país não pertencente ao continente europeu pertença à "lista branca" de legislações equivalentes de proteção de dados que não violam os princípios regidos pelo Regulamento Geral sobre a Proteção de Dados. Esta decisão autoriza a circulação de dados pessoais transfronteiriços nos termos acordados e facilitará o comércio entre países[74].

[71] A primeira constituição na Europa a legislar a matéria da proteção de dados foi a Constituição Portuguesa de 1976.

[72] Além dos mencionados, o artigo também refere o registo, a estruturação, adaptação, recuperação, divulgação, consulta, difusão e comparação. Cf. Artigo 4.º, n.º 2. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas.

[73] Greenleaf,G. (2015). Global data privacy law 2015: 109 countries, with European laws now a minority. *133 Privacy Laws & Business Internacional Report,* p. 2-5 e Comissão Europeia. (2017). *Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Intercâmbio e proteção de dados pessoais num mundo globalizado.* Bruxelas. p.8.

[74] Cf. Artigo 45.º, n.º 1. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas e Comissão Europeia. (2017). Ob.Cit. p.4-7.

Foram sujeitas e aprovadas as *decisões de adequação* da Suíça[75], Andorra[76], Ilhas Faroé[77], Guernsey[78], Jersey[79], Ilha de Man[80], Argentina[81], Canadá[82], Nova Zelândia[83], Uruguai[84], Israel[85] e Japão[86], estando a decorrer as conversações com a Coreia do Sul[87]. A União Europeia para consentir estas candidaturas tem em conta o contexto geográfico, cultural e político em que o país vive e de que modo é que os dados dos titulares podem estar em segurança. As relações internacionais existentes ou em negociações e o comércio livre serve, igualmente, como fundamento para esta decisão[88].

Anuída a legislação cabe à Comissão Europeia, ao abrigo do artigo 45.º, números 3.º, 4.º e 5.º do RGPD, acompanhar continuadamente o desenvolvimento do país terceiro com exames feitos, pelo menos, de quatro em quatro anos.

Concluindo, estima-se que as leis de proteção de dados no mundo venham a ter uma base uniforme e segundo os mesmos princípios, levando os países a cooperar e a confiar uns nos outros para que a segurança destas informações, quer de cidadãos e de empresas, se mantenha.

---

[75] Cf. Artigo 1.º. Decisão da Comissão 2000/518/CE, de 26 de julho. *Jornal Oficial das Comunidades Europeias.* Comissão das Comunidades Europeias. Bruxelas.
[76] Cf. Artigo 1.º. Decisão da Comissão 2010/625/UE, de 19 de outubro. *Jornal Oficial da União Europeia*. Comissão Europeia. Bruxelas.
[77] Cf. Artigo 1.º. Decisão da Comissão 2010/146/UE, de 5 de março. *Jornal Oficial da União Europeia*. Comissão Europeia. Bruxelas.
[78] Cf. Artigo 1.º. Decisão da Comissão 2003/821/CE, de 21 de novembro. *Jornal Oficial da União Europeia.* Comissão das Comunidades Europeias. Bruxelas.
[79] Cf. Artigo 1.º. Decisão da Comissão 2008/393/CE, de 8 de maio. *Jornal Oficial da União Europeia*. Comissão das Comunidades Europeias. Bruxelas.
[80] Cf. Artigo 1.º. Decisão da Comissão 2004/411/CE, de 28 de abril. *Jornal Oficial da União Europeia.* Comissão das Comunidades Europeias. Bruxelas.
[81] Cf. Artigo 1.º. Decisão da Comissão 2003/490/CE, de 30 de junho. *Jornal Oficial da União Europeia.* Comissão da Comunidade Europeias. Bruxelas.
[82] Cf. Artigo 1.º. Decisão da Comissão 2002/2/CE, de 20 de dezembro. *Jornal Oficial das Comunidades Europeias.* Comissão das Comunidades Europeias. Bruxelas.
[83] Cf. Artigo 1.º. Decisão de Execução da Comissão 2013/65/UE, de 19 de dezembro. *Jornal Oficial da União Europeia*. Comissão Europeia. Bruxelas.
[84] Cf. Artigo 1.º. Decisão de Execução da Comissão 2012/484/UE, de 21 de agosto. *Jornal Oficial da União Europeia*. Comissão Europeia. Bruxelas.
[85] Cf. Artigo 1.º. Decisão da Comissão 2011/61/UE, de 31 de janeiro. *Jornal Oficial da União Europeia.* Comissão Europeia. Bruxelas.
[86] Cf. Artigo 1.º. Decisão de Execução (UE) 2019/419 da Comissão, de 23 de janeiro. *Jornal Oficial da União Europeia.* Comissão Europeia. Bruxelas.
[87] Prevêem-se negociações entre a Índia, Indonésia e Taiwan. Comissão Europeia. (2019). *Comunicação da Comissão ao Parlamento Europeu e ao Conselho: As regras de proteção de dados como instrumento gerador de confiança dentro e fora da UE – ponto de situação*. Bruxelas. p.12-13.
[88] Comissão Europeia. (2017). *Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Intercâmbio e proteção de dados pessoais num mundo globalizado.* Bruxelas. p.9.

1. A proteção de dados na Europa e no Bloco Asiático

O Regulamento Geral sobre a Proteção de Dados foi aplicado nos vinte e oito Estados-Membros[89] a partir de dois mil e dezoito e destina-se ao setor público e privado. O sucesso deste regulamento, à semelhança de todas as leis emanadas pelos órgãos da União Europeia, deve-se ao facto de os países que a compõem partilharem origens e valores idênticos, entre eles, a democracia.

Considerando o continente asiático e a sua divisão geográfica[90], não podemos afirmar o mesmo. As legislações nestes países são dispersas e heterogéneas, consequência dos contextos políticos e dos regimes em que muitos dos países vivem[91]. Os cenários de guerra, o terrorismo e a instabilidade política que assistimos incitam, muitas das vezes, a que os governos tomem medidas que violam a privacidade e a liberdade da população julgando que, as mesmas, vão ter um efeito oposto. Podemos interpretar esta visão como uma falsa utopia ou sentimento falso de proteção.

A nossa investigação permitiu-nos concluir que nem todos os países têm leis que se aplicam a ambos os setores: público e privado. A Malásia, cuja aplicação móvel ter por base a tecnologia de geolocalização e se intitula "*Mysejahtera*", aplicou a Lei de Proteção de Dados da Malásia, em dois mil e treze, ao setor privado. Considera-se que a omissão do setor público constitui um "*défit democrático*"[92]. Esta lei é fortemente influenciada em matéria de consentimento, no entanto podemos ainda salientar, sete princípios que, comparados com o RGPD, são paralelos: a generalidade, notificação e escolha, divulgação, segurança, retenção e integridade de dados e acesso[93].

A Tailândia, país asiático analisado no capítulo anterior, adotou em dois mil e dezanove, a Lei de Proteção de Dados Pessoais BE 2562. Esta lei confronta princípios locais com princípios regulados na União Europeia. Constatamos, de forma símile, que os parâmetros

[89] Incluindo o Reino Unido.
[90] Ásia Central, Ásia Setentrional, Médio Oriente, Ásia Meridional, Ásia Oriental e Sudeste Asiático.
[91] O Afeganistão, por exemplo, vive numa guerra civil desde mil novecentos e setenta e oito e, como tal, a sua lei de proteção de dados é, compreensivelmente, inexistente. Da mesma forma, a Coreia do Norte vive num regime autoritário que não permite que um diploma desta matéria seja produzido.
[92] Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade & Human Rights Perspectives*. Oxford University Press. United Kingdom.p.318.
[93] *Ibid.* p.401-402.

do consentimento são transferidos para a legislação tailandesa, sendo certo que pretendem que o mesmo seja obtido de maneira fácil e não complexa[94].

Uma das legislações mais herméticas que analisamos é a lei da Arábia Saudita[95]. Não existe uma lei de proteção de dados pessoais neste país, porém os juízes utilizam como direito subsidiário, os Princípios de Sharia - a principal coletânea de princípios derivados do Alcorão e Suna. Uma das máximas presentes que retiramos é a proibição da invasão de privacidade e a importância da proteção de cada indivíduo. Assim sendo, em caso de violação destes fundamentos, o juiz tem a liberdade de interpretar e penalizar a pessoa da forma que achar mais apropriada, nomeadamente, atribuindo uma pena de prisão, privando-o de certos direitos, constituindo uma obrigação de compensação monetária e/ou suspendendo-o do seu exercício[96]. Comparando com a União Europeia, esta lei é a que mais se diferencia e deixa dúvidas relativamente aos direitos dos titulares dos dados, como é que deve ser dado e interpretado o consentimento, qual é a entidade responsável pelo processo, de que forma são tratados, entre outras questões.

Em síntese, são evidentes as influências europeias nas legislações nacionais asiáticas, não só através do Regulamento Geral sobre a Proteção de Dados, como também pela presença da Coreia do Sul, de Israel, do Japão e da Turquia na Organização Europeia de Cooperação Económica (OCDE)[97]. Assistimos à evolução no bloco asiático no que diz respeito à regulação e à aplicação das leis de proteção de dados, todavia este caminho não deve ficar por aqui. A atualização constante da tecnologia e a forma como estes dados são

[94] Magrath, M. (2021, 31 de março). Principais Requisitos de Conformidade de Segurança e Regulamentos Bancários de 2020. *OneSpanBlog.* Acedido a 29 de março de 2021, em: https://www.onespan.com/pt-br/blog/top-banking-regulations-security-compliance-requirements.

[95] A *APP* da Arábia Saudita (*Tabaud)* é voluntária e tem por base a tecnologia Bluetooth Low Energy.

[96] DLA Piper. (2021). *Data Protection Laws of the World, Saudi Arabia.*Mohamed Moussallati. Arábia Saudita. p.2-3 e Latham & Watkins LLP. Middle East & Africa Technology, IP and Sourcing Focus. *Data Protection in the Kingdom of Saudi Arabia: A Primer*. Noor Al-Fawzan e Omar Elsayed. Arábia Saudita. p.2-3.

[97] A Organização Europeia de Cooperação Económica foi fundada em 1948 com o principal objetivo da cooperação económica. Atualmente tem como membros: a Alemanha, Austrália, Áustria, Bélgica, Canadá, Chile, Coreia do Sul, Dinamarca, Eslováquia, Eslovénia, Espanha, Estados Unidos da América, Estónia, Finlândia, França, Grécia, Hungria, Irlanda, Islândia, Israel, Itália, Japão, Letónia, Lituânia, Luxemburgo, México, Noruega, Nova Zelândia, Países Baixos, Polónia, Portugal, Reino Unido, República Checa, Suécia, Suíça e Turquia. Direção-Geral das Atividades Económicas. *Organização para a Cooperação e Desenvolvimento Económico*. Acedido em 15 de março de 2021, em: https://www.dgae.gov.pt/servicos/comercio-internacional-e-relacoes-internacionais/multilaterais/organizacao-para-a-cooperacao-e-desenvolvimento-economico-ocde-.aspx.

geridos, requer uma atenção e um acompanhamento contínuo dos governos e dos responsáveis.

1.1. Os dados protegidos sensíveis

Os dados recolhidos nas aplicações móveis em estudo não diferenciam de aplicação para aplicação. Por norma, ao utilizador é pedido o género, a idade[98], países visitados nos últimos catorze ou trinta dias, profissão e informações relativas à saúde, em caso de contacto suspeito com outro utilizador. Estes elementos compõem o conceito de dados pessoais de saúde que, por sua vez, são integrados pelos dados sensíveis subscritos pelo RGPD e, cada vez mais, por legislações asiáticas. O fator diferenciável no tratamento é se a *APP* utiliza *Bluetooth Low Energy* ou Geolocalização.

Os dados pessoais de saúde são todas as informações que direta ou indiretamente estão ligadas a este serviço. Para este ponto será importante observar, em concreto, as categorias de dados especiais que, além da saúde, abrange também a orientação sexual, a religião, a origem racial ou étnica, política e filiação sindical. Definem-se como "*especiais*" ou "*sensíveis*" devido à sua vulnerabilidade que, por si só, exige uma proteção planeada de forma a não proporcionar discriminação entre a população[99]. Além do mais, são suscetíveis de correr riscos do ponto de vista dos direitos fundamentais e, como tal, o seu tratamento é proibido salvo nas exceções reguladas no número 2.º, do artigo 9.º do RGPD, onde salientamos as circunstâncias de consentimento explícito do titular, a proteção dos interesses vitais do mesmo e o interesse público[100].

A Convenção 108 do Conselho da Europa, sobre a "Proteção das Pessoas relativamente ao Tratamento Autorizado de Dados de Caráter Pessoal", entrou em vigor a um de outubro de mil novecentos e oitenta e cinco. Este foi o primeiro diploma vinculativo em matéria de proteção de dados e proíbe, outrossim, o processamento de dados sensíveis e dados relativos

[98] Na Eslovénia, *APP #Ostanizdrav* destina-se a pessoas residentes com idade igual ou superior a 16 anos. Por outro lado, é necessário ter 18 anos para se instalar a *APP do Brunei* (*BruHealth*). #OstanizdravApp. (2020). *Privacy Notice*. Eslovénia. p.2 e BruHealth. (2020). *Terms of Use*. Acedido em 17 de março de 2021, em: https://www.healthapp.gov.bn/covid19/bruhealth/term_of_use.html.

[99] Segado, F. (1997). El régimen jurídico del tratamiento autorizado de los datos de carácter personal en España. Derecho PUPC, (51). p.15 e Bioni, B.R. (2019). *Proteção de dados pessoais: a função e os limites do consentimento.* Editora Forense. Rio de Janeiro. p.85.

[100] Cf. Artigo 9.º, n.º 1 e 2. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas.

a condenações criminais, no artigo 6.º. Pretendia-se salvaguardar os direitos e as liberdades fundamentais e garantir um tratamento seguro, leal e lícito de dados no setor público e privado, contra eventuais abusos de poder[101].

No continente asiático, alguns países subscrevem este entendimento conforme a sua realidade. Na Coreia do Sul a *APP 자가격리자안전보호 (Self-Quarantine Safety Protection*) tem por base o Código de Proteção de Informações Pessoais (PIPA) que vigora desse dois mil e onze. Os dados sensíveis designam-se de "*dados confidenciais*" e incluem: a ideologia, a religião, a filiação em sindicatos e partidos políticos, as convicções políticas, a saúde, a orientação sexual, informações ADN e, em certos casos, antecedentes criminais[102]. Por outro lado, relembrando as Filipinas, a Lei de Privacidade de Dados entrou em vigor em dois mil e doze. Integram as "*informações pessoais confidenciais*", reguladas no Capítulo I, Secção 3, (l): a origem racial e étnica, estado civil, idade, cor, religião, ideologias filosóficas e políticas, saúde, educação, vida genética e sexual, antecedentes criminais, documentos pessoais como o bilhete de identidade, declarações fiscais ou licenças e, ainda, certificados com conteúdo sigiloso[103].

Tendo tudo isto em conta, no capítulo anterior concluímos que o uso da tecnologia de geolocalização contribuiria para a invasão na vida privada do ser humano e não alcançaria os objetivos pretendidos, tal como, perceber quando foram sentidos os primeiros sintomas. Os responsáveis pelo tratamento de dados, nestes casos, terão uma tarefa mais complexa: tratar os dados pessoais de saúde e os dados de localização do usuário. Por outro lado, as entidades das *APP*s que utilizam a tecnologia *Bluetooth Low Energy* vão concentrar-se no tratamento de dados de saúde.

Assim sendo, embora ambos os tratamentos requeiram um sigilo profissional, as aplicações móveis que utilizam a tecnologia de geolocalização têm um menor alcance pelo seu procedimento composto. A influência será maior com a tecnologia *Bluetooth Low Energy,* atendendo ao objetivo pelo qual estas *APP*s foram criadas.

---

[101] Agência Europeia dos Direitos Fundamentais, Conselho da Europa, Tribunal Europeu dos Direitos do Homem. (2014). *Manual da legislação europeia sobre proteção de dados*. Serviço das Publicações da União Europeia. Luxemburgo. p. 16 e Pinheiro, A.S. (2015). *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional.* AAFDL – Associação Académica da Faculdade de Direito de Lisboa. Lisboa. p.538-539.

[102] Greenleaf, G. (2014). *Asian Data Privacy Laws:Trade & Human Rights Perspetives*. Oxford University Press. United Kingdom. p.145.

[103] National Privacy Commission. (2012). *Republic Act 10173 – Data Privacy Act of 2012.* Acedido em 30 de março de 2021, em: https://www.privacy.gov.ph/data-privacy-act/#3.

1.2. As entidades responsáveis - públicas e privadas

As entidades responsáveis podem ser pessoas singulares ou coletivas, serviços ou organismos e autoridades públicas, conforme estejamos a falar de entes públicos ou privados. A estas cabem determinar as finalidades e os métodos de tratamento de dados pessoais de forma transparente e clara para que o titular tenha conhecimento do procedimento[104].

Na maioria dos nossos casos, as entidades selecionadas são autoridades públicas ou entidades administrativas independentes criadas por lei. A ausência de um vínculo de submissão permite que estas operem segundo as suas próprias premissas[105]. Em Portugal, a Comissão Nacional de Proteção de Dados foi criada por lei ao abrigo do artigo 267.º, número 3.º da CRP e é a principal responsável pelo processo competindo-lhe as "*atribuições*" e "*poderes*" dos artigos 57.º e 58.º do RGPD.

Observando os restantes países europeus, podemos destacar outras comissões com o mesmo âmbito: *Österreichische Datenschutzbehörde* (Áustria), *Autorité de la protection des données - Gegevensbeschermingsautoriteit* (Bélgica), *Commission for Personal Data Protection* (Bulgária), *Datatilsynet* (Dinamarca), entre outros[106]. Similarmente, a própria União Europeia (UE) tem um órgão que serve o mesmo efeito - a Autoridade Europeia para a Proteção de Dados (AEDP), que garante a proteção dos dados da UE e auxilia-os na mesma matéria[107].

Ainda que possam atuar de forma independente, nos casos em que uma lei ou regulamento determine que uma autoridade pública fique encarregue deste processamento, estas devem dar importância ao impacto sobre a proteção de dados no disposto do artigo 35.º do RGPD[108]. Por outras palavras, compete à autoridade pública em caso de novas

---

[104] Castro, C.S. "Art8.º - Proteção de dados pessoais" em Silveira, A. e Canotilho, M. (2013). *Carta dos Direitos Fundamentais da União Europeia: comentada*. Almedina. Coimbra. p.123.

