Os impactos do coronavírus no cumprimento do Regulamento Geral de Proteção de Dados da União Européia(*)

The impacts of coronavirus on compliance with the General Data Protection Regulations of the European Union

Los impactos del coronavirus en el cumplimiento de las Normas Generales de Protección de Datos de la Unión Europea

Milena Loyola Conci[1]

Marcelo Fernando Quiroga Obregón[2]

Sumário: Introdução.**1**. Regulamento Geral de Proteção de Dados da União Européia. **2**. A Crise do Coronavírus.**3**. Os impactos do coronavírus: limitações ao cumprimento da RGPD. – Considerações finais – Referências.

Resumo: O presente artigo busca mostrar a necessidade de se harmonizar a atual pandemia provocada pelo novo coronavírus com o cumprimento das normas previstas no Regulamento Geral de Proteção de Dados pessoais 2016/679 (UE). Utilizou-se como base teórica as recomendações da Organização Mundial da Saúde, bem como de orientações e relatórios expedidos pelas Autoridades de Proteção de Dados Pessoais em Portugal, Espanha e Itália. Para tanto, foram feitas breves considerações acerca do Regulamento Geral de Proteção de Dados pessoais 2016/679 (UE) e os

(*) Recibido: 05/06/2020 | Aceptado: 01/08/2020 | Publicación en línea: 01/10/2020.

1 Acadêmica de Direito da Faculdade de Direito de Vitória – FDV.
milena.conci@gmail.com

2 Doutor em Direitos e Garantias Fundamentais na Faculdade de Direito de Vitória -FDV, Mestre em Direito Internacional e Comunitário pela Pontifícia Universidade Católica de Minas Gerais, Especialista em Política Internacional pela Fundação Escola de Sociologia e Política de São Paulo, Graduado em Direito pela Universidade Federal do Espírito Santo, Coordenador Acadêmico do curso de especialização em Direito Marítimo e Portuário da Faculdade de Direito de Vitória -FDV -, Professor de Direito Internacional e Direito Marítimo e Portuário nos cursos de graduação e pós-graduação da Faculdade de Direito de Vitória -FDV.
mfqobregon@yahoo.com.br

desafios tecnológicos junto ao princípio da proporcionalidade. Após, foi exposta a atual situação da pandemia do novo coronavírus, com a atuação marcante da Organização Mundial da Saúde. Por fim, foi analisado como a pandemia está impactando no cumprimento do Regulamento, notadamente em três países, Portugal, Espanha e Itália, e como estes estão lidando com o surgimento de novos aplicativos de rastreio e notificação de casos.

Palavras-chave: Regulamento Geral de Proteção de Dados, novo coronavírus, impactos ao cumprimento do Regulamento, aplicativos de rastreio de casos.

Abstract: This article seeks to show the need to harmonize the current pandemic caused by the new coronavirus with compliance with the standards set out in the General Regulation on Personal Data Protection 2016/679 (EU). The recommendations of the World Health Organization, as well as guidelines and reports issued by the Personal Data Protection Authorities in Portugal, Spain and Italy were used as a theoretical basis. To this end, brief considerations were made about the General Regulation on Personal Data Protection 2016/679 (EU) and the technological challenges along with the principle of proportionality. The current situation of the new coronavirus pandemic was then exposed, with the World Health Organization's landmark action. Finally, it was analyzed how the pandemic is impacting on compliance with the Regulation, notably in three countries, Portugal, Spain and Italy, and how these are dealing with the emergence of new applications for screening and notification of cases.

Keywords: General Regulation of Data Protection, new coronavirus, impacts on compliance with the regulation, case tracking applications.

Resumen: Este artículo pretende mostrar la necesidad de armonizar la actual pandemia causada por el nuevo coronavirus con el cumplimiento de las normas establecidas en el Reglamento General de Protección de Datos Personales 2016/679 (UE). Se utilizaron como base teórica las recomendaciones de la Organización Mundial de la Salud, así como las directrices e informes emitidos por las autoridades de protección de datos personales de Portugal, España e Italia. Con ese fin, se hicieron breves consideraciones sobre el Reglamento General de Protección de Datos Personales 2016/679 (UE) y los desafíos tecnológicos junto con el principio de proporcionalidad. La situación actual de la nueva pandemia de coronavirus quedó entonces expuesta, con la histórica actuación de la Organización Mundial de la Salud. Por último, se analizó la forma en que la pandemia está repercutiendo en el cumplimiento del Reglamento, en particular en tres países, Portugal, España e Italia, y cómo éstos están haciendo frente a la aparición de nuevas solicitudes de detección y notificación de casos.