[105] Diário da República Eletrónico. *Lexionário – Entidades Administrativas Independentes.* Acedido em 30 de março de 2021, em: https://dre.pt/web/guest/lexionario/-/dj/117357313/view.

[106] European Data Protection Board. *Our Members*. Acedido em 31 de março de 2021, em https://edpb.europa.eu/about-edpb/board/members_en.

[107] European Data Protection Supervisor. *About*. Acedido em 31 de março de 2021, em https://edps.europa.eu/about-edps_en.

[108] European Commission. (2020). *Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection.* Communication from the commission. Bruxelas. p.12 e Castro, C.S. (2005). *Direito da informática, privacidade e dados pessoais: a propósito da legalização de tratamentos de dados pessoais*

tecnologias, proceder a uma avaliação do embate da sua utilização nos direitos fundamentais das pessoas. Este exame, feito *ex ante*, pode ou não ser obrigatório conforme as circunstâncias do número 3.º, sendo que no nosso caso é indispensável uma vez que há um tratamento "*em grande escala de categorias especiais de dados*" [109].

Na Europa, os Estados-Membros são incentivados a criar códigos de conduta, principalmente no seio das empresas cuja fluência de dados é maior. Estas orientações constituem medidas preventivas de segurança para os funcionários de maneira a que não haja transgressões no seu desempenho[110].

1.3. O consentimento implícito e explícito

A autorização dada pelo titular para o tratamento de dados pessoais designa-se de consentimento[111]. O titular que assente o tratamento deverá fazê-lo de forma livre, específica e inequívoca como reconhecimento da sua vontade. O consentimento é livre quando é dado sem nenhuma influência de terceiro e específico quando diga respeito a um período de tempo e a uma finalidade definida previamente[112].

Distinguem-se duas modalidades de consentimento: explícito e implícito. Para o nosso estudo importa analisar e verificar, a partir de alguns exemplos, o consentimento dado de forma explícita, sendo certo que em ambos os casos não podem existir dúvidas do desejo do titular e que o mesmo pode ser revogado a todo o tempo[113]. Quando a declaração é deduzida a partir das circunstâncias, diz-se que o consentimento foi dado implicitamente, por outro lado quando há uma manifestação verbal ou por escrito, deduz-se que há um consentimento

---

(incluindo vigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso. Almedina. Coimbra. p.340.

[109] Cf. Artigo 35.º, n.º 3, alínea b). Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas e Pinheiro, A.S., Coelho, C., Duarte, T., Gonçalves, C. e Gonçalves, C. (2018). *Comentário ao Regulamento Geral de Proteção de Dados.* Almedina. Coimbra. p.457-462.

[110] Agência Europeia dos Direitos Fundamentais, Conselho da Europa, Tribunal Europeu dos Direitos do Homem. (2014). *Manual da legislação europeia sobre proteção de dados*. Serviço das Publicações da União Europeia. Luxemburgo. p. 98 e 107.

[111] Cf. Artigo 6.º, n.º 1, alínea a). Regulamento (UE) 2016/679, de 27 de abril. Ob.Cit.

[112] Castro, C.S. "Art8.º - Proteção de dados pessoais" em Silveira, A. e Canotilho, M. (2013). *Carta dos Direitos Fundamentais da União Europeia: comentada*. Almedina. Coimbra. p.127 e Castro, C.S. (2005). *Direito da informática, privacidade e dados pessoais: a propósito da legalização de tratamentos de dados pessoais (incluindo vigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso.* Almedina. Coimbra. p.207.

[113] Cf. Artigo 7.º, n.º 3. Regulamento (UE) 2016/679, de 27 de abril. Ob.Cit.

explícito da vontade do titular[114]. No tratamento de dados sensíveis, o consentimento tem de ser expresso.

Nas *APP*s, o consentimento é pedido via eletrónica. Os países desenvolveram estas aplicações com um design e grafismo idêntico e disponibilizaram o idioma inglês, como língua comum. Note-se que esta configuração é relevante pois quando um cidadão viaja para outro país e instala a *APP* de origem, tem de consentir e informar-se de forma clara dos termos e condições.

Em resumo, esta permissão demonstra que o processo de tratamento de dados é voluntário e, no continente europeu, realizado de acordo com o RGPD. Nas aplicações obrigatórias essa contenda não se aplica porque não existe consentimento do titular. Por fim se os requisitos da autorização se alterarem, deve ser prestado um novo consentimento[115].

1.4. A limitação da conservação dos dados e o direito ao esquecimento: a finalidade temporária das *APP*s

O crescimento da tecnologia e a disponibilização de informação pessoal na internet e em dispositivos móveis fez crescer a noção de "*memória digital*", isto é, a conservação dos dados temporária ou permanentemente na rede, sem sabermos se foram ou não apagados pelo responsável.

Nas aplicações móveis criadas em contexto pandémico, o mesmo poderia acontecer, porém o titular tem o direito de ver os seus dados pessoais apagados ou esquecidos assim que a finalidade estiver cumprida[116]. A entidade, recebido o pedido, tem um mês para os extinguir e notificar do apagamento[117]. Na eventualidade de indeferir, a mesma deverá fundamentar a sua decisão ao abrigo do artigo 12.º, números 3.º e 4.º do RGPD.

Entende-se que a conservação é um passo natural no tratamento de dados pessoais e é possível o titular preservá-los no sistema. Nesses casos, os dados pseudonimizados ficam

[114] Agência Europeia dos Direitos Fundamentais, Conselho da Europa, Tribunal Europeu dos Direitos do Homem. (2014). Ob.Cit. p. 60.
[115] Castro, C.S. (2005). Ob.Cit. p.207.
[116] Cf. Artigo 17.º. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas.
[117] Cf. Artigo 19.º. *Ibid.*

anónimos, ou seja, já não contêm nenhum elemento que permita identificar a pessoa singular[118].

No mundo, o fim da pandemia levará a que as estas *APP*s fiquem obsoletas, dado que se destinam especificamente a auxiliar no combate à pandemia Covid-19. No entanto, nada nos garante que estas informações não se percam ou não sejam utilizadas para outros fins. O crescimento das redes sociais e de plataformas que permitem a troca de informações pessoais, principalmente no seio das grandes empresas, surge como perigo no nosso quotidiano. Nas palavras de Filipa Calvão, estas sociedades "*(...) são detentoras de um conhecimento muito extenso sobre as pessoas e, por vezes, têm uma percepção mais exata da vida do que elas têm*"[119].

1.5. O tratamento automatizado e não automatizado

A criação das *APP*s em estudo implica que façamos uma distinção entre o tratamento de dados pessoais automatizados e não automatizados.

Entende-se que há tratamento automático quando este é feito através de um meio tecnológico. Para este efeito é criado um algoritmo[120] que serve a finalidade pré-estabelecida e que irá definir um perfil[121] e fazer previsões sobre o utilizador[122]. Pelo contrário, o tratamento de dados não automatizados engloba um procedimento da responsabilidade de um indivíduo, sem auxílio de um instrumento tecnológico.

Existem cada vez mais setores que tomam as suas decisões através de um procedimento automatizado, tais como: bancário, financeiro, de saúde, marketing, entre outros. O artigo

[118] Agência Europeia dos Direitos Fundamentais, Conselho da Europa, Tribunal Europeu dos Direitos do Homem. (2014). *Manual da legislação europeia sobre proteção de dados*. Serviço das Publicações da União Europeia. Luxemburgo. p. 37 e 45-46.
[119] Calvão, F. U. (2018). *Direito da proteção de dados pessoais: relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina.* Universidade Católica Editora. Porto. p.16.
[120] O conceito de algoritmo foi oficializado em 1936 por Alan Turing e Alonzo Church como o "*conjunto não ambíguo e ordenado de passos executáveis que definem um processo finito".* Por outras palavras, trata-se de um conjunto de regras precisas e eficazes que aplicadas à base de dados levam a uma solução. Filho, G. e Alexandre, E. (2014). *Introdução à Computação*. 2ª edição. Editora da UFPB. Brasil.
[121] Cf. Artigo 4.º, n.º 4. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas.
[122] Comissão Europeia. *Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?* Acedido em 3 de março de 2021, em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt.

22.º do RGPD[123] cuja epígrafe é "Decisões individuais automatizadas, incluindo definição de perfis", remeto-nos ao facto do titular não ficar sujeito a estas resoluções de forma exclusiva, no caso de afetarem os seus direitos fundamentais (n.º 1). Deste modo, devem ser estabelecidos meios alternativos de tratamento, como por exemplo, a intervenção humana.

O controlo não automatizado, como meio alternativo, garante que a decisão possa ser alterada por um responsável com a devida habilitação. Num procedimento em que estes dois métodos se encontram, os moldes em que a decisão foi tomada deve ser registada[124].

A regra do número 1.º contém exceções enumeradas no número 2.º: a celebração de um contrato (alínea a)), autorização do direito da União Europeia ou do Estados-Membros (alínea b)) e o consentimento explícito (alínea c)). Relativamente a este último, a manifestação e a declaração de vontade do usuário[125] servirá para o informar e salvaguardar dos riscos que este sistema comporta. O detentor deve manter-se informado e controlar, durante todo o processo, os seus dados e conhecer os seus direitos. Assim sendo, a linguagem utilizada tem de ser clara, simples e transparente, de maneira a que não surjam dúvidas relativamente ao funcionamento e ao modo como são tomadas as decisões[126].

Esta atividade pode gerar perigos para os utilizadores e para os seus direitos fundamentais. Em causa estão perfis íntimos analisados que podem levar a uma análise abusiva[127]. Ao mesmo tempo, o próprio algoritmo pode apresentar falhas e gerar soluções erróneas[128], levando as pessoas a optar por diferentes opções ou comportamentos no seu quotidiano ou, em muitos dos casos, originando discriminação (no emprego, investimentos, créditos, seguros)[129].

---

[123] Este artigo correspondia ao artigo 15.º da Diretiva 95/46/CE. Diretiva 95/46/CE, de 24 de outubro. *Jornal Oficial das Comunidades Europeias.* Parlamento Europeu e Conselho da União Europeia. Luxemburgo e Pinheiro, A.S., Coelho, C., Duarte, T., Gonçalves, C. e Gonçalves, C. (2018). *Comentário ao Regulamento Geral de Proteção de Dados.* Almedina. Coimbra. p.387.

[124] Data Protection Working Party. (2018). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Bruxelas. p.21.

[125] Cf. Artigo 4.º, n.º 11. Regulamento (UE) 2016/679, de 27 de abril. *Regulamento Geral sobre a Proteção de Dados*. Parlamento Europeu e do Conselho da União Europeia. Bruxelas e Pinheiro, A.S., Coelho, C., Duarte, T., Gonçalves, C. e Gonçalves, C. (2018). Ob. Cit. p.134.

[126] Cf. Artigo 12.º, n.º1. *Ibid.* e Data Protection Working Party. (2018). Ob.Cit. p.16-25.

[127] Doneda, D. (2011). A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL].* 12(2), 91-108.

[128] Comissão Europeia. *Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?* Acedido em 3 de março de 2021, em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt.

[129] Data Protection Working Party. (2018). Ob.Cit. p.5-6 e 10.

Nas aplicações móveis criadas em contexto pandémico, o tratamento de dados pode conjugar as duas formas. O artigo 22.º, número 4.º declara que os algoritmos não se aplicam às categorias especiais de dados, incluindo a saúde, exceto quando o titular consentir expressamente ou o tratamento for necessário para o interesse público[130]. Em Portugal, através do código de legitimação, o cidadão entra em contacto com o profissional de saúde que lhe fará um combinado de perguntas e respostas por forma a obter um diagnóstico, como: sintomas, a duração e o local (espaço fechado ou aberto) do contacto, os contactos posteriores, as condições de saúde, o agregado familiar, se durante o contacto estava ou não a utilizar máscara, entre outras.

Neste âmbito podemos questionar se é mais vantajoso optar por um tratamento automatizado ou não automatizado atendendo aos riscos e à invasão na vida privada do cidadão. Será apropriado manter apenas um formato quando as faixas etárias mais velhas não têm acesso facilitado à tecnologia? Na intervenção humana será prudente concluir que a abordagem dos especialistas, nas principais linhas de saúde, pode criar dualidade de critérios?

Conclui-se que a conjugação dos dois sistemas aumenta a precisão do tratamento dos dados pessoais. Se o algoritmo falhar, os peritos podem assegurar o processo não perdendo toda a recolha realizada. Ambos contribuem, ainda, para que os perfis sejam completos com as informações pretendidas para as finalidades. No nosso caso, os médicos que questionam os pacientes, via telefónica, têm como objetivo final perceber que cuidados são necessários. Em contrapartida, a inexistência de um guião com critérios pré-estabelecidos, pode criar a sua dualidade, isto é, diferentes maneiras dos técnicos lidarem com a circunstância. Constatamos que em Portugal as questões e as instruções variaram de pessoa para pessoa, fruto destes requisitos não fixados.

Relativamente às faixas etárias mais velhas, o parecer mantém-se. No primeiro capítulo vimos que as aplicações móveis da Europa não abrangem esta população. Já em Singapura seria possível adotar um tratamento automático uma vez que estes pensaram num dispositivo adaptado para este intervalo de idades.

Em suma, parece-nos que o tratamento híbrido é a melhor opção para estas aplicações móveis. Os governos do mundo devem garantir que a recolha e o tratamento de dados são feitos conforme as legislações, assegurando que os cidadãos conhecem os riscos associados

[130] Cf. Artigo 9.º, n.º1 e 2.º, alínea a) ou g). *Ibid* e Comissão Europeia. Ob. cit.

desta atividade e quais são os seus direitos. Numa declaração assinada pela sociedade civil, em dois mil e vinte, afirma-se que "*não podemos permitir que a pandemia sirva como desculpa para destruir o direito do indivíduo à privacidade"*[131].

[131] *Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human right.* (2020).

III. A *APP* STAYAWAY COVID e o direito fundamental à privacidade

Nos dois capítulos iniciais debruçamo-nos sobre o funcionamento das aplicações móveis criadas em contexto da pandemia Covid-19 e os seus principais critérios diferenciadores no continente europeu e asiático.

De seguida, num enquadramento mais técnico, compreendemos de que forma é que os utilizadores são informados da gestão das suas informações, nomeadamente, do momento em que as mesmas são esquecidas, que tipo de dados são tratados e quem são as entidades responsáveis pelo tratamento nestas *APP*s.

Em ambos os capítulos, fomos confrontados com as limitações destes instrumentos. Relembrando o que concluímos anteriormente, estas não são ferramentas únicas. Por outras palavras, não são vistas como soluções ímpares no combate à pandemia por limitarem, ao mesmo tempo, as liberdades dos utilizadores.

Uma boa comunicação entre os governos do mundo e a população revela-se crucial para o uso destas aplicações. Os cidadãos que têm a obrigação de instalar a *APP* questionam-se se obrigatoriedade faz parte de um aproveitamento político ou se a restrição é ou não devida. A pandemia coloca à prova os nossos direitos fundamentais mas também muitos bens jurídicos, tais como: a saúde pública, a vida, o estado da economia, entre outros. Assim, é importante perceber se a conjuntura em que vivemos é ou não justificação para violar o seu núcleo.

Neste último capítulo, será importante analisar o conceito de privacidade enquanto direito fundamental em Portugal confrontando, inclusive, com a *privacy* americana (modelo manifestamente mais amplo). De igual forma, iremos traçar um caminho dos direitos fundamentais, concretamente do direito à liberdade e à vida privada na Europa e nos Países Asiáticos desde a sua origem à atualidade como a conhecemos. Este parecer servirá para perceber de que forma é que os dois continentes se influenciaram ao longo da história.

Por fim, com base na jurisprudência a propósito dos metadados, observaremos as medidas adotadas em Portugal no âmbito da proteção da privacidade.

Em conclusão, apraz-nos verificar o sucesso ou o insucesso destas *APP*s no combate à pandemia nos continentes europeu e asiático e as consequências e desafios testemunhados pelos governos e as populações do mundo.

1. A privacidade como um direito fundamental

A privacidade, direito fundamental regulado no ordenamento jurídico português e âmago da nossa dissertação, não tem um conceito claro na doutrina. A elasticidade e a consequente sensibilidade do tema são abordadas por vários autores que, de forma regular, apontam novas problemáticas. Esta "*bola de neve*" a que nos propomos analisar tem vindo a desenvolver-se, assim como a preocupação das populações mundiais em ver as suas informações pessoais protegidas de qualquer interferência pública ou privada.

Julga-se que este conceito foi, pela primeira vez reconhecido, em mil oitocentos e noventa por Samuel Warren e Louis Brandeis na *Revista Harvard Law Review*. O artigo "*Right to Privacy*" [132], fundado na *Common Law*, foi considerado como um dos mais influentes na história dos Estados Unidos da América e identifica o "*direito a ser deixado a sós*" [133], ou seja, o direito a não ser perturbado.

Ao longo do texto, os dois autores distinguem uma América rural que desconhece este direito como tal, de uma América urbana que devido às novas formas de interagir e às invenções tecnológicas, como é o caso da fotografia, evidencia a inevitabilidade de o fazer[134].

A *privacy*, enquanto direito autónomo, não proibia que fossem publicadas informações de conteúdo público e de interesse geral, defendia sim que todas as informações da esfera íntima do visado, incluindo sentimentos, emoções, dados pessoais e outras informações, fossem protegidas garantindo a devida liberdade e controlo[135]. Surge, tal como Jorge

---

[132] Warren, S. e Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*. v. IV, No. 5. Acedido a 30 de maio de 2021, em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[133] Antes do artigo, em mil oitocentos e trinta e quatro, o direito "*a ser deixado a sós*" já tinha sido mencionado pela Suprema Corte no caso Wheaton v. Peters. Igualmente, em mil oitocentos e oitenta, o juiz Thomas Cooley publicou a obra "*A Treatise on the Law Torts*" onde utilizava, pela primeira vez, a expressão "*right to be let alone"*. Assis Zanini, L. (2015). O Surgimento e o Desenvolvimento do *Right of Privacy* nos Estados Unidos. *RJLB*. Ano 1, n.º4. p. 793-796.

[134] Cit. «*Recent inventions and business methods call atention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good prediction that "what is whispered in the closet shall be proclaimed from the house-tops." (...)*».Warren, S. e Brandeis, L. (1890). Ob. Cit. e Santos Macedo, F., Dias Bublitz, M. e Linden Ruaro, R. (2013). A *Privacy* Norte-Americana e a Relação com o Direito Brasileiro. *Revista Jurídica Cesumar-Mestrado*. v. 13, n.1. p.164-165.

[135] Facchini Neto, E. (2020). A Noção de Privacy na Jurisprudência da Suprema Corte Norte-Americana: Existe um conceito unificador? *Revista de Direito Brasileira*. v. 25, n.10. p.419.

Miranda e Rui Medeiros descrevem, como "*a expressão paradigmática*" dos direitos pessoais, o direito à reserva da intimidade da vida privada e o direito de oposição à investigação sobre a vida privada[136].

Desde logo, surgiram casos polémicos e de diferentes matérias na Suprema Corte Americana que receberam acolhimento na jurisprudência e em leis. Servem de exemplo, *Meyer v. Nebraska* (1923)[137], *Griswold v. Connecticut* (1965)[138], *Bowers v. Hardwick (*1986)[139], entre outros.

Em mil novecentos e setenta e quatro, publicou-se o *Privacy Act* – diploma que regula o papel das agências governamentais em matéria de dados pessoais. Assim no exercício das suas funções, salvo as exceções impostas, estas agências deveriam aplicar uma política transparente no que diz respeito aos registos dos indivíduos, incluindo na sua recolha, manutenção, uso e disseminação[140].

Este código, originário dos projetos do Senado e do Congresso, padeceu de algumas variações desde o atentado de onze de setembro de dois mil e onze. Se outrora a privacidade americana se caracterizava pela sua polimorfia, desde então este conceito reduziu-se pelo zelo praticado. No entanto, note-se que este código, assim como estes acórdãos, constituíram importantes metas para colocar a *privacy* no centro da discussão da sociedade americana.

Em Portugal, os direitos fundamentais, nomeadamente a privacidade, estão concatenados com os direitos de personalidade, não obstante estes corresponderem a uma posição privada em relação aos primeiros. Para o autor Paulo Mota Pinto esta ligação é estabelecida porque os direitos *"incidem sobre a personalidade humana globalmente considerada ou em algumas das suas particulares refrações ou aspetos (...)*"[141] e, por isso, os seres humanos,

[136] Miranda, J. e Medeiros, R. (2017). *Constituição Portuguesa Anotada*. 2ª edição revista, v.1, Universidade Católica Editora. Lisboa. p.452.
[137] No acórdão *Meyer* v. Nebraska é reconhecida a liberdade aos pais de decidirem a educação que melhor se adequa aos seus filhos.
[138] Pela primeira vez, no acórdão *Griswold v. Connecticut*, é apreciada a questão do aborto. Esta decisão revelou-se fundamental para a evolução do conceito de *privacy* e é o principal diploma de estudo pelos autores.
[139] O acórdão *Bowers v. Hardwick* teve como tema a orientação sexual. Atualmente nos Estados Unidos América, embora se tenha debatido desde cedo a homossexualidade, existem estados que não punem de forma alguma qualquer tipo de discriminação feita contra estas pessoas.
[140] Santos Macedo, F., Dias Bublitz, M. e Linden Ruaro, R. (2013). Ob. Cit. p.170-172.
[141] Os direitos de personalidade são direitos gerais, intransmissíveis e irrenunciáveis que, de acordo como artigo 70.º do Código Civil, visam proteger os indivíduos contra qualquer ofensa ilícita ou ameaça à sua personalidade física ou moral. Acrescenta-se ainda, no artigo 81.º do Código Civil, que o seu exercício não pode sofrer qualquer limitação voluntária. Mota Pinto, P. (2018). *Direitos de Personalidade e Direitos Fundamentais.* 1ª edição, Gestlegal. Coimbra. p.325.

enquanto pessoas autónomas e livres devem gozar destes direitos que tutelam os interesses da sua própria personalidade para estabelecerem relações interpessoais de confiança e praticarem as suas atividades diárias sem estarem limitados[142].

Observando o constitucionalismo português e a sua história, comprova-se que o regime político de António de Oliveira Salazar sacralizado pela constituição de mil novecentos e trinta e três conhece o seu epílogo no Marcelismo. As supressões de liberdades e garantias, a decadência económica e social do país, as pressões políticas internas e externas pelo findar da Guerra Colonial, marcam a eclosão, a vinte cinco de abril de mil novecentos e setenta e quatro, da "Revolução dos Cravos" levada a cabo pelo Movimento das Forças Armadas (MFA) e por uma parte significativa da sociedade civil. O processo de transição democrática subsequente a setenta e quatro, pautado por permanentes conflitos políticos, resulta na entrega do poder à Junta de Salvação e a instauração dos governos provisórios (PREC) que se seguiram até mil novecentos e setenta e seis.

Com o fim do processo revolucionário, a criação de uma nova constituição de índole democrática universalista e, tendencialmente socialista, torna-se uma prioridade para a formação da 3ª República Portuguesa, constituindo-se, para esse efeito, uma Assembleia Constituinte com poderes para elaborar e aprovar aquela que viria a ser a, ainda vigente, constituição de mil novecentos e setenta e seis[143].

Em matéria de privacidade e proteção de dados, o diploma original previa o direito à identidade, ao bom nome e à intimidade (artigo 33.º), a inviolabilidade do domicílio e da correspondência (artigo 34.º) e a utilização informática (artigo 35.º). Atualmente, após sete revisões constitucionais[144], destacam-se os artigos 26.º e 34.º que passaremos a estudar.

Considerando o artigo 26.º da CRP comprovamos, prontamente, que estamos perante um conjunto de nove direitos que se inserem na categoria do direito geral de personalidade[145]:

---

[142] Cit. «*(…) a privacidade tem uma grande importância a vários níveis, não só como valor em si, mas como instrumento para a realização de outros bens (…) para o desenvolvimento da sua individualidade e de relações humanas de confiança pessoal, amor, amizade, etc. – torna possível o relaxamento e a criação de "válvulas se segurança" para a agressão, permite criar o espaço necessário para a auto-avaliação do individuo, promove a sua liberdade de ação e autonomia, permite criar comunicações limitadas e protegidas, bem como uma seletividade controlada na auto-apresentação da pessoa face aos outros, etc.*». *Ibid*.

[143] No essencial, este texto teve como principais influências a Lei Fundamental de Bona de mil novecentos e quarenta e nove, o texto constitucional italiano de mil novecentos e cinquenta e oito, o modelo francês e ainda constituições socialistas de países ex-comunistas. Gomes Canotilho, J.J. (2003). *Direito Constitucional e Teoria da Constituição*. 7ª edição, Almedina, Coimbra. p.199.

[144] Ao todo, a CRP foi submetida a sete revisões constitucionais (1982,1989,1992,1997,2001,2004 e 2005).

[145] Cf. Artigo 70.º do Código Civil.

direito à identidade pessoal, direito ao desenvolvimento da personalidade, direito à capacidade civil, direito à cidadania, direito ao bom nome e reputação, direito à imagem, direito à palavra, direito à reserva da intimidade da vida privada e familiar e o direito à proteção legal contra quaisquer formas de discriminação (número 1.º) [146].

O direito à reserva da intimidade da vida privada e familiar é o mais relevante para a nossa análise e podemos salientar, desde logo, o seu grande alcance prático. A ideia de que as pessoas têm a liberdade de definir os limites de acesso, divulgação e utilização dos seus dados pessoais e familiares por terceiros[147], evidencia a autodeterminação informacional do ser humano. Atentando no artigo 80.º do Código Civil, esta ideia é reforçada – "*Todos devem guardar reserva quanto à intimidade da vida privada de outrem*" [148]. Veja-se, contudo, que quando nos referimos à esfera íntima da pessoa estamos a aludir ao núcleo da intimidade que, por sua vez, é diferente da dimensão da esfera privada e social[149].

O princípio geral do respeito pela dignidade e personalidade humana, emanado neste artigo, chama-nos também à atenção para "*o outro lado da moeda*". Todas as informações que são transmitidas sem o consentimento da pessoa constituem um comportamento abusivo e contrário à dignidade humana. Gomes Canotilho e Vital Moreira referem mesmo que "*certas informações relativas às pessoas e famílias podem despersonalizar, desagradar, desindividualizar os seres humanos*"[150].

O artigo 34.º da CRP, por sua vez, mantém o texto original da constituição de mil novecentos e setenta e seis. De acordo com o número 1.º, o direito ao domicílio e ao sigilo da correspondência e dos outros meios de comunicação privada são invioláveis, com objetivo de proteger bens jurídicos comuns[151].

Para o nosso estudo, interessa observar o número 4.º: "*é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação (...)*[152]".

---

[146] Gomes Canotilho, J.J e Moreira, V. (2007). *Constituição da República Portuguesa Anotada*. 4ª edição revista, v.1, Coimbra Editores. Coimbra. p. 461.
[147] Gomes Canotilho, J.J e Moreira, V. (2007). Ob.Cit. p. 467 e Miranda, J. e Medeiros, R. (2017). *Constituição Portuguesa Anotada*. 2ª edição revista, v.1, Universidade Católica Editora. Lisboa. p.452.
[148] Cf. Artigo 80.º do Código Civil.
[149] Miranda, J. e Medeiros, R. (2017). Ob.Cit. p. 452.
[150] Gomes Canotilho, J.J e Moreira, V. (2007). Ob.Cit. p. 472.
[151] Cf. Artigo 34.º, número 1.º da CRP.
[152] Cf. Artigo 34.º, número 4.º da CRP.

As relações entre os destinatários não devem ser alvo de intromissões, salvo nos casos previstos na lei[153]. Ainda assim, nem todas as comunicações são aqui acolhidas. O critério da mínima inviolabilidade, regulado pela constituição, garante que as comunicações não devem ser de acesso facilitado a terceiros. Jorge Miranda e Rui Medeiros exemplificam este raciocínio com a correspondência aberta. Depreende-se que no envio de cartas para outros, a mesma vá devidamente fechada certificando-se a mínima inviolabilidade. Contrariamente, as redes sociais não podem ser admitidas dada a sua infinidade de ligações facilmente acedidas pelos usuários[154].

Em suma, num mundo onde a exposição e o uso das tecnologias tem aumentado, há uma dúvida geral sobre o futuro da privacidade. Embora estejamos perante um direito que em Portugal é universal e se mantém desde o preceito original, no nosso entender, esperam-se novos desafios que transformarão este conceito, adequando-o ao desenvolvimento humano.

Importa, também, frisar que a *privacy* americana abrange mais situações práticas do que a privacidade em Portugal, mantendo-se alguma subjetividade na definição de casos que a nossa lei acolhe.

Para terminar, em matéria de proteção de dados, os Estados Unidos da América (EUA) e a Europa celebraram, em fevereiro de dois mil e dezasseis, um acordo designado "*Privacy Shield"* ou "Escudo de Proteção da Privacidade da UE para empresas participantes nos EUA", com base no processo de adequação analisado no capítulo anterior.

Este acordo, assinado entre a Comissão Europeia e o Departamento de Comércio dos EUA, tinha como objetivo assegurar uma interoperabilidade de dados com fins comerciais protegendo os direitos fundamentais e garantindo a devida segurança das empresas europeias[155].

No entanto, apesar da digitalização do comércio ser uma bandeira do futuro, o Tribunal de Justiça da União Europeia (TJUE) considerou que a *Privacy Shield* não garante a proteção de dados admitidos pela Europa. Esta conclusão advém de um processo movido pelo austríaco Maximilliam Schrems, na qualidade de utilizador do *facebook*, cujo acórdão,

---

[153] Cf. Artigo 18.º da CRP que regula os critérios da necessidade, adequação, proporcionalidade e determinabilidade em circunstâncias de restrições legais.

[154] Miranda, J. e Medeiros, R. (2017). *Constituição Portuguesa Anotada*. 2ª edição revista, v.1, Universidade Católica Editora. Lisboa. p.560-561.

[155] European Commission. (2016). *EU-U.S. Privacy Shield: Frequently Asked Questions*. Acedido em 09 de junho de 2021, em: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462.

emitido a dezasseis de julho de dois mil e vinte, ficou conhecido por "*Data Protecion Commissioner/Maximillian Schrems e Facebook Ireland*"[156].

2. A *matriz europeia* da privacidade

2.1. O direito à liberdade e à vida privada na Europa e nos Países Asiáticos - a origem dos direitos fundamentais e a atualidade

A história enquanto ciência que estuda os factos ocorridos no passado e o ser humano num determinado tempo e espaço ajuda a compreender o progresso da humanidade e relacionar os eventos cronológicos. No nosso caso, é essencial forcarmo-nos nos acontecimentos históricos que decorreram entre o século XVII e a atualidade, de forma a perceber o desenvolvimento dos direitos fundamentais, sendo certo que nem sempre foram reconhecidos nos principais diplomas internacionais ou nem sempre foram conhecidos tais como são, isto é, eram subjetivos na vida do ser humano.

Encetando pelo paradigma asiático onde os reinos e os sultanatos ainda eram visíveis na maior parte do continente, a chegada dos europeus à Ásia e a consequente colonização, entre os séculos XVII e XIX, contribuiu para que estes países desenvolvessem princípios ocidentais ainda hoje existentes, tais como: a democracia, direitos e liberdades individuais, a noção de governo e estado e o conceito de constituição enquanto fonte de direito[157].

Ao mesmo tempo, na Europa, difundia-se o Iluminismo (séc. XVIII), um movimento contra o Antigo Regime e que se centrava no indivíduo, na sua autonomia, individualidade, liberdade e dignidade. O "*Século das Luzes*", como também ficou conhecido, foi revolucionador para a época no que diz respeito ao espírito crítico e à opinião da população.

Os pilares deste movimento vão, mais tarde, contribuir para uma conceção mais concreta do que hoje conhecemos como "*direitos fundamentais"* ou "*direitos do homem*". Porém, não podemos deixar de frisar que também contribuiu para que a Europa olhasse para a Ásia (ainda colonizada) de forma "*inferior*", "*estranha*" e "*estrangeira*"[158]. Atendendo ao contexto em que vivemos, é aliciante explorar este paralelismo. O autor Arnaldo Gonçalves,

---

[156] Comunidado de Imprensa n.º91/20. *Acórdão no processo C-311/18, Data Protection Commissioner/Maximillian Schrems e Facebook Ireland*. Tribunal de Justiça da União Europeia. Luxemburgo.
[157] Hassal, G e Saunders, C. (2002). *Asia-Pacific Constitutional Systems.* Cambridge: Cambridge University Press. Reino Unido. p. 29-34.
[158] Gonçalves, A. (2005). Os valores asiáticos e os direitos humanos. *Política Internacional*. n.º27. p.15.

no mesmo excerto, afirma que os pensadores iluministas conceberam uma imagem deste continente como "*atrasado e inerte, composta por Estados despóticos e repugnantes (...)*"[159]. A Europa atual é menos desenvolvida que a Ásia, inclusive na área da tecnologia e, ainda assim, a história e o sentimento de superioridade repete-se.

Tendo em conta tudo isto, os processos de independência destes países revelaram-se cópias dos valores e fundamentos ocidentais com intuito de agradar estas potências que, até então, tinham sido as responsáveis pela sua modernização[160].

A pós-colonização, por sua vez, ficou marcada pela definição dos seus próprios princípios[161]. As diferenças entre culturas, etnias, idiomas e religiões levaram a que estes povos debatessem, em primeiro lugar, que tipo de Estado deviam adotar – um Estado Liberal-Democrático ou um Estado Socialista-Democrático sendo que estes influenciam a capacidade de distinguir os direitos fundamentais. Enquanto o Estado Liberal-Democrático protege os indivíduos e os seus direitos e permite-lhes, ao mesmo tempo, alcançar os seus próprios objetivos, o Estado Socialista-Democrático conjuga os direitos das pessoas com a sociedade, subordinando-os[162].

Observando a Ásia atual, este debate ditou a escolha de modelos de Estado que ainda hoje conhecemos desde os mais liberais aos mais corporativistas e nacionalistas[163] e, ainda, nos permite distinguir uma matriz europeia de uma matriz asiática. Esta referência estudada por vários autores serve, em grande parte, para explicar a diferença entre sociedades: por um lado posiciona os Estados Unidos da América, o Canadá e a Europa Ocidental num lado individualista cujos interesses se refletem no indivíduo autónomo e, por outro lado, devido às suas sociedades organizadas e proteção e objetivos coletivos, posiciona países da América Latina, Ásia e África num lado coletivista onde prevalece um interesse de grupo em relação ao individual[164].

---

[159] *Ibid.*

[160] Hassal, G e Saunders, C. (2002). Ob. Cit. p. 54-55 e 241-246.

[161] Note-se que nem todos os Países Asiáticos estiveram sujeitos ao Imperialismo ocidental. Serve de exemplo a China, o Japão e a Tailândia. Chen, Albert. H.Y. (2014). *Constitutionalism in Asia in the early twenty-first century*. Cambridge: Cambridge University Press. Reino Unido. p.16-31.

[162] Hassal, G e Saunders, C. (2002). *Asia-Pacific Constitutional Systems.* Cambridge: Cambridge University Press. Reino Unido. p. 34-39 e Miranda, J. (2018). *Direitos Fundamentais*. 2ª edição, Almedina. Coimbra. p.27-33.

[163] Hassal, G e Saunders, C. (2002). Ob. Cit. 43-50.

[164] Num artigo escrito ao Jornal Expresso elegemos a melhor frase que explica a diferença entre individualismo da Europa e coletivismo da Ásia no contexto da pandemia Covid-19: "*Houve e há um espírito de coletivismo na cultura asiática que chega a ser tocante – cada um é responsável por todos e proteger-se a si é proteger a*

O século XX ficou marcado pela tensão e falta de tolerância vivida durante a II Guerra Mundial (1939-1945). Quando o conflito se deu por terminado, a Europa com vista a restabelecer as relações europeias e a criar um mercado europeu comum, formou a Comunidade Económica Europeia (CEE). O Tratado de Roma[165], além de criar esta organização, debruçou-se sobre a circulação de pessoas, de bens, capitais, liberdades económicas, entre outros[166]. Todavia, a matéria de direitos fundamentais era omissa.

Recordando a nossa introdução, os direitos fundamentais nem sempre foram entendidos enquanto tais. Em mil setecentos e oitenta e nove, foi ratificada a Declaração dos Direitos do Homem e do Cidadão (DUDH), resultado das Revoluções Liberais, concretamente, da Revolução Francesa[167]. Assim, se no Tratado de Roma não existia referência a este tópico, certo é que no pós-guerra surgiram desafios e momentos que levaram a CEE a encarar esta problemática e a zelar pelos direitos individuais.