Palabras clave: Reglamento General de Protección de Datos, nuevo coronavirus, impactos en el cumplimiento del reglamento, aplicaciones de seguimiento de casos.

Introdução

Diante da atual crise decorrente do surto do novo coronavírus (COVID-19) foram adotadas diversas medidas de combate ao vírus em todo o mundo, sendo esta a atual preocupação da maioria dos governos.

Atrelado ao novo cenário mundial, cresce também as questões acerca da proteção de dados pessoais. Com o desenvolvimento de novas tecnologias e o aumento do investimento nos setores de Tecnologia da Informação, procura-se desvendar como será possível harmonizar as medidas de combate ao novo coronavírus e as normas previstas no Regulamento Geral de Proteção de Dados pessoais 2016/679 da União Européia.

Após os escândalos de espionagem e divulgação de dados, como o da *Cambridge Analytica* (2016) e do *Facebook* (2016 e 2018), foi aprovado o *General Data Protection Regulation (GPDR*), que regulamenta no âmbito da União Européia sobre a proteção de dados.

Tendo em vista o delicado momento vivenciado mundialmente, torna-se necessário refletir como cumprir as normas dispostas no Regulamento frente a pandemia do COVID-19.

Desse modo, pretende-se analisar como a atual pandemia do novo coronavírus está a impactar o cumprimento do Regulamento Geral de Proteção de Dados pessoais, a fim de que haja um resultado harmônico entre eles.

Para tentar responder esta questão, o presente artigo está divido em três capítulos. O primeiro trata do Regulamento Geral de Proteção de Dados, sob uma visão geral, preocupada com os desafios tecnológicos e a aplicação correta do princípio da proporcionalidade.

O segundo capítulo versa sobre a atual pandemia do novo coronavírus, expondo o que é esse novo vírus, os impactos globais sofridos com o crescente número de infectados e mortes, bem como quais são as ações e recomendações da Organização Mundial da Saúde (OMS) diante desse cenário.

Por fim, no terceiro capítulo sustenta-se a preocupação com o vazamento de dados pessoais, notadamente os dados sensíveis referentes à saúde, e a importância do cumprimento das normas previstas no RGPD. Para tanto são explanados o caso específico de três países da União Européia: Portugal, Espanha e Itália, e como eles estão lidando com os novos aplicativos usados para rastreio e notificação de infectados.

1 Regulamento Geral de Proteção de Dados da União Européia

O Regulamento Geral de Proteção de Dados da União Européia (RGPD), n. 679/2016 estabelece a regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoa na União Européia.

De início, cumpre esclarecer que não é a pretensão do presente artigo exaurir a análise do Regulamento, mas sim proporcionar ao leitor uma visão global do mesmo, sem adentrar em questões específicas.

Antes do RGPD, a Organização para a Cooperação e Desenvolvimento Econômicos (OCDE) publicou em 1980 Diretrizes relativas à política internacional sobre a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais, tendo em vista a introdução da tecnologia de informação nas áreas econômicas e sociais, bem como a importância e poder crescentes do processamento automatizado de dados (OCDE, 2002).

Assim, com a intenção de criar um sistema de proteção de dados em toda a Europa, publicou em 1980 "As Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais", (as "Diretrizes sobre Privacidade"), que foram adotadas enquanto Recomendação do Conselho da OCDE.

As Diretrizes sobre a Privacidade baseavam-se em três princípios comuns aos países membros da OCDE, quais sejam, democracia pluralista, respeito aos direitos humanos e economias de mercado aberto (OCDE, 2002).