O primeiro choque de opiniões esteve relacionado com a premência de se criar um catálogo de direitos fundamentais ou aderir à Convenção Europeia dos Direitos do Homem[168] (CEDH). Estas duas visões eram defendidas, não obstante existirem defensores das duas em conjunto[169].

---

comunidade". Dias, A.P. (2020). Puxadores de portas e botões de elevadores desinfetados hora a hora. A experiência de uma portuguesa residente em Macau [Versão eletrónica]. *Jornal Expresso*. Acedido em 19 de maio de 2021, em: https://expresso.pt/opiniao/2020-03-06-Puxadores-de-portas-e-botoes-de-elevadores-desinfetados-hora-a-hora.-A-experiencia-de-uma-portuguesa-residente-em-Macau?fbclid=IwAR1rlUdrAbjSf1beNLc_XkGlsnMiM04S-jn_mKoPUregJk3YkQz5zHvwedk e Ferreira, M.C., Leal Assmar, E. M. e Oliveira Souto, S. (2002). O individualismo e o coletivismo como indicadores de culturas nacionais: convergências e divergências teórico-metodológicas. *Psicologia em Estudo*. v. 7, n.1.º, p.81-89.

[165] O Tratado de Roma foi assinado a 25 de março de mil novecentos e cinquenta e sete por seis países: Alemanha, Bélgica, França, Itália, Luxemburgo e Países Baixos. Portugal aderiu à CEE em mil novecentos e oitenta e seis. Parlamento Europeu. *Tratado de Roma (CEE).* Acedido em 23 de abril de 2021, em: https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/treaty-of-rome e EUR-Lex. (2017). *Tratado de Roma (CEE).* Acedido em 23 de abril de 2021, em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:xy0023.

[166] Moreira, V. (2007). A Constitucionalização dos Direitos Fundamentais da União Europeia (UE). In: Nascimento Silva, L. (coord.), *Estudos Jurídicos de Coimbra*. Curitiba: Juruá Editora. Brasil. p.147-150.

[167] Vieira de Andrade, J. C. (2019). *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. 6ª edição, Almedina. Coimbra. p.49-51.

[168] A Convenção Europeia dos Direitos do Homem (CEDH) foi assinada em mil novecentos e cinquenta pelo Conselho da Europa. EUR-Lex. (2017). *Convenção Europeia dos Direitos do Homem (CEDH)*. Acedido em 24 de abril de 2021, em: https://eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=pt.

[169] Moreira, V. (2007). Ob. Cit. p.150-161.

Em mil novecentos e noventa e dois e, mais tarde, em mil novecentos e noventa e sete, foram assinados os Tratados de Maastricht[170] e de Amesterdão. Estes acontecimentos são vistos como duas importantes fases na consciencialização dos direitos fundamentais[171]. Os Estados-Membros comprometeram-se, com base nas constituições e nas legislações internacionais, a reconhecer estes direitos, incluindo, o direito à cidadania.

Embora a evolução fosse notória, o objetivo ainda não estava atingido. Em dois mil, é assinada a Carta dos Direitos Fundamentais da União Europeia (CDF). Este diploma assenta em seis importantes pilares: dignidade, liberdade, igualdade, solidariedade, cidadania e justiça[172]. Paralelamente, representa um ónus político nas relações internas e externas da União Europeia. Nestas últimas, a Carta, nas palavras de Vital Moreira, representa um instrumento de "*credibilidade e eficácia da política de direitos humanos da UE*"[173].

A conquista civilizacional da Europa e a internacionalização dos direitos fundamentais permite-nos, agora, defini-los como direitos reconhecidos ao homem e à sua esfera própria. O indivíduo é visto como um ser autónomo, individual, livre e com capacidade de desenvolver a sua personalidade e os seus bens. Assim, por se tratar de direitos com um teor sensível e que facilmente podem ser ofendidos, o Estado tem o dever de os proteger de

[170] O Tratado de Maastricht ou Tratado da União Europeia foi assinado na Holanda a 7 de fevereiro de mil novecentos e noventa e dois. Este passou a identificar a Comunidade Económica Europeia (CEE) como Comunidade Europeia (CE). Parlamento Europeu. *Tratado da União Europeia (TUE)/ Tratado de Maastricht*. Acedido em 23 de abril de 2021, em: https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/maastricht-treaty.

[171] Gomes Canotilho, J.J. (2003). *Direito Constitucional e Teoria da Constituição*. 7ª edição, Almedina. Coimbra. p.523-525.

[172] Vital Moreira faz uma comparação entre estes valores com os pilares da Revolução Francesa: "*Liberdade, Igualdade e Fraternidade"*. Moreira, V. (2007). A Constitucionalização dos Direitos Fundamentais da União Europeia (UE). In: Nascimento Silva, L. (coord.), *Estudos Jurídicos de Coimbra*. Curitiba: Juruá Editora. Brasil. p.162-163.

[173] Moreira, V. (2007). Ob. Cit. p.171-172.

terceiros[174]. O autor Vieira de Andrade realça que "*a segurança é o pressuposto da liberdade*"[175].

A democracia e o seu exercício têm por base estes elementos e, por essa razão, há uma preocupação em positivá-los nas Constituições[176] não descorando aqueles que, apesar de não estarem tipificados[177], têm uma igual importância na existência e na dignidade do ser humano.

Ao Estado de Direito, fundado na dignidade da pessoa humana, compete assegurar as condições e o igual acesso aos bens protegidos pelos direitos fundamentais. O respeito e reconhecimento integrarão o sujeito na sociedade como um equivalente que tem controlo, autonomia e liberdade sobre si. Não obstante surgirem novos desafios, perigos ou poderes que precisam de uma resposta atualizada por parte do Estado de forma a proteger o cidadão[178].

Hodiernamente, vivemos numa sociedade que se informa e comunica uns com os outros sem grandes dificuldades e distâncias. A "*sociedade da comunicação*", como é conhecida, tem a capacidade de acompanhar a evolução tecnológica e científica e contribuir para a sua inovação[179]. Por outro lado, cria-se um fosso em relação à população mais velha que,

---

[174] A Declaração Universal dos Direitos do Homem, no artigo 1.º, regula: "*Todos os seres humanos nascem livres e iguais em dignidade e em direitos. Dotados de razão e de consciência, devem agir uns para com os outros em espírito de fraternidade*". Todos os seres humanos são titulares destes direitos e não podem renuncia-los. À semelhança dos direitos fundamentais, a dignidade humana constitui um elemento fundante, isto é, estes direitos devem ser reconhecidos e respeitados pelos demais uma vez que regulam o modo como os homens vivem individual e socialmente. O Estado tem o dever de cumprir estas normas nacionais e internacionais, responsabilizando-se sempre que violar um direito humano e um titular instaurar o devido pedido procedimento num tribunal competente. Unicef. *O que são direitos humanos? Os direitos humanos pertencem a todos e a todas e a cada um de nós igualmente.* Acedido em 17 de maio de 2021, em: https://www.unicef.org/brazil/o-que-sao-direitos-humanos e Gomes Canotilho, J.J. (2003). Ob. Cit. p.110-111 e 409.

[175] Vieira de Andrade, J. C. (2019). *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. 6ª edição. Almedina. Coimbra. p.49-51.

[176] Cit. "*Allí donde no hay Constitución (...) no habrá derechos fundamentales. Habrá otras cosas, con seguridad más importantes, derechos humanos, dignidad de la persona; habrá cosas parecidas, acaso igual de importantes, libertades públicas francesas, derechos públicos subjetivos alemanes; habrá, en fin, cosas distintas, como fueros o privilegios. Pero no habrá derechos fundamentales*". Cruz Villalon, P. (1989). Formación y Evolución de los Derechos Fundamentales. *Revista Española de Derecho Constitucional*. 25:41 e Gomes Canotilho, J.J. (2003). Ob. Cit. p.377.

[177] Princípio da não tipicidade dos direitos fundamentais ou cláusula aberta.

[178] Vieira de Andrade, J. C. (2019). *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. 6ª edição, Almedina. Coimbra. p.65-68 e Reis Novais, J. (2017). *Direitos Fundamentais e Justiça Constitucional.* Reimp. 2019. AAFDL Editora. Lisboa. p.49-68.

[179] A sociedade da comunicação tem, igualmente, algumas problemáticas a apontar. Durante o nosso estudo encontramos alusões ao aproveitamento que os "*descontentes*" fazem destes instrumentos, nomeadamente, das redes sociais. Desde o início da pandemia Covid-19, inúmeras foram as notícias falsas (*fake news*) com intuito de alarmar a população ou, no contexto da vacinação e uso de máscara na via pública, comentários ou campanhas contra estas medidas. Vieira de Andrade, J. C. (2019). Ob. Cit. 49-65 e Hassal, G e Saunders, C.

naturalmente, não assiste ou tem maior dificuldade de acompanhar este processo. Face a este crescimento inato, entendemos que as gerações futuras devem ser um ponto de preocupação nas principais fontes de direito, nomeadamente, nas Constituições para que não fiquem envelhecidas[180].

No nosso caso conclui-se que, desde o início, o mundo não estava preparado para uma pandemia. Veja-se que a Europa tinha conhecimento da presença do vírus na Ásia desde dezembro mas a sua preparação e preocupação apenas começou quando a Organização Mundial de Saúde declarou a pandemia em março.

A falta de capacidade e de instrumentos para lidar com a doença e as questões relacionadas com a mesma fez com que os governos, incluindo o de Portugal, adotassem estados de exceção previstos nas Constituições onde se restringem ou suspendem direitos fundamentais – estado de sítio, estado de emergência e situação de calamidade.

A criação das aplicações móveis serve como exemplo dos limites que podem ou não ser ultrapassados no âmbito da emergência sanitária. Durante este período, todas as decisões tomadas pelos executivos têm origem num desconhecido, isto é, não se comparam a nenhuma outra situação e por isso, à semelhança de uma balança, é necessário pesar os limites juntamente com os núcleos destes direitos individuais.

Não há dúvida que este tipo de tecnologia veio revolucionar o controlo dos números diários da pandemia e, nos casos em que a geolocalização é adotada, na delimitação das zonas mais afetadas. Todavia, a taxa de utilização não foi alcançada e, desde logo, surgiram críticas de violação de privacidade e mau funcionamento. Consequentemente, a população deixou de confiar nestas ferramentas ignorando o seu objetivo e preferindo o tratamento das suas informações de forma não automatizada. A pessoalidade e a interação entre o paciente e o profissional de saúde aumentou exponencialmente e, muitas das vezes, em situações não urgentes.

Carecemos, de forma similar, de fazer uma comparação entre a restrição feita à livre circulação de pessoas (entre concelhos, países, períodos festivos) e a limitação feita com base nas *APP*s. A escolha da tecnologia *Bluetooth Low Energy* ou geolocalização em nada influencia no momento em que o indivíduo sai à rua ou frequenta uma área e muda o seu percurso atendendo o alerta de um contacto próximo. Este tipo de prevenção, às vezes

(2002). *Asia-Pacific Constitutional Systems.* Cambridge: Cambridge University Press. Reino Unido. p. 241-246.

[180] Miranda, J. (2018). *Direitos Fundamentais*. 2ª edição, Almedina. Coimbra. p.47-54.

desnecessária, levou a que muitas pessoas entrassem num estado de inquietação e nervosismo. Num estudo realizado em Portugal intitulado "*Estudo Saúde Mental em Tempos de Pandemia SM-Covid19*", 25% dos participantes apresentaram sintomas de ansiedade, depressão e *stress* pós-traumático. A situação pandémica favoreceu estes sentimentos aliado ao desassossego de voltar a viver uma crise económica, de não trabalhar ou trabalhar presencialmente e recuperar o modo de vida anterior[181].

A apoquentação pode gerar, também, grupos de privilegiados e desprivilegiados. Vimos, anteriormente, que as faixas etárias mais velhas não acedem facilmente a estas *APP*s, no entanto nos países e cidades europeias e asiáticas, onde a qualidade de vida não é grande o mesmo acontece. Estes povos constituem grupos marginalizados ou minorias raciais cujas oportunidades não se irmanam aos restantes. A crise de saúde pública em que vivemos veio perturbar a paz e a sua organização demonstrando que estes habitantes não só não tiveram acesso a esta tecnologia, como também não tiveram acesso a um tratamento médico digno[182].

Em suma, a comunicação entre os criadores destas *APP*s e os governos e, consequentemente, com os cidadãos não foi bem sucedida. Considerando que cada nação é diferente, a publicidade e a explicação feita à volta destes instrumentos deve ser clara e concreta. Porém, vemos que passado um ano desde o início da pandemia as pessoas retêm os aspetos negativos e não os positivos e, em determinados casos, mantêm-se as dúvidas de como é que uma aplicação móvel funciona e como é que é útil nesta condição.

As restrições dos direitos fundamentais são possíveis e nos casos de emergências sanitárias podem ser justificadas, contudo parece-nos que o núcleo da privacidade e da liberdade foi violado e que as incertezas dos utilizadores não são despropositadas. Os Estados durante o seu exercício reflexivo são obrigados a problematizar e a ponderar os bens jurídicos e que direitos vão ser afetados. Em matéria de acesso e proteção de dados, dada a novidade, evidencia-se a desconsideração.

Se a pandemia Covid-19 é um problema e se estas *APP*s, criadas com um propósito e para um determinado tempo, caíram em desuso não há razão para continuarem ativas e serem

---

[181] Coordenado pelo Departamento de Promoção da Saúde e Prevenção de Doenças Não Transmissíveis do Instituto Nacional de Saúde Doutor Ricardo Jorge, em colaboração com o Instituto Nacional de Saúde Ambiental da Faculdade de Medicina da Universidade de Lisboa e Sociedade Portuguesa de Psiquiatria e Saúde Mental. Serviço Nacional de Saúde. (2021). *Estudo Saúde Mental em Tempos de Pandemia (SM-COVID19): principais resultados.* Acedido em 27 de abril de 2021, em: http://www.insa.min-saude.pt/estudo-saude-mental-em-tempos-de-pandemia-sm-covid19-principais-resultados/.

[182] Tavares da Silva, S. (2014). *Direitos fundamentais na arena global*. 2ª edição, Coimbra: Imprensa da Universidade de Coimbra. Coimbra p. 44-45.

sujeitas a ataques informáticos. Á existência de um obstáculo adita-se um segundo quando a probabilidade dos dados dos utilizadores serem roubados aumenta. Nestes casos, a capacidade de resposta por parte do Estado é diminuta e a do usuário envolve custas.

3. As medidas adotadas em Portugal no âmbito da proteção da privacidade

Os portugueses, à semelhança dos países europeus e do mundo, criaram, como já tivemos a oportunidade de descortinar, a aplicação móvel STAYAWAY COVID como instrumento de combate à pandemia mundial em que vivemos.

Vimos que os principais motivos para a população portuguesa desacreditar neste método advêm da ausência de códigos gerados, a falta de conhecimento no uso da aplicação móvel e a falta de recomendação por parte do executivo e autoridades de saúde.

Recentemente, quando os portugueses já consideravam a *APP* inútil ao objetivo principal e, igualmente, com as fases de desconfinamento cada vez mais alargadas, Henrique Faria, aluno do Mestrado de CiberSegurança da Escola Superior de Tecnologia e Gestão do Politécnico de Viana do Castelo (IPCV), veio reforçar esta dispensabilidade com a descoberta de um *bug* ou erro, designado "*advertising* overflow", em todas as aplicações que utilizam o sistema da "Notificação de Exposição Google-Apple" (GAEN)[183], incluindo a portuguesa.

No exposto pela faculdade, este erro permite que as *APP*s sejam acedidas por um terceiro, geralmente considerado *hacker*, e compromete o rastreamento e a transmissão de dados enviados por uma pessoa infetada com intuito de avisar os utilizadores que se encontrem próximos, não enviando nenhum aviso de exposição[184]. A vulnerabilidade com que nos deparamos é patente.

Inserindo o tema dos metadados em Portugal, ou seja, dados de dados, deparamo-nos com o Acórdão do Tribunal Constitucional n.º464/2019 e com a consequente crítica de Maria Clara Sottomayor (Juíza do Supremo Tribunal de Justiça) que convoca a fragilidade deste assunto.

[183] A multinacional norte-americana Google reconheceu o *bug* reportado pelo aluno no programa *Google Vulnerability Reward Program*, valendo uma menção honrosa no *Bughunter Hall of Fame.*

[184] Instituto Politécnico de Viana do Castelo. (2021). *Aluno do IPCV deteta Bug que afeta Apps de rastreamento Covid a nível mundial*. Acedido em 14 de junho de 2021, em: https://www.ipvc.pt/11447-2/?cli_action=1623665497.503.

O presente acórdão aprecia a constitucionalidade, em processo de fiscalização abstrata sucessiva, dos artigos 3.º[185] e 4.º[186] da Lei Orgânica n.º4/2017, de 25 de agosto que aprova e regula o "*procedimento especial de acesso a dados de telecomunicações*[187] *e Internet*[188] *pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário)*".

A sobredita lei foi aprovada em Assembleia da República, com os votos favoráveis do PSD, PS e CDS-PP, desfavoráveis do BE, PCP e PEV e abstenção do PAN, e tem como origem a proposta de lei n.º79/XIII/2ª da iniciativa do Governo e o projeto de lei n.º480/XIII/2ª da iniciativa de dezoito deputados do Grupo Parlamentar do CDS-PP[189].

Observando o artigo 3.º, o Tribunal Constitucional dividiu a norma em dois segmentos. Por um lado, declara inconstitucional, por violação dos artigos 26.º, número 1.º, 35.º, número 1.º e 4.º e 18.º, número 2.º da CRP, a secção que admite o acesso dos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas e de Defesa (SIED), relativamente a dados de base[190] e de localização de equipamento[191],

---

[185] Cit. Artigo 3.º da Lei Orgânica n.º4/2017, de 25 de agosto: "*Os oficiais de informações do SIS e do SIED podem ter acesso a dados de base e de localização de equipamento para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito*".

[186] Cit. Artigo 4.º da Lei Orgânica n.º4/2017, de 25 de agosto: "*Os oficiais de informações do SIS e do SIED apenas podem ter acesso a dados de tráfego para efeitos de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo*".

[187] Cit. Artigo 2.º, número 1.º, alínea a) da Lei Orgânica n.º4/2017, de 25 de agosto: "*«Dados de telecomunicação», os registos ou informação constantes de banco de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas relativos à prestação de serviços telefónicos acessíveis ao público e à rede de suporte à transferência, entre pontos terminais da rede, de comunicações vocais, serviços de mensagens e multimédia e de outras formas de comunicação*".

[188] Cit. Artigo 2.º, número 1.º, alínea a) da Lei Orgânica n.º4/2017, de 25 de agosto: "*«Dados de Internet», os registos ou informações constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, relativos a sistemas de transmissão e a equipamentos de comutação ou encaminhamento que permitem o envio de sinais ou dados, quando não deem suporte a uma concreta comunicação*".

[189] Gomes Machado, M. (2019). *O acesso aos metadados pelos serviços de informações da República Portuguesa, à luz da lei e da constituição.* Tese de Mestrado em Direito e Segurança – Faculdade de Direito da Universidade de Lisboa. Lisboa. p. 22-23.

[190] Cit. Artigo 2.º, número 2.º, alínea a) da Lei Orgânica n.º4/2017, de 25 de agosto: "*«Dados de base», os dados para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede*".

[191] Cit. Artigo 2.º, número 2.º, alínea b) da Lei Orgânica n.º4/2017, de 25 de agosto: "*«Dados de localização de equipamento», os dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público, quando não deem suporte a uma concreta comunicação*".

quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e segurança interna.

Por outro lado, admite o segmento dos oficiais de informações destes serviços no âmbito das respetivas atribuições, relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada[192].

Similarmente, o Tribunal Constitucional divide o artigo 4.º em duas partes, declarando-as inconstitucionais. Numa primeira parcela, aprecia a inconstitucionalidade, por violação do artigo 34.º, número 4.º, no acesso aos dados de tráfego[193] que envolvem comunicação intersubjetiva e, numa segunda, por violação do disposto nos artigos 26.º, número 1.º, 35.º, números 1.º e 4.º e 18.º, número 2.º, no que se refere ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva[194].

Cotejado o cerne da lei, vejamos a crítica de Maria Clara Sottomayor intitulada "*Uma análise crítica do Acórdão do Tribunal Constitucional n.º464/2019: o sistema de acesso a metadados ou a segurança versus liberdade*"[195]. Ora, a autora selecionada por sorteio para relatora do acórdão explica, de forma pormenorizada, os motivos pelos quais não se revê no seu conteúdo. Independentemente do teor das normas, conclui-se que o Tribunal Constitucional, doravante TC, utilizou critérios díspares e vagos na apreciação da inconstitucionalidade de ambos os artigos e, por isso, a fundamentação assenta numa intricada leitura.

Olhando para o artigo 3.º, a inconstitucionalidade do primeiro segmento baseia-se na incompatibilidade com as restrições estabelecidas nos termos do artigo 18.º, número 2.º da CRP. Entende a juíza que, estando em causa a proteção dos bens jurídicos da segurança e da defesa nacional, não se justifica o raciocínio do TC relativo à indeterminação destes

---

[192] Acórdão n.º464/2019, de 21 de outubro. *Diário da República n.º202/19 – 1ª Série*. Tribunal Constitucional. Lisboa.

[193] Cit. Artigo 2.º, número 2.º, alínea c) da Lei Orgânica n.º4/2017, de 25 de agosto: "*«Dados de tráfego», os dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações, ou para efeitos da faturação da mesma*".

[194] Acórdão n.º464/2019, de 21 de outubro. Ob. Cit.

[195] Sottomayor, M. C. (2020). Uma análise crítica do Acórdão do Tribunal Constitucional n.º464/2019: o sistema de acesso a metadados ou a segurança versus liberdade [Versão eletrónica]. *Julgar*. Acedido a 15 de junho de 2021, em: http://julgar.pt/uma-analise-critica-do-acordao-do-tribunal-constitucional-n-o-4642019-o-sistema-de-acesso-a-metadados-ou-a-seguranca-versus-liberdade/.

conceitos, uma vez que o artigo 4.º sugere o semelhante e, mesmo assim, a norma foi declarada inconstitucional, na sua totalidade.

Assim sendo, não nos parece proporcional utilizarem um critério numa norma e dessaber para a outra. Acrescente-se ainda que a intervenção do SIS e do SIED deve direcionar-se para os bens jurídicos que decorram da dignidade da pessoa humana e, como tal, tendo em conta estes argumentos, a redatora considera que toda a norma deve ser inconstitucional por violação nos artigos 26.º, número 1.º, 35.º, número 1.º e 4.º, em conjugação com o artigo 18.º, número 2.º da CRP.

Em contrapartida, no artigo 4.º, Maria Clara Sottomayor salienta a mesma disparidade na atuação do SIS e do SIED em matéria de prevenção de atos de espionagem e terrorismo. O critério utilizado não é proporcional pois os dados de tráfego que não envolvem comunicação intersubjetiva, nas suas palavras, "*podem ser tão mais reveladores da personalidade do utilizador do que os dados de tráfego que envolvem comunicação intersubjetiva*"[196].

As empresas de telecomunicações e *internet* que retêm informações dos cidadãos, geralmente durante um ano, estariam a autorizar o acesso à esfera privada dos cidadãos por parte destes serviços de informações do Estado[197] e a potenciar a criação de perfis considerados "perigosos" sem razão aparente e fora de um processo penal ou judicial.

Não descurando a importância do terrorismo e o seu combate, os motivos que levaram a autora a não concordar com a argumentação no Acórdão n.º464/2019 parecem-nos pertinentes e plausíveis: (1) a indeterminação do conceito de perigo, (2) a não exigência de um dever de notificação *a posteriori* aos cidadãos visados pela ingerência e (3) a incerteza em relação à extensão do conceito do terrorismo[198].

Tratando-se de direitos fundamentais, entende-se que a posição que o TC tomou não é concreta e cognoscível a todas as circunstâncias. A vaguidade destes conceitos leva a que os serviços de informação possam interceder sem causa justificável até porque, com o desenvolvimento da tecnologia, novas formas de terrorismo e espionagem são criadas.

Deste modo, de forma a evitar uma excessiva intervenção, sugere a relatora que a notificação aos visados seja obrigatória em casos como estes. Qualquer pessoa, incluindo as apontadas como suspeitas, teria a oportunidade de acionar os "*meios de reação e de*

[196] *Ibid.* p.11.
[197] Veja-se que os serviços de informações não são órgãos de polícia criminal.
[198] Sottomayor, M. C. (2020). Ob. Cit. p.35.

responsabilização do Estado" necessários e adequados em caso de acesso ilícito, solicitação de destruição de dados e indemnização.

Num artigo de opinião escrito pela juíza, "*a posição que veio a ficar consagrada no Acórdão, apesar de reconhecer o problema, acaba por se conformar com ele*"[199]. Embora não seja a primeira lei apresentada concernente a metadados, fica aberta a possibilidade de, no futuro, ser proposta uma nova lei conforme à Constituição e às novas formas de abordagem utilizadas no terrorismo e espionagem.

Em virtude dos factos mencionados, citamos Maria Clara Sottomayor, com aquela que nos parece ser a conclusão apropriada ao acórdão aludido e ao risco que as *APP*s estão expostas: «*a luta contra o terrorismo, se bem que satisfazendo uma legítima necessidade coletiva de segurança dos Povos, não se deve transformar num "direito penal do inimigo", que conduz à estigmatização de determinados indivíduos e à perda de privacidade e de liberdade dos cidadãos em geral*»[200].

4. A "intransponibilidade" deste standard de proteção e as consequências no combate à pandemia

Ao longo da nossa dissertação procuramos, de forma informal, reunir opiniões de diferentes personalidades relativamente às aplicações móveis, o seu sucesso e insucesso e o que de novo podia trazer no combate às pandemias. Na sua generalidade, diríamos que o descontentamento ou a irrelevância foi a resposta mais escutada, porém há uma que sobressai pela analogia construída.

As aplicações móveis assemelham-se ao código da estrada, ou seja, quando circulamos, seja qual for o meio, respondemos às normas que nos são dispostas, como por exemplo: um sinal de stop, uma cedência de passagem ou uma passadeira para peões. Sabemos, também, que à partida, se não respeitarmos esses símbolos temos uma consequência.

Nas *APP*s são-nos apresentadas, de igual forma, regras de funcionamento. Contudo enquanto que na sinalética da estrada os sinais são exibidos de forma organizada e apresentável, nas *APP*s da maioria do mundo, o mesmo não acontece e geram-se dúvidas que levam as populações a circularem sem entenderem o propósito. Comparando-o com um

[199] Sottomayor, M. C. (2019). É mina honra de juíza [Versão eletrónica]. *Jornal Públic*o. Acedido em 15 de junho de 2021: em https://www.publico.pt/2019/12/09/politica/opiniao/honra-juiza-1896464.
[200] Sottomayor, M. C. (2020). Ob. Cit. p.35.

radar, numa utopia onde tudo funcionaria, saberíamos a que velocidade poderíamos andar e compreenderíamos as limitações impostas pelos executivos e pelas próprias aplicações.

Fazendo um balanço das *APP*s entre os dois continentes em estudo, asseguramos que as aplicações móveis dos Países Asiáticos tiveram melhores resultados que na Europa. O sucesso está, em grande parte, relacionado com o avançado desenvolvimento tecnológico, com o planeamento organizado e a mentalidade da população.

Na Ásia, existem dois países que se destacam – a Coreia do Sul e a China. Atente-se, em primeiro lugar, na Coreia do Sul. Em dois mil e quinze, este território registou cento e oitenta e cinco casos e seis mortes por Síndrome Respiratório do Médio Oriente (MERS-CoV)[201], entre maio e julho. Este surto, de menor escala, preparou-os, de certa forma, para uma resposta contra a Covid-19 achatando a curva de contágio mais rápido que os restantes países.

O governo coreano procurou, desde a fase preliminar, incentivar e recomendar a população a realizar testes de despiste e a rastrear cadeias de contacto. As aplicações móveis, neste âmbito, eram indispensáveis para aqueles que se encontravam em quarentena e deviam alertar as autoridades para os seus sintomas e no caso de quebrarem o isolamento. Em comparação com as medidas que conhecemos, este país não tomou medidas restritivas uma vez que a mentalidade destes habitantes é, por si só, disciplinada. Assim, devido à grande responsabilidade e dever cívico em utilizar a máscara de proteção, manter a distância social e desinfetar as mãos frequentemente, a Coreia do Sul permitiu que a sua economia se mantivesse equilibrada e não sofressem um abalo.

Confrontando com a Itália, este país europeu foi o mais afetado pela pandemia na primeira vaga. O confinamento total foi dos primeiros a ser decretado devido ao número elevado de contágio e de mortes. As imagens deste povo fechado em casa percorreram o mundo no entanto, embora a disseminação tenha sido rápida, multiplicaram-se testemunhos em como os italianos não respeitaram estas medidas e, inclusive, praticavam ajuntamentos em datas festivas sem respeitar as regras de saúde pública.

No que concerne à *APP Immuni*, tal como em Portugal, não foram atingidos os efeitos desejados em virtude da falta de investimento em publicidade e de conhecimento por parte

[201] O MERS-CoV foi pela primeira vez identificado em dois mil e doze na Arábia Saudita e afeta o aparelho respiratório. Tal com o síndrome SARS-CoV-2, não há uma certeza da sua origem, contudo crê-se que se trata de uma zoonose, isto é, doenças transmitidas por animais. Serviço Nacional de Saúde. *MERS-CoV*. Acedido em 20 de junho de 2021, em: https://www.dgs.pt/paginas-de-sistema/saude-de-a-a-z/coronavirus/mers-cov.aspx.

dos responsáveis que cuidavam do rastreio. Deste modo, confirma-se que a deceção é superior à confiança.

A China, a maior nação em termos populacionais e económicos na Ásia, aplicou regras exigentes que se fizeram ressentir na Europa[202] e, ao contrário da estratégia mundial, optou for confinar zonas e não o território nacional. Wuhan, território onde se crê que está a origem da doença, foi a primeira região a entrar em quarentena seguindo-se as restantes províncias de Hubei. As razões para esta planificação estão na curva de contágio e, essencialmente, na concentração de recursos humanos por áreas registadas através do sistema de geolocalização da *APP Alipay Health Code*.

Assim, a China não só praticou uma testagem em massa entre os chineses, como restringiu o acesso ao seu território por turistas, fechou locais de interesse público e, de forma surpreendente, investiu de forma vigorosa na área da saúde construindo hospitais em tempo recorde, nunca outrora visto.

Causa-nos alguma surpresa ver que a Singapura não é um dos países bem-sucedidos no combate contra a pandemia Covid-19. O seu modelo de aplicação móvel demonstrou ser, na nossa opinião, dos melhores executados e com impacto na sociedade. Todavia, enquanto mundo e a Organização Mundial de Saúde viam este país como um exemplo, no seio dos habitantes que vivem em condições vulneráveis, os números aumentavam. Estes trabalhadores estrangeiros vivem em dormitórios com condições precárias onde se chegam a albergar vinte pessoas.

Este facto vem salientar o que já referimos em capítulos anteriores. A discriminação daqueles que vivem em melhores e piores condições reflete-se na ação dos executivos. Igualmente, com o desenvolvimento das vacinas pelos laboratórios, essa desigualdade ressalta. Entre os países em estudo, o poder económico e o poder político diferencia-se e, muitas das vezes, os mesmos sobrepõem-se à urgência em findar esta doença[203].

---

[202] Relembre-se que em abril de dois mil e vinte, na Europa, existia uma escassez de equipamentos de proteção individual para os cidadãos e equipas hospitalares. Esta carência levou à inflação de preços destes materiais e à utilização de outras técnicas de proteção pessoal.

[203] Cit. "*A crise tem exercido pressão sobre as relações já fragilizadas entre países da zona euro e da UE e, certamente, exacerbou as tensões entre os EUA e a China, além de outras relações comerciais importantes*" e "*Alguns líderes autoritários já estão a usar esta crise como oportunidade para consolidar poder e suspender a democracia. À medida que as eleições são adiadas e as aglomerações públicas são poribidas por razões de saúde, muitos países com normas e instituições democráticas que já eram frágeis antes da Covid-19 podem vir a adotar formas mais autocráticas de governo"*. World Business Council for Sustainable Development. (2020). *As consequências da Covid-19 para a próxima década. Nota Informativa da Visão 2050*. Portugal. p.12 e 13.

Nesta nova etapa em que vivemos, as *APP*s são também visíveis. A União Europeia criou, a vinte de maio do presente ano, o Certificado Digital COVID que permitirá a todos os que já estão vacinados viajarem sem restrições entre países europeus. Porém, para aqueles que optarem por não tomar a vacina, não será impeditivo de viajar dado que a liberdade de circulação constitui um direito fundamental.

Cada Estado-Membro, de forma a facilitar o fluxo humano e adequar as medidas dentro do país, tem a liberdade de decidir em que moldes é que estes documentos vão ser emitidos: seja em suporte papel, digital ou através das aplicações móveis que temos vindo a analisar. Assim, através de um QR Code que contém dados pessoais como[204]: nome, data de nascimento, data de emissão, informações sobre a vacina/teste/recuperação, um identificador único, o cidadão europeu poderá reconhecer o seu estado e as empresas criadoras das aplicações móveis poderão relançar as suas ferramentas.

No dia em que o certificado entrar em vigor, concretamente no dia um de julho, os Estados-Membros, além de solicitarem este documento, poderão também pedir um teste negativo ou uma prova de como já teve Covid e está recuperado. Num quadro disponibilizado pela Comissão Europeia constatamos que embora os países, onde se incluem Listenstaine, Suíça, Islândia e Noruega, já estejam aptos à ligação efetiva ao portal, a Hungria e a Malta ainda se encontram em "fase de ensaio" [205].

Iniciativas como esta encorajam o fim desta conjuntura. Se recuarmos até o início de dois mil e vinte nada nos faria julgar que, nos dias de hoje, estaríamos a meses de atingir a imunidade de grupo. À questão "como é que se combate uma pandemia?", diríamos que não existe uma resposta correta. Cada enfermidade facilmente transmissível traz novos problemas e, com a evolução das sociedades, surgirão novas formas de as combater seja com medidas mais ou menos favoráveis.

Num estudo intitulado "*As consequências da Covid-19 para a próxima década. Nota Informativa da Visão 2050*", são identificadas mais de 30 mil zoonoses. Estes fenómenos devem-se às alterações climáticas, à urbanização e globalização, a pressão feita nos

[204] De acordo com a Comissão Europeia estas informações não são armazenadas pelos Estados-Membros de destino.

[205] Comissão Europeia. *Certificado Digital COVID da UE.* Acedido em 22 de junho de 2021, em: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_pt#o-que-o-certificado-digital-covid-da-ue.

ecossistemas e na biosfera[206]. É, por isso, urgente o investimento na área da sustentabilidade para que períodos como este não se repitam.

Se, por um lado, esta crise fomentou laços de solidariedade e de comunidade, por outro, gerou cenários de recessão económica e dificuldades sociais entre as grandes e pequenas economias. Os autores da análise anteriormente mencionada afirmam que "*parece ser consensual que a crise COVID-19 expõe fragilidades bem mais profundas e que a resposta terá de ser mais estrutural, disruptiva e de longo prazo*"[207].

Concluindo, os governos do mundo implementaram os confinamentos obrigatórios, fecharam fronteiras entre países, apostaram na testagem e no rastreio de infetados, investiram em apoios sociais para os mais carenciados e lançaram aplicações móveis como ferramenta surpresa e de resposta imediata. Todavia, o que viria a ser o passo tecnológico mais mediático deste caminho, transformar-se-ia num fiasco.

As aplicações móveis não acrescentaram nada ao ser humano até porque existem milhares de pessoas infetadas que são assintomáticas e, à partida, não vão sinalizar a sua conta como perigosa ou sujeita a contagiar. Ressalva-se o papel das equipas médicas, o motor neste hiato de tempo, não só em Portugal mas em qualquer zona do mundo que, mesmo com as debilidades dos sistemas de saúde a serem expostas, permitiram que o auxílio chegasse.

Hodiernamente, as reflexões devem ser feitas por quem é devido. Espera-se que o mundo tenha aprendido que o nosso modo de viver, promovido pelo consumo em excesso, potencia estas infeções. Desta maneira, novas práticas de sustentabilidade devem ser implementadas e incutidas aos cidadãos e, quiçá no futuro, estas aplicações móveis que analisamos ao longo de três capítulos e outras que virão sejam a ferramenta ideal para proteger as sociedades.

[206] World Business Council for Sustainable Development. (2020). p.3.
[207] *Ibid.*

Conclusão

A presente investigação leva-nos a concluir que as aplicações móveis e outras tecnologias semelhantes são o futuro na resposta a necessidades de rastreio de contactos. Todavia, há ainda uma necessidade de aperfeiçoamento e de rigor que deve ser trabalhado para se chegar a resultados que, durante esta pandemia, não se verificaram.

As *APP*s constituíram um primeiro teste ao uso da tecnologia de automação como forma de auxílio na execução de tarefas administrativas. Mas foram também um teste de stress ao modo como o uso destas tecnologias se pode compatibilizar com os direitos, liberdades e garantias que são a matriz das sociedades ocidentais, contrastando com a "menor relevância" que lhes é dada nos sistemas asiáticos.

A cooperação mundial foi, também, posta à prova persistentemente. Os líderes mundiais olvidaram que a colaboração entre si é essencial para que as sociedades sintam confiança em sistemas deste tipo. As divergências contantes entre os países e as suspeitas quanto à "bondade" do uso destes meios tecnológicos puseram de sobreaviso as sociedades. Espera-se, por isso, que no futuro possam ser construídas soluções tecnológicas que suscitem confiança a todos os líderes políticos para que possamos enfrentar crises futuras com novos instrumentos.

As novas gerações têm vindo a demonstrar que confiam no uso da tecnologia. A sua relação com dispositivos móveis, ambiente, sustentabilidade, mobilidade, direitos fundamentais, entre outros, apresenta novos contornos que é pertinente debater. Assim, espera-se que os sistemas e as legislações que agora vigoram possam acomodar estas novas soluções.

A nova etapa da vacinação surge como esperança de voltarmos a viver nos moldes em que sempre vivemos. Ficará registado na história este período conturbado, ainda sem data para findar, caracterizado não só por perdas, pelo isolamento, pela falta de relacionamentos interpessoais e esforços coletivos, como também, de um espírito de solidariedade e interajuda, da importância da investigação científica, dos sistemas nacionais de saúde e os seus profissionais e outros tantos ensinamentos para um vindouro fenómeno igual ou parecido.

Bibliografia

Albert, H..Y. CHEN, *Constitutionalism in Asia in the early twenty.first century*, Cambridge: Cambrimbridge University Press, Reino Unido, 2014.

Alexandre Sousa PINHEIRO, Cristina Pimenta COELHO, Tatiana DUARTE, Carlos Jorge GONÇALVES e Catarina Pina GONÇALVES, *Comentário ao Regulamento Geral de Proteção de Dados*, Almedina, Coimbra, 2018.

Alexandre Sousa PINHEIRO, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, AAFDL – Associação Académica da Faculdade de Direito de Lisboa, Lisboa, 2015.

André MILANI, *Programando para iPhone e iPad*, 2ª edição, Novatec, Brasil, 2014.

Bruno Ricardo BIONI, *Proteção de dados pessoais: a função e os limites do consentimento*, Editora Forense, Rio de Janeiro, 2019.

Catarina Sarmento e CASTRO, «Art8.º - Proteção de dados pessoais», in *Carta dos Direitos Fundamentais da União Europeia: comentada,* sob a direção de Alessandra SILVEIRA e Mariana CANOTILHO, Almedina, Coimbra, 2013. p. 120-128.

Catarina Sarmento e CASTRO, *Direito da informática, privacidade e dados pessoais: a propósito da legalização de tratamentos de dados pessoais (incluindo vigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso*, Almedina, Coimbra, 2015.

Filipa Urbano CALVÃO, *Direito da proteção de dados pessoais: relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*, Universidade Católica Editora, Porto, 2018.

Gilberto Farias de Sousa FILHO e Eduardo de Santana Medeiros ALEXANDRE, *Introdução à Computação*, 2ª edição, Editora da UFPB, Brasil, 2014.

Graham GREENLEAF, *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford University Press, United Kingdom, 2014.

Graham HASSAL e Cheryl SAUNDERS, *Asia-Pacific Constitutional Systems*, Cambridge: Cambridge Uniersity Press. Reino Unido, 2002.

Jorge MIRANDA, *Direitos Fundamentais*, 2ª edição, Almedina, Coimbra, 2018.

Jorge MIRANDA e Rui MEDEIROS, *Constituição Portuguesa Anotada*, 2ª edição, v.1, Universidade Católica Editora, Lisboa, 2017.

Jorge Reis NOVAIS, *Direitos Fundamentais e Justiça Constitucional*, AAFDL Editora, Lisboa, 2017.

José Carlos Vieira de ANDRADE, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 6ª edição, Almedina, Coimbra, 2019.

José Joaquim Gomes CANOTILHO, *Direito Constitucional e Teoria da Constituição*, 7ª edição, Almedina, Coimbra, 2003.

José Joaquim Gomes CANOTILHO e Vital Moreira, *Constituição da República Portuguesa Anotada*, 4ª edição, v.1, Coimbra Editores, Coimbra, 2007.

Luiz Carlos Querino FILHO, *Desenvolvendo o seu primeiro aplicativo Android*, 2ª edição, Novatec, Brasil, 2017.

Paulo Mota PINTO, *Direitos de Personalidade e Direitos Fundamentais*, 1ª edição, Gestlegal, Coimbra, 2018.

Suzana Tavares da SILVA, *Direitos Fundamentais na Arena Global*, 2ª edição, Coimbra: Imprensa da Universidade de Coimbra, Coimbra, 2014.
Vital MOREIRA, «A Constitucionalização dos Direitos Fundamentais da União Europeia (UE)» in *Estudos Jurídicos de Coimbra*, sob a direção de Luciano Nascimento SILVA, Curitiba: Juruá Editora, Brasil, 2007. p. 147-183.

Documentos Disponíveis Online:

- **Artigos de Jornais – Versão Eletrónica:**

Diário de Notícias. (2020). "O que dizem os partidos sobre a obrigatoriedade da app StayAwayCovid", *Diário de Notícias*. Disponível em: <https://www.dn.pt/poder/o-que-dizem-os-partidos-sobre-a-proposta-de-obrigatoriedade-da-app-stayaway-covid-12924386.html>. Acesso em: 20 de janeiro de 2021.

Dias, A.P. (2020). "Puxadores de portas e botões de elevadores desinfetados hora a hora. A experiência de uma portuguesa residente em Macau". *Jornal Expresso*. Disponível em: <https://expresso.pt/opiniao/2020-03-06-Puxadores-de-portas-e-botoes-de-elevadores-desinfetados-hora-a-hora.-A-experiencia-de-uma-portuguesa-residente-em-Macau?fbclid=IwAR1rlUdrAbjSf1beNLc_XkGlsnMiM04S-jn_mKoPUregJk3YkQz5zHvwedk>. Acesso em: 19 de maio de 2021.

Pequenino, K. (2020). "China atribui código QR aos cidadãos para conter coronavírus", *Jornal Público*. Disponível em: <https://www.publico.pt/2020/03/06/tecnologia/noticia/china-atribui-codigo-qr-cidadaos-conter-coronavirus-1906462>. Acesso em: 23 de janeiro de 2021.

Pequenino, K. (2021). "60% já pagaram a StayAwayCovid: são 1,8 milhões de portugueses", *Jornal Público*. Disponível em: <https://www.publico.pt/2021/01/15/tecnologia/noticia/60-ja-apagaram-stayaway-covid-sao-18-milhoes-portugueses-1946366>. Acesso em: 18 de janeiro de 2021.

Séneca, H. (2021).“StayAway Covid já está disponível para iPhones mais antigos”, *Jornal Expresso*. Disponível em: <https://expresso.pt/sociedade/2021-01-26-StayAway-Covid-ja-esta-disponivel-para-iPhones-mais-antigos>. Acesso em: 11 de fevereiro de 2021.

Sottomayor. M. C. (2019). “É mina honra de juíza”. *Jornal Públic*o. Disponível em: <https://www.publico.pt/2019/12/09/politica/opiniao/honra-juiza-1896464>. Acesso em: 15 de junho de 2021.

The Moscow Times, Independent News From Russia. (2020). “Russia Develops Coronavirus Contact-Tracing App”. *The Moscow Times*. Disponível em: <https://www.themoscowtimes.com/2020/11/17/russia-develops-coronavirus-contact-tracing-app-a72068>. Acesso em: 30 de janeiro de 2021.

- **Artigos Online:**

Abdelkrim. (2020) “Covid-19, Mobile apps that preserve privacy, And the winner is …”, *Medium*. Disponível em: <https://medium.com/@Abdelkrim/covid-19-mobile-apps-that-preserve-privacy-and-the-winner-is-68c72e098fca>. Acesso em: 15 de janeiro de 2021.

Amnistia Internacional. (2020). “Aplicações de rastreio de contactos de Noruega, Bahrein e Kuwait entre as mais perigosas para a privacidade”. Disponível em: <https://www.amnistia.pt/aplicacoes-de-rastreio-de-contactos-de-noruega-bahrein-e-kuwait-entre-as-mais-perigosas-para-a-privacidade/>. Acesso em: 27 de janeiro de 2021.

Associação D3-Defesa dos Direitos Digitais. (2020). “Comunicado sobre Stayaway Covid”. Disponível em: <https://www.direitosdigitais.pt/comunicacao/comunicados/106-comunicado-sobre-stayaway>. Acesso em: 20 de janeiro de 2021.

Associação D3-Defesa dos Direitos Digitais. (2021). “D3 condena ataque aos médicos e exige o fim da app Stayaway Covid”. Disponível em: <https://www.direitosdigitais.pt/comunicacao/comunicados/114-d3-condena-ataque-aos-medicos-e-exige-fim-da-app-stayaway-covid>. Acesso em: 20 de janeiro de 2021.

BruHealth. (2020). “Privacy Policy”. Disponível em: <https://www.healthapp.gov.bn/covid19/bruhealth/privacy_policy.html>. Acesso em: 30 de janeiro de 2021.

_____. “Terms of Use”. Disponível em: <https://www.healthapp.gov.bn/covid19/bruhealth/term_of_use.html>. Acesso em: 17 de março de 2021.

Comissão Nacional de Proteção de Dados. (2021). “O que somos e quem somos”. Disponível em: <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>. Acesso em: 16 de janeiro de 2021.

Comissão Europeia. “Certificado Digital COVID da EU”. Disponível em: <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_pt#o-que-o-certificado-digital-covid-da-ue>. Acesso em: 22 de junho de 2021.

Comissão Europeia. “Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?”. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt>. Acesso em: 3 de março de 2021.

Corona Melder. (2020). “Corona Melder Privacy Statement”. Disponível em: <https://coronamelder.nl/en/privacy>. Acesso em: 30 de janeiro de 2021.

Corona Tracer BD. (2020). “Terms of Service”. Disponível em: <https://tracercdn.shohoz.com/privacy_policy/index.html>. Acesso em: 30 de janeiro de 2021.

Covid Alert. (2020). “Privacy Policy-Covid Alert Malta”. Disponível em: <https://covidalert.gov.mt/privacy-policy/>. Acesso em: 30 de janeiro de 2021.

_____. “Frequently Asked Questions”. Disponível em: <https://covidalert.gov.mt/faqs/>. Acesso em: 30 de janeiro de 2021.

CovTracer. (2020). “FAQS”. Disponível em: <https://covid-19.rise.org.cy/en/faqs>. Acesso em 30: de janeiro de 2021.

Diário da República Eletrónico. “Entidades Administrativas Independentes”, *Lexionário*. Disponível em: <https://dre.pt/web/guest/lexionario/-/dj/117357313/view>. Acesso em: 30 de março de 2021.

Direção-Geral das Atividades Económicas. “Organização para a Cooperação e Desenvolvimento Económico”, *República Portuguesa*. Disponível em: <https://www.dgae.gov.pt/servicos/comercio-internacional-e-relacoes-internacionais/multilaterais/organizacao-para-a-cooperacao-e-desenvolvimento-economico-ocde-.aspx>. Acesso em: 15 de março de 2021.

Direção-Geral da Saúde. (2021). “Perguntas Frequentes”. Disponível em: <https://covid19.min-saude.pt/category/perguntas-frequentes/?t=retoma-das-atividades-e-agora#retoma-das-atividades-e-agora>. Acesso em: 12 de janeiro de 2021.

eRouška. (2020). “Termos e Condições”. Disponível em: <https://erouska.cz/podminky-pouzivani>. Acesso em: 30 de janeiro de 2021.

EUR-Lex. (2017). “Convenção Europeia dos Direitos do Homem (CEDH)”. Disponível em: <https://eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=pt>. Acesso em: 24 de abril de 2021.

_____. “Tratado de Roma (CEE)”. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:xy0023>. Acesso em: 23 de abril de 2021.

European Commission. (2016). “EU-U.S. Privacy Shield: Frequently Asked Questions”. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462>. Acesso em: 9 de junho de 2021.

European Data Protection Board. “Our Members”. Disponível em: <https://edpb.europa.eu/about-edpb/about-edpb/members_en>. Acesso em: 31 de março de 2021.

European Data Protection Supervisor. “About”. Disponível em: <https://edps.europa.eu/about-edps_en>. Acesso em: 31 de março de 2021.

E-Tabib. (2020). “Privacy Policy”. Disponível em: <https://www.privacypolicies.com/privacy/view/0cf9245670c0f199f55826d00eb522c9>. Acesso em: 30 de janeiro de 2021.

First Channel. (2020).”STOP COVID App launched in Georgia, enabling users to find out if they were in contact with COVID-infected person”. Disponível em: <https://1tv.ge/en/news/stop-covid-app-launched-in-georgia-enabling-users-to-find-out-if-they-have-been-in-contact-with-a-person-infected-with-covid-19/>. Acesso em: 30 de janeiro de 2021.

Github. (2020). “Immuni’s High” – Level Description”. Disponível em: <https://github.com/immuni-app/immuni-documentation>. Acesso em: 30 de janeiro de 2021.

_____. “Shlonik – شد لوذ ك”. Disponível em: <https://github.com/AmnestyTech/covid19-apps/tree/master/kuwait>. Acesso em: 30 de janeiro de 2021.

_____. “Stop Covid-19 Hrvatska”. Disponível em: <https://github.com/Stop-COVID-19-Croatia/stopcovid19-android>. Acesso em: 30 de janeiro de 2021.

Gouvernment. (2020). “Je me Protége, Je Protége les antres”. Disponível em: <https://www.gouvernement.fr/info-coronavirus/tousanticovid>. Acesso em: 30 de janeiro de 2021.

Government Communications Office. (2021). “Preventive Measures”, *State of Qatar*. Disponível em: <https://www.gco.gov.qa/en/preventative-measures/>. Acesso em: 28 de janeiro de 2021.

Governo da Jordânia. (2020). “About AMAN”. Disponível em: <https://amanapp.jo/en/page/8/AboutAman>. Acesso em: 30 de janeiro de 2021.

_____. “FAQS”. Disponível em: <https://amanapp.jo/en/page/12/FAQs>. Acesso em: 30 de janeiro de 2021.

_____. “Terms of Use”. Disponível em: <https://amanapp.jo/en/page/14/Terms>. Acesso em: 30 de janeiro de 2021.

Governo da Polónia. (2020). “Pytania I Odpowiedzi”. Disponível em: <https://www.gov.pl/web/protegosafe/pytania-i-odpowiedzi>. Acesso em: 30 de janeiro de 2021.

Governo da República do Cazaquistão. (2020). “Политика конфиденциальности и обработки персональных данных мобильного приложения Saqbol”. Disponível em: <https://egov.kz/cms/ru/articles/privacy_Saqbol_mobile_app>. Acesso em: 30 de janeiro de 2021.

Health Service Executive (2020). “Covid Tracker App Terms of Use”. Disponível em: <https://www2.hse.ie/conditions/coronavirus/covid-tracker-app-terms-of-use.html>. Acesso em: 30 de janeiro de 2021.

_____.“Privacy Statement”. Disponível em: <https://covidtracker.gov.ie/privacy-statement/>. Acesso em: 30 de janeiro de 2021.

_____.“Technology the Covid Tracker App Use”. Disponível em: <https://www2.hse.ie/conditions/coronavirus/covid-tracker-app/technology-the-covid-tracker-app-uses.html>. Acesso em: 30 de janeiro de 2021.

Hoia. (2020). “Perguntas e Respostas”. Disponível em: <https://www.hoia.me/>. Acesso em: 30 de janeiro de 2021.

ILoveQatar.net. (2020). “Ehteraz App”. Disponível em: <https://www.iloveqatar.net/coronavirus/guideTips/ehteraz-app-frequently-asked-questions>. Acesso em: 30 de janeiro de 2021.

Instituto Politécnico de Viana do Castelo. (2021). “Aluno do IPCV deteta Bug que afeta Apps de rastreamento covid a nível mundial”. Disponível em: <https://www.ipvc.pt/11447-2/?cli_action=1623665497.503>. Acesso em: 14 de junho de 2021.

ITU Digital World. (2020). “Nepal Covid-19 Surveillance”. Disponível em: <https://digital-world.itu.int/nepal-covid-19-surveillance/>. Acesso em: 30 de janeiro de 2021.

Kim. M.S. (2020). “South Korea is watching quarantined citizens with a smartphone app”. *MIT Technology Review*. Disponível em: <https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine>. Acesso em: 30 de janeiro de 2021.

Koronavilkky. (2020). “Usein Kysyttya”. Disponível em: <https://koronavilkku.fi/ukk/>. Acesso em: 30 de janeiro de 2021.

Magrath, M. (2020). “Principais Requisitos de Conformidade de Segurança e Regulamentos Bancários de 2020”, *OneSpanBlog*. Disponível em: <https://www.onespan.com/pt-br/blog/top-banking-regulations-security-compliance-requirements>. Acesso em: 29 de março de 2021.

Ministère Des Solidarités el de la Santé. (2020). “TousAntiCovid: Respostas às suas perguntas”. Disponível em: <https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/tousanticovid>. Acesso em: 25 de janeiro de 2021.

Ministry of Health. (2020). “’BeAware Bahrain’ App”. Disponível em: <https://healthalert.gov.bh/en/category/beaware-bahrain-app>. Acesso em: 30 de janeiro de 2021.

_____.“Privacy Policy and Information Security”. Disponível em: <https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/>. Acesso em: 30 de janeiro de 2021.

Ministry of Health and Centre for Disease Prevention and Control. (2020). “Frequently Asked Questions”. Disponível em: <https://www.apturicovid.lv/biezak-uzdotie-jautajumi>. Acesso em: 30 de janeiro de 2021.

Ministry of Health, Labour and Welfare. (2020). “新型コロナウイルス接触確認アプリ（COCOA) COVID-19 Contact-Confirming Application”. Disponível em: <https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html>. Acesso em: 30 de janeiro de 2021.

MyHealth. (2020). “MyHealth Sri Lanka Mobile App Privacy Policy”. Disponível em: <https://docs.google.com/document/d/1cp5iMi-V33mLTUk6DMk8gJgELQR1ni_OsbhavpgEpOI/edit>. Acesso em: 30 de janeiro de 2021.

Mysejahtera. (2020). “Mysejahtera App”. Disponível em: <https://mysejahtera.malaysia.gov.my/FAQ_en/>. Acesso em: 30 de janeiro de 201.

_____.“Mysejahtera Privacy Policy”. Disponível em: <https://mysejahtera.malaysia.gov.my/privasi_en/>. Acesso em: 30 de janeiro de 2021.

Noleto, C. (2021). “Código-fonte: o que é e qual sua importância na programação”, *Trybe*. Disponível em: <https://blog.betrybe.com/tecnologia/codigo-fonte/>. Acesso em: 11 de fevereiro de 2021.

Osterreichisches Rotes Krenz. (2021). “Datenschutzinformation Der Stopp Coroma App”. Disponível em: <https://www.roteskreuz.at/datenschutzerklaerung-stopp-corona-app>. Acesso em: 30 de janeiro de 2021.

Parlamento Europeu. “Tratado de Roma (CEE)”. Disponível em: <https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/treaty-of-rome>. Acesso em: 23 de abril de 2021.

_____. “Tratado da União Europeia (TUE)/Tratado de Maastricht”. Disponível em: <https://www.europarl.europa.eu/about-parliament/pt/in-the-past/the-parliament-and-the-treaties/maastricht-treaty>. Acesso em: 23 de abril de 2021.

Programa INCoDe.2030, “INCoDe.2030”. Disponível em: <https://www.incode2030.gov.pt/incode2030>. Acesso em: 16 de janeiro de 2021.

Radar Covid. (2020). “Información Geral”. Disponível em: <https://radarcovid.gob.es/faq-uso-de-la-aplicacion>. Acesso em: 30 de janeiro de 2021.

_____.“Información Geral”. Disponível em: <https://radarcovid.gob.es/faq-informacion-general>. Acesso em: 30 de janeiro de 2021.

Republic of Lebanon, Ministry of Public Health. (2021). «“Ma3an” Together Against Corona». Disponível em: <https://moph.gov.lb/en/ma3an>. Acesso em: 30 de janeiro de 2021.

Robert Koch Institut. (2020). “Wie funktioniert die Corona-Datenspende?”, Corona-Datenspende. Disponível em: <https://corona-datenspende.de/science/reports/how/>. Acesso em: 25 de janeiro de 2021.

Saw Saw Shar. (2020). “Privacy Policy”. Disponível em: <https://www.sawsawshar.gov.mm/privacypolicy.html>. Acesso em: 30 de janeiro de 2021.

Singapore Government Agency. (2020). “How does the app TraceTogether App work?”. Disponível em: <https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473-How-does-the-TraceTogether-App-work->. Acesso em: 30 de janeiro de 2021.

_____.“TraceTogether – Terms of Use”. Disponível em: <https://www.tracetogether.gov.sg/common/terms-of-use/index.html>. Acesso em: 30 de janeiro de 2021.

_____.“Who built TraTogether?”. Disponível em <https://support.tracetogether.gov.sg/hc/en-sg/articles/360043504753-Who-built-TraceTogether->. Acesso em: 30 de janeiro de 2021.

StayAway Covid. (2020). “Política de Privacidade”. Disponível em: <https://stayawaycovid.pt/politica-de-privacidade/>. Acesso em: 16 de janeiro de 2021.

_____.“Termos de Utilização”. Disponível em: <https://stayawaycovid.pt/termos-condicoes/>. Acesso em: 30 de janeiro de 2021.

Stay Safe.Ph. (2020). “Privacy Notice”. Disponível em: <https://www.staysafe.ph/data-privacy>. Acesso em: 30 de janeiro de 2021.

_____. “Data Privacy”. Disponível em: <https://www.staysafe.ph/data-privacy>. Acesso em: 25 de janeiro de 2021.

Serviço Nacional de Saúde. (2021). “Estudo Saúde Mental em Tempos de Pandemia (SM-COVID19): principais resultados”. Disponível em: <http://www.insa.min-saude.pt/estudo-saude-mental-em-tempos-de-pandemia-sm-covid19-principais-resultados/>. Acesso em: 27 de abril de 2021.

_____. “MERS-CoV”. Disponível em: <https://www.dgs.pt/paginas-de-sistema/saude-de-a-a-z/coronavirus/mers-cov.aspx>. Acesso em: 20 de junho de 2021.

Smittestop. (2020). “Frequently Asked Questions and answers about the app”. Disponível em: <https://smittestop.dk/en/q-and-a/>. Acesso em: 30 de janeiro de 2021.

Strategic Business Group. (2020). “Privacy Policy”. Disponível em: <https://sbg.la/about-us/privacy-policy/>. Acesso em: 30 de janeiro de 2021.

Tabaud. (2020). “Privacy Policy”. Disponível em: <https://tabaud.sdaia.gov.sa/PrivacyEn>. Acesso em: 30 de janeiro de 2021.

_____. “Terms Conditions”. Disponível em: <https://tabaud.sdaia.gov.sa/TCEN>. Acesso em: 30 de janeiro de 2021.

TraceEkee. (2020). “TraceEkee Privacy Statement”. Disponível em: <https://trace.hpa.gov.mv/privacy.html?lang=en>. Acesso em: 30 de janeiro de 2021.

TraceTogether. (2020). “TraceTogetherToken”. Disponível em: <https://www.tracetogether.gov.sg/common/token/index.html>. Acesso em: 27 de janeiro de 2021.

Unicef. “O que são direitos humanos? Os direitos humanos pertencem a todos e a todas e a cada um de nós igualmente”. Disponível em: <https://www.unicef.org/brazil/o-que-sao-direitos-humanos>. Acesso em: 17 de maio de 2021.

VirusRadar. (2020). “Adatkezelèsi Tájékoztató”. Disponível em: <https://virusradar.hu/privacy-policy>. Acesso em: 30 de janeiro de 2021.

_____. “Ki fejlesztette a VírusRadart?”. Disponível em: <https://virusradar.hu/>. Acesso em: 30 de janeiro de 2021.

VirusSafe. (2020). “Termos e condições”. Disponível em: <https://virusafe.io/information/terms-of-use.html>. Acesso em: 27 de janeiro de 2021.

Doutrina e Jurisprudência:

Acórdão n.º 464/2019, de 21 de outubro. *Diário da República n.º202/19 -1ª Série*. Tribunal Constitucional. Lisboa.

Publicações de um Organismo Coletivo:

Agência Europeia dos Direitos Fundamentais, Conselho da Europa, Tribunal Europeu dos Direitos do Homem. (2014). Manual da legislação europeia sobre proteção de dados. Serviço das Publicações da União Europeia. Luxemburgo.

Apple e Google. (2020). Exposure Notifications, Frequently Asked Questions. Preliminary – Subject to Modification and Extension. Estados Unidos da América.

Comissão Europeia. (2017). Comunicação da Comissão ao Parlamento Europeu e ao Conselho: Intercâmbio e Proteção de dados pessoais. Bruxelas.

_____. (2019). Comunicação da Comissão ao Parlamento Europeu e ao Conselho: As regras de proteção de dados como instrumento gerador de confiança dentro e fora da UE – ponto de situação. Bruxelas.

_____. (2020). Orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID-19 na perspetiva da proteção de dados. Jornal Oficial da União Europeia. Bruxelas.

Comunidade de Imprensa n.º 91/20. Acórdão no processo C-311/18, Data Protection Commissioner/Maximillian Schrems e Facebook Ireland. Tribunal de Justiça da União Europeia. Luxemburgo.

Corona-Warn-App. (2020). Terms of use. Alemanha.

CovTracer. (2020). CovTracer Privacy Policy. Chipre.

Data Protection Working Party. (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Bruxelas.

DLA Piper. (2021). Data Protection Laws of the World, Saudi Arabia. Mohamed Moussallati. Arábia Saudita.

eHealth. (2020). Interoperability guidelines for approved contact tracing mobile applications in the EU. Bruxelas.

_____. Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member Stares. Bruxelas.

European Commission. (2020). Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection. Communication from the commission. Bruxelas.

Gillmor, D.K. (2020). Principles for Technology-Assisted Constact-Tracing. ACLU. Estados Unidos da América.

Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human right. (2020).

Korona Stop LT. (2020). Política de Privacidade. Lituânia.

Latham & Watkins LLP. Data Protection in the Kingdom of Saudi Arabia: a Primer. Middle East & Africa Technology, IP and Sourcing Focus. Noor Al-Fawzan e Omar Elsayed. Arábia Saudita.

Liang. F. (2020). Covid-19 and Health Code: How Digital Plataforms Tackle the Pandemic in China. Michigan.

Maharjan, R.M., Koirala, S., Maharjan, R e Scherchand, J. (2020). Analysif of online medical services availability during Covid-19 pandemic in Nepal. *Tribhuvan University Journal*.

Ministry of Electronics & IT. (2020). MEITY issues Clarification regarding orders passed by Central Information Commission on an RTI query with regard to AsrogyaSety App. India.

Norton Rose Fulbright. (2020). Contact Tracing apps in Indonesia: A new world for data privacy. Estados Unidos da América.

_____. Contact Tracing apps in Turkey: A new world for data privacy. Estados Unidos da América.

Organização Mundial de Saúde. (2014). Contact tracing during an outbreak of Ebola virus disease. Disease Surveillance and Response Programme Area Disease Prevention and Control Cluster. Genebra.

_____. (2020). Digital tools for COVID-19 contact tracing. Annex: Contact tracing in the context of COVID-19. Genebra.

_____. (2020). Ethical considerations to guide the use of digital proximity tracking tecnhologies for COVID-19 contact tracing. Interim guidance. Genebra.

Osterreichisches Rotes Krenz. (2020). *Bericht über die Datenschutz-Folgenabschätzung für die Anwendung* Áustria.

Sundheds-Oh Aeldreministeriet. (2020). Aftale om frivilling smittesporingsapp for Covid-19. Dinamarca.

World Business Council for Sustainable Development. (2020). As consequências da Covid-19 para a próxima década. Nota Informativa da Visão 2050. Portugal.

#Ostanizdrav App. (2020). Privacy Notice. Eslovénia.

Revistas Científicas:

Arnaldo GONÇALVES, «Os valores asiáticos e os direitos humanos», *Política Internacional*, 27 (2005). p. 141 – 161.

Danilo DONEDA, «A proteção dos dados pessoais como um direito fundamental», *Espaço Jurídico Journal of Law [EJJL]*, 12 (2011). p. 91-108.

Eugênio Facchini NETO, «A Noção de Privacy na Jurisprudência da Suprema Corte Norte-Americana: existe um conceito unificador?» *Revista de Direito Brasileira*, 10 (2020). P 414-440.

Graham GREENLEAF, «Global data privacy 2015: 109 countries, with European laws now a minotiry», *133 Privacy Laws & Business International Report*, 21 (2015), p. 18-28.

Leonardo Estevam de Assis ZANINI, «O Surgimento e o Desenvolvimento do Right of Privacy nos Estados Unidos», *RJLB*, 4 (2015), p.791-817.

Maria Cristina FERREIRA, Eveline Maria Leal ASSMAR e Solange de Oliveira SOUTO, «O individualismo e o coletivismo como indicadores de culturas nacionais: convergências e divergências teórico-metodológicas», *Psicologia em Estudo*, 1 (2002). p.81-89.

Pedro Cruz VILLALON, «Formación y Evolución de los Derechos Fundamentales», *Revista de Derecho Constitucional*, 25 (1989), p. 35-62.

Alexandre Sousa PINHEIRO e Carolina MOURA, «Utilização de tecnologia de geolocalização e o tratamento de dados pessoais no regime jurídico português: a propósito da Deliberação n.º7680/2014 da Comissão Nacional de Proteção de Dados e jurisprudência posterior», *Fórum de Proteção de Dados*, 3 (2016). p.15-31.

Fernanda dos Santos MACEDO, Michelle Dias BUBLITZ, Regina Liden RUARO, «A Privacy Norte-Americana e a Relação com o Direito Brasileiro», *Revista Jurídica Cesumar-Mestrado*, 1 (2013), p. 161-178.

Francisco Fernández SEGADO, «El régimen jurídico del tratamiento autorizado de los datos de carácter personal en España», *Derecho PUPC*, 51 (1997). p. 7-48.

Maria Clara SOTTOMAYOR, «Uma análise crítica do Acórdão do Tribunal Constitucional n.º 464/2019: o sistema de acesso a metadados ou a segurança versus liberdade. *Julgar*. (2020). Disponível em: <http://julgar.pt/uma-analise-critica-do-acordao-do-tribunal-constitucional-n-o-4642019-o-sistema-de-acesso-a-metadados-ou-a-seguranca-versus-liberdade/>. Acesso em: 15 de junho de 2021.

Samuel WARREN e Louis BRANDEIS, «The Right to Privacy», *Harvard Law Review*, 5 (1890). Disponível em: <https://www.jstor.org/stable/1321160?seq=2#metadata_info_tab_contents>. Acesso em 09 de julho de 2021.

Teses de Mestrado:

Gomes Machado, M. (2019). O acesso aos metadados pelos serviços de informações da República Portuguesa, à luz da lei e da constituição. *Tese de Mestrado em Direito e Segurança* – Faculdade de Direito da Universidade de Lisboa. Lisboa.

ANEXOS

Tabela n.º1 – Aplicações Móveis Europeias

Aplicação Móvel:	**Voluntário/ Obrigatório**	**Entidade Responsável:**	**Tecnologia:**
Corona-Warn-App (Alemanha)	Voluntário[208]	Instituto Robert Koch, Instituto Nacional de Saúde Pública[209]	BLE[210]
Stopp Corona (Áustria)	Voluntário[211]	Cruz Vermelha Austríaca[212]	BLE[213]
Corona Alert (Bélgica)	Voluntário[214]	Sciensano, Instituto Nacional de Saúde Pública[215]	BLE[216]
ViruSafe (Bulgária)	Voluntário[217]	Ministério da Bulgária[218]	Geolocalização[219]
eRouška – Part of Smart Quarentine (República Checa)	Voluntário[220]	Ministério da Saúde da República Checa e Agência Nacional de Tecnologia de Informação e Comunicação[221]	BLE[222]

[208] Corona-Warn-App. (2020). *Terms of use*. Alemanha. p.5.
[209] *Ibid.* p.1.
[210] *Ibid.* p.2.
[211] Osterreichisches Rotes Krenz. (2020). *Bericht über die Datenschutz-Folgenabschätzung für die Anwendung* Áustria. p.40.
[212] Osterreichisches Rotes Krenz. (2021). *Datenschutzinformation Der Stopp Coroma App*. Acedido em 30 de janeiro de 2021, em: https://www.roteskreuz.at/datenschutzerklaerung-stopp-corona-app.
[213] *Ibid.*
[214] Cf. Art14º, §1 Real Decreto nº44 de 26 de junho de 2020. *Revista do Estado Belga* – Ed.2. Monitor Belge. Ministério dos Assunto Sociais e Saúde Pública.
[215] *Ibid.* p. 48433.
[216] *Ibid.* p.48432.
[217]Virusafe. (2020.) *Termos e Condições*. Acedido em 30 de janeiro de 2021, em: https://virusafe.io/information/terms-of-use.html.
[218] *Ibid.*
[219] *Ibid.*
[220] eRouška. (2020). *Termos e Condições.* Acedido em 30 de janeiro de 2021, em: https://erouska.cz/podminky-pouzivani.
[221] *Ibid.*
[222] *Ibid.*

CovTracer (Chipre)	Voluntário[223]	Centro de Excelência em Pesquisa e Inovação RISE – Centro de Pesquisa em Média Interativa, Sistemas Inteligentes e Tecnologias[224]	Geolocalização[225]
Stop Covid-19 (Croácia)	Voluntário[226]	Ministério da Saúde da República da Croácia[227]	BLE[228]
Smittestop (Dinamarca)	Voluntário[229]	Ministério da Saúde, Autoridade Dinamarquesa do Paciente, Statens Serum Instut, Autoridade de Saúde Dinamarquesa e Agência Dinamarquesa para a Digitalização[230]	BLE[231]
(Eslováquia)	---	---	---
#Ostanizdrav (Eslovénia)	Voluntário[232]	Instituto Nacional de Saúde Pública e Ministério da Administração Pública[233]	BLE[234]
Radar Covid (Espanha)	Voluntário[235]	Secretaria de Estado da Digitalização e Inteligência Artificial do Ministério dos Assuntos Económicos e Transformação Digital[236]	BLE[237]

[223] CovTracer. (2020). *FAQS*. Acedido em 30 de janeiro de 2021, em: https://covid-19.rise.org.cy/en/faqs.
[224] CovTracer. (2020). *CovTracer Privacy Policy.* Chipre. p.7.
[225] *Ibid.* p.3-4.
[226] Github. (2020). *Stop Covid-19 Hrvatska.* Acedido em 30 de janeiro de 2021, em: https://github.com/Stop-COVID-19-Croatia/stopcovid19-android.
[227] *Ibid.*
[228] *Ibid.*
[229] Sundheds-Og Aeldreministeriet. (2020). *Aftale om frivillig smittesporingsapp for COVID-19*. Dinamarca. p.2.
[230] Smittestop. (2020). *Frequently Asked Questions and answers about the app.* Acedido em 30 de janeiro de 2021, em: https://smittestop.dk/en/q-and-a/.
[231] Cf. Kapitel 2**,** § 3, 1). BEK nº1539 de 29 de outubro. *Sundhedsog*. Ministério da Saúde e do Idoso.
[232] #Ostanizdrav App. (2020). *Privacy notice.* Eslovénia. p.1.
[233] *Ibid.* p.1.
[234] *Ibid.* p.4.
[235] Radar Covid. (2020). *Información Geral*. Acedido em 30 de janeiro de 2021, em: https://radarcovid.gob.es/faq-uso-de-la-aplicacion.
[236] Radar Covid. (2020). *Información Geral*. Acedido em 30 de janeiro de 2021, em: https://radarcovid.gob.es/faq-informacion-general.
[237] Cf. Séptimo. Resolución de 13 de octubre de 2020. *BOE Legislación Consolidada.* Ministério da Economia e Transformação Digital e Ministério da Saúde. Espanha.

Hoia (Estónia)	Voluntário[238]	Ministério dos Assuntos Sociais, Centro de Sistemas de Informação de Saúde e Bem-Estar, Conselho de Saúde, Cybernetica, Fujitsu Estónia, Guardtime, Icefire, Iglu, Mobi Lab, Mooncascade, Velvet, Soluções FOB, Heisi IT OU, Byetelofics e Asa Quality Services[239]	BLE[240]
Koronavilkku (Finlândia)	Voluntário[241]	Instituto Finlandês de Saúde e Bem-Estar, Ministério dos Assuntos Sociais e Saúde, Kela, SoteDigi Oy e Solita Oy[242]	BLE[243]
TousAnti Covid (França)	Voluntário[244]	Inria, ANSSI, Orange, Dassault, Ministério da Saúde e Ministério de Estado dos Assuntos Digitais[245]	BLE[246]
(Grécia)	---	---	---
Virus Radar (Hungria)	Voluntário[247]	KIFU, Biztributor, Nextsense e doado ao Estado Húngaro[248]	BLE[249]

[238] Hoia. (2020). *Perguntas e Respostas.* Acedido em 30 de janeiro de 2021: https://www.hoia.me/.
[239] *Ibid.*
[240] *Ibid*.
[241] Koronavilkky. (2020). *Usein Kysyttya*. Acedido em 30 de janeiro de 2021, em: https://koronavilkku.fi/ukk/.
[242] *Ibid*.
[243] *Ibid*.
[244] Gouvernment. (2020). *Je me Protége, Je Protége les antres.* Acedido em 30 de janeiro de 2021, em: https://www.gouvernement.fr/info-coronavirus/tousanticovid.
[245] *Ibid*.
[246] *Ibid*.
[247] VirusRadar. (2020). *Adatkezelèsi Tájékoztató.* Acedido em 30 de janeiro de 2021, em: https://virusradar.hu/privacy-policy.
[248] VirusRadar. (2020). "*Ki fejlesztette a* ***VírusRadar****t?".* Acedido em 30 de janeiro de 2021, em: https://virusradar.hu/.
[249] VirusRadar. Ob. Cit.

Covid Tracker (Irlanda)	Voluntário[250]	Serviço Executivo de Saúde[251]	BLE[252]
Immuni (Itália)	Voluntário[253]	Comissário Extraordinário para a Emergência COVID-19, Ministério da Saúde e o Ministério da Inovação, Tecnologia e Digitalização[254]	BLE[255]
Apturi Covid Latvia (Letónia)	Voluntário[256]	LMT, MakIT, Autentica, TestDevLab, Centro IT, Zippy Vision, Universidade da Letónia, cofundador do TechHub, Andris K. Berzins, Chancelaria do Presidente da Letónia, NATO StratCom e profissionais de saúde[257]	BLE[258]
Korona Stop LT (Lituânia)	Voluntário[259]	Ministério da Saúde da República da Lituânia e Centro Nacional de Saúde Pública[260]	BLE[261]
Corona-Warn App (Luxemburgo)	---	---	---

[250] Health Service Executive (2020). *Covid Tracker App Terms of Use.* Acedido em 30 de janeiro de 2021, em: https://www2.hse.ie/conditions/coronavirus/covid-tracker-app-terms-of-use.html.
[251] Health Service Executive. (2020). *Privacy Statement*. Acedido em 30 de janeiro de 2021, em: https://covidtracker.gov.ie/privacy-statement/.
[252] Health Service Executive. (2020). *Technology the Covid Tracker App Use*. Acedido em 30 de janeiro de 2021, em: https://www2.hse.ie/conditions/coronavirus/covid-tracker-app/technology-the-covid-tracker-app-uses.html.
[253] Github. (2020). *Immuni's High – Level Description.* Acedido em 30 de janeiro de 2021, em: https://github.com/immuni-app/immuni-documentation.
[254] *Ibid*.
[255] *Ibid*.
[256] Ministry of Health and Centre for Disease Prevention and Control. (2020). *Frequently Asked Questions.* Acedido em 30 de janeiro de 2021, em: https://www.apturicovid.lv/biezak-uzdotie-jautajumi.
[257] *Ibid*.
[258] *Ibid*.
[259] Korona Stop LT. (2020). *Política de Privacidade.* Lituânia. p.2.
[260] *Ibid*. p.2.
[261] *Ibid*. p.6.

Covid Alert Malta (Malta)	Voluntário[262]	Agência de Tecnologia da Informação, Ministério da Saúde e Autoridade de Inovação Digital de Malta [263]	BLE[264]
Corona Melder (Países Baixos)	Voluntário[265]	Ministério da Saúde Pública, Bem-Estar e Desporto em parceria com o Instituto Nacional de Saúde Pública e Meio Ambiente e os Serviços Municipais de Saúde[266]	BLE[267]
ProteGo App (Polónia)	Voluntário[268]	Coligação de empresas polonesas de TI a pedido do Ministério da Digitalização[269]	BLE[270]
Stayaway Covid (Portugal)	Voluntário[271]	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC), Instituto de Saúde Pública da Universidade do Porto (ISPUP), Empresas Keyruptive e Ubirider[272]	BLE[273]
(Roménia)	---	---	---
(Suécia)	---	---	---

[262] Covid Alert. (2020). *Privacy Policy-Covid Alert Malta.* Acedido em 30 de janeiro de 2021, em: https://covidalert.gov.mt/privacy-policy/.
[263] Covid Alert. (2020). *Frequently Asked Questions.* Acedido em 30 de janeiro de 2021, em: https://covidalert.gov.mt/faqs/.
[264] *Ibid*.
[265] Corona Melder. (2020). *Corona Melder Privacy Statement*. Acedido em 30 de janeiro de 2021, em: https://coronamelder.nl/en/privacy.
[266] *Ibid*.
[267] *Ibid*.
[268] Governo da Polónia. (2020). *Pytania I Odpowiedzi*. Acedido em 30 de janeiro de 2021, em: https://www.gov.pl/web/protegosafe/pytania-i-odpowiedzi.
[269] *Ibid*.
[270] *Ibid*.
[271] StayAwayCovid. (2020). *Termos de Utilização*. Acedido em 30 de janeiro de 2021, em: https://stayawaycovid.pt/termos-condicoes/.
[272] *Ibid*.
[273] *Ibid*.

Tabela n.º2 – Aplicações Móveis Asiáticas

Aplicação Móvel:	**Voluntário/ Obrigatório**	**Entidade Responsável:**	**Tecnologia:**
(Afeganistão)	---	---	---
Tabaud (Arábia Saudita)	Voluntário[274]	Autoridade Saudita de Dados e Inteligência Artificial[275]	BLE[276]
(Arménia)	---	---	---
e-Tabib (Azerbeijão)	---	---	Geolocalização [277]
BeAware Baharin (Barém)	---	Autoridade de Informação e eGovernment do Reino do Barém[278]	Geolocalização [279]
Corona Tracer BD (Bangladesh)	---	Shohoj[280]	BLE/ Geolocalização [281]
BruHealth (Brunei)	---	Governo do Brunei[282]	BLE/ Geolocalização [283]
(Butão)	---	---	---
(Camboja)	---	---	---

[274] Tabaud. (2020). *Terms Conditions.* Acedido em 30 de janeiro de 2021, em: https://tabaud.sdaia.gov.sa/TCEN.
[275] Tabaud. (2020). *Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://tabaud.sdaia.gov.sa/PrivacyEn.
[276] *Ibid.*
[277] E-Tabib. (2020). *Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://www.privacypolicies.com/privacy/view/0cf9245670c0f199f55826d00eb522c9.
[278] Ministry of Health. (2020). *'BeAware Bahrain' App*. Acedido em 30 de janeiro de 2021, em: https://healthalert.gov.bh/en/category/beaware-bahrain-app.
[279] *Ibid.*
[280] Corona Tracer BD. (2020). *Terms of Service.* Acedido em 30 de janeiro de 2021, em: https://tracercdn.shohoz.com/privacy_policy/index.html.
[281] *Ibid.*
[282] BruHealth. (2020). *Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://www.healthapp.gov.bn/covid19/bruhealth/privacy_policy.html.
[283] *Ibid.*

Saqbol (Cazaquistão)	Voluntário[284]	Nacional Information Technologies JSC[285]	BLE[286]
AliPay Health Code (China)	Obrigatório [287]	Ant Financial and Alipay - Alibaba[288]	Geolocalização [289]
(Coreia do Norte)	---	---	---
자가격리자안전보호 *(Self-Quarantine Safety Protection*) (Coreia do Sul)	---	Ministério do Interior e Segurança[290]	BLE/ Geolocalização [291]
(Egipto)	---	---	---
(Emirados Árabes Unidos)	---	---	---
StaySafePH (Filipinas)	---	Interagency Task Force on Emerging Infectious Diseases and National Task Force Against Covid-19[292]	BLE[293]
Stop Covid (Geórgia)	---	Companhia Austríaca, iniciativa Ministério da Saúde da Geórgia[294]	BLE/ Geolocalização [295]

[284] Governo da República do Cazaquistão. (2020). *Политика конфиденциальности и обработки персональных данных мобильного приложения Saqbol.* Acedido em 30 de janeiro de 2021, em: https://egov.kz/cms/ru/articles/privacy_Saqbol_mobile_app.
[285] *Ibid.*
[286] *Ibid.*
[287] Liang. F. (2020). *Covid-19 and Health Code: How Digital Plataforms Tackle the Pandemic in China*. Michigan. p.2.
[288] *Ibid*. p.1.
[289] *Ibid*. p.2.
[290] Kim. M.S. (2020, 6 de março). South Korea is watching quarantined citizens with a smartphone app. *MIT Technology Review.* Acedido a 30 de janeiro de 2021, em: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine.
[291] *Ibid*.
[292] Stay Safe.Ph. (2020). *Privacy Notice*. Acedido em 30 de janeiro de 2021, em: https://www.staysafe.ph/data-privacy.
[293] *Ibid.*
[294] First Channel. (2020, 16 de abril). STOP COVID App launched in Georgia, enabling users to find out if they were in contact with COVID-infected person. *First Channel*. Acedido a 30 de janeiro de 2021, em: https://1tv.ge/en/news/stop-covid-app-launched-in-georgia-enabling-users-to-find-out-if-they-have-been-in-contact-with-a-person-infected-with-covid-19/.
[295] *Ibid*.

(Iémen)	---	---	---
Aarogya Setu (India)	---	Governo da Índia[296]	BLE/ Geolocalização [297]
Pedulilindungi (Indonésia)	Voluntário[298]	Ministério da Informação e Comunicação[299]	BLE/ Geolocalização [300]
(Irão)	---	---	---
(Iraque)	---	---	---
HaMagen (Israel)	---	Ministro da Saúde, companhias comerciais e voluntários de organizações[301]	BLE/ Geolocalização [302]
Cocoa-covid-19 Contact App (Japão)	Voluntário[303]	Ministério da Saúde, Trabalho e Bem-Estar[304]	BLE[305]
AMAN APP (Jordânia)	Voluntário[306]	Ministério da Saúde da Jordânia e grupo de voluntários[307]	Geolocalização [308]

[296] Ministry of Electronics & IT. (2020). *MEITY issues Clarification regarding orders passed by Central Information Commission on an RTI query with regard to AsrogyaSety App*. India. p.1.
[297] *Ibid*. p.2-3.
[298] Norton Rose Fulbright. (2020). *Contact Tracing apps in Indonesia: A new world for data privacy*. Estados Unidos da América. p.1.
[299] *Ibid*. p.1.
[300] *Ibid*. p.1.
[301] Ministry of Health. (2020). *Privacy Policy and Information Security*. Acedido em 30 de janeiro de 2021, em: https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/.
[302] *Ibid*.
[303] Ministry of Health, Labour and Welfare. (2020). 新型コロナウイルス接触確認アプリ（*COCOA) COVID-19 Contact-Confirming Application*. Acedido em 30 de janeiro de 2021, em: https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html.
[304] *Ibid*.
[305] *Ibid*.
[306] Governo da Jordânia. (2020). *FAQS*. Acedido em 30 de janeiro de 2021, em: https://amanapp.jo/en/page/12/FAQs.
[307] Governo da Jordânia. (2020). *About AMAN*. Acedido em 30 de janeiro de 2021, em: https://amanapp.jo/en/page/8/AboutAman.
[308] Governo da Jordânia. (2020). *Terms of Use.* Acedido em 30 de janeiro de 2021, em: https://amanapp.jo/en/page/14/Terms.

ش لون ك *(How are you?)* (Kuwait)	---	Ministério da Saúde, Agência Central de Tecnologia da Informação do Kuwait e Zain[309]	BLE/ Geolocalização [310]
Lao Kyc (Laos)	Voluntário[311]	Ministério dos Correios e Telecomunicações, Lao PDR e SB Lab 856 Co., Ltd.[312]	Geolocalização [313]
Ma3an – Together Against Corona (Líbano)	Voluntário[314]	Ministério da Saúde Pública, equipa de especialistas da Universidade Americana de Beirute e TedMob[315]	BLE[316]
Mysejahtera (Malásia)	---	Conselho de Segurança Nacional, Ministério da Saúde, Unidade de Modernização Administrativa e Planeamento de Gestão, Comissão de Comunicações e Multimédia da Malásia e Ministério da Ciência e Tecnologia e Inovação[317]	Geolocalização [318]
TraceEkee (Maldivas)	Voluntário[319]	Agência de Proteção à Saúde[320]	BLE[321]

[309] Github. (2020). *Shlonik* – شلونك. Acedido em 30 de janeiro de 2021, em: https://github.com/AmnestyTech/covid19-apps/tree/master/kuwait.
[310] *Ibid*.
[311] Strategic Business Group. (2020). *Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://sbg.la/about-us/privacy-policy/.
[312] *Ibid*.
[313] *Ibid*.
[314] Republic of Lebanon, Ministry of Public Health. (2021). *"Ma3an" Together Against Corona.* Acedido em 30 de janeiro de 2021, em: https://moph.gov.lb/en/ma3an.
[315] *Ibid*.
[316] *Ibid*.
[317] Mysejahtera. (2020). *Mysejahtera App*. Acedido em 30 de janeiro de 2021, em: https://mysejahtera.malaysia.gov.my/FAQ_en/.
[318] Mysejahtera. (2020). *Mysejahtera Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://mysejahtera.malaysia.gov.my/privasi_en/.
[319] TraceEkee. (2020). *TraceEkee Privacy Statement*. Acedido em 30 de janeiro de 2021, em: https://trace.hpa.gov.mv/privacy.html?lang=en.
[320] *Ibid*.
[321] *Ibid*.

Saw Saw Shar (Mianmar)	---	Federação de Computadores de Mianmar[322]	---
Shuurkhai 119 (Mongólia)	---	---	---
Nepal Covid-19 Surveillance (Nepal)	---	Rede de Pesquisa e Educação do Nepal e parceiros de tecnologia, medicina e desenvolvimento[323]	BLE/ Geolocalização [324]
Tarassud+ (Omã)	---	---	---
Covid-19 Gov PK (Paquistão)	---	---	---
EHTERAZ (Qatar)	Obrigatório [325]	Ministérios do Estado do Qatar[326]	BLE/ Geolocalização [327]
Stopcoronavirus. MyContacts (Rússia)	Voluntário[328]	Ministério do Desenvolvimento Digital, Comunicações e Média de Massa e Moscow City Hall[329]	BLE[330]

[322] Saw Saw Shar. (2020). *Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://www.sawsawshar.gov.mm/privacypolicy.html.
[323] ITU Digital World. (2020). *Nepal Covid-19 Surveillance*. Acedido em 30 de janeiro de 2021, em: https://digital-world.itu.int/nepal-covid-19-surveillance/.
[324] Maharjan, R.M., Koirala, S., Maharjan, R e Scherchand, J. (2020, setembro). Analysif of online medical services availability during Covid-19 pandemic in Nepal. *Tribhuvan University Journal*. p.66.
[325] ILoveQatar.net. (2020). *Ehteraz App*. Acedido em 30 de janeiro de 2021, em: https://www.iloveqatar.net/coronavirus/guideTips/ehteraz-app-frequently-asked-questions.
[326] *Ibid*.
[327] *Ibid*.
[328] The Moscow Times, Independent News From Russia. (2020). Russia Develops Coronavirus Contact-Tracing App. [Versão eletrónica]. *The Moscow Times*. Acedido a 30 de janeiro de 2021, em: https://www.themoscowtimes.com/2020/11/17/russia-develops-coronavirus-contact-tracing-app-a72068.
[329] *Ibid*.
[330] *Ibid*.

TraceTogether (Singapura)	Voluntário[331]	Ministério da Saúde e Agência da Tecnologia do Governo em apoio à SGUnited[332]	BLE[333]
(Síria)	---	---	---
My Health Sri Lanka (Sri Lanka)	---	Agência de Tecnologia da Informação e Comunicação do Sri Lanka e Ministério da Saúde[334]	---
(Tajiquistão)	---	---	---
MorChana (Tailândia)	---	---	---
(Timor-Leste)	---	---	---
(Turquemenistão)	---	---	---
Hayat Eve Sigar (Turquia)	Obrigatório [335]	Autoridade de Tecnologias de Informação e Comunicação e operadoras de telecomunicações turcas[336]	BLE[337]
(Uzbequistão)	---	---	---

[331] Singapore Government Agency. (2020). *TraceTogether – Terms of Use*. Acedido em 30 de janeiro de 2021, em: https://www.tracetogether.gov.sg/common/terms-of-use/index.html.
[332] Singapore Government Agency. (2020). *Who built TraTogether?*. Acedido em 30 de janeiro de 2021, em: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043504753-Who-built-TraceTogether-.
[333] Singapore Government Agency. (2020). *How does the app TraceTogether App work?*. Acedido em 30 de janeiro de 2021, em: https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473-How-does-the-TraceTogether-App-work-.
[334] MyHealth. (2020). *MyHealth Sri Lanka Mobile App Privacy Policy*. Acedido em 30 de janeiro de 2021, em: https://docs.google.com/document/d/1cp5iMi-V33mLTUk6DMk8gJgELQR1ni_OsbhavpgEpOI/edit.
[335] Norton Rose Fulbright. (2020). *Contact Tracing apps in Turkey: A new world for data privacy*. Estados Unidos da América. p.1.
[336] *Ibid*. p.1.
[337] *Ibid*. p.2.