Conforme a OCDE, as Diretrizes sobre a Privacidade representam um consenso internacional sobre a orientação geral a respeito da coleta e do gerenciamento da informação pessoal. Nesse sentido, princípios como clareza e flexibilidade de aplicação e pela formulação, suficientemente ampla para possibilitar a adaptação às mudanças tecnológicas são característicos das Diretrizes (OCDE, 2002).

Para garantir o cumprimento das Diretrizes, os princípios, aplicados a nível nacional e internacional, devem abranger todos os meios utilizados para o processamento automatizado de dados referentes a indivíduos, desde o computador local à rede de complexas ramificações nacionais e internacionais. Ademais, deve abranger todos os tipos de processamento de dados pessoais (da administração do pessoal ao levantamento de perfis de consumidores) e todas as categorias de dados (da circulação de dados ao seu conteúdo, dos mais comuns aos mais sensíveis) (OCDE, 2002).

Alguns dos princípios elencados nas Diretrizes para a Privacidade eram os princípios de limitação da coleta, de qualidade dos dados, de definição da finalidade, de limitação de utilização, do back-up de segurança, de abertura, de participação do indivíduo e princípio de responsabilização (OCDE, 2002).

No entanto estas diretrizes não eram obrigatórias e as leis de privacidade de dados variavam de acordo com os países. Estas variações acabaram por levar a que se propusesse uma diretiva a nível Europeu, a Diretiva de Proteção de dados 95/46/EC.

Nesse ponto, uma das considerações feitas pelo RGPD foi justamente que os princípios e objetivos da Diretiva 95/46/CE, apesar de válidos, não evitaram a fragmentação da aplicação da proteção de dados ao nível da União Européia, a saber:

> (9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte,

> constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE (UE, 2016).

A diretiva 95/46/EC tinha o propósito de uniformizar as leis dos diferentes estados membros, mas sendo uma diretiva, ainda havia espaço para cada país fazer a sua interpretação e as organizações também nunca deram grande importância à mesma. Juntando a estes fatos, o rápido crescimento dos dados online e da virtualização, surgiu a necessidade de uma atualização desta diretiva, agora sob a forma de um regulamento, o Regulamento Geral de Proteção de Dados Pessoais.

O RGPD foi aprovado pelo Parlamento Europeu em abril de 2016, com aplicação forçosa e inevitável em 25 de maio de 2018.

Diante desse cenário, o Regulamento trouxe uma complexidade significante, com grandes mudanças e impactos nos negócios. Além disso, por se tratar de um regulamento, deve ser cumprido de igual forma em todos os países membros da União Européia, sendo sua implementação obrigatória.

O cumprimento com este Regulamento tem como princípio fundamental a gestão de riscos para os dados pessoais dos titulares dos dados, e implica que as organizações necessitem de realizar análises de risco aos seus processos que tratem dados pessoais e às suas atividades que os processam.

Em seu texto, o Regulamento dispôs que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental, bem como que os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais (UE, 2016).

Frisa-se, pois, a afirmação de que "[...] o RGPD deverá ser a nova bitola do fluxo relacional entre organizações e pessoas singulares, que intenciona ajustar-se às normas tecnológicos dos nossos dias" (CORDEIRO; GOUVEIA, 2018, p. 3), senão vejamos:

> O RGPD deverá ser a nova bitola do fluxo relacional entre organizações e pessoas singulares, que intenciona ajustar-se às normas tecnológicos dos nossos dias. Vivemos hoje à luz de escândalos de abuso do usufruto de dados pessoais por redes sociais e sob o fantasma da interrogação de que organizações possuem os nossos dados e daquilo que dados conseguem obter, saber e até prever, de cada um de nós. **O RGPD mostra-se uma alteração que embora não ansiada pelas empresas, é uma indispensável atualização no quadro da sociedade da informação atual, revogando regulamentação com mais de 20 anos e pouco hábil em nos proteger de comunicações (cada vez mais) tecnológicas e pouco precavida em questões de e-Privacy e do digital** (CORDEIRO; GOUVEIA, 2018, p. 3, **grifo nosso**).

Nesse sentido, o RGPD utiliza como pilares o tratamento lícito e transparente dos dados, a minimização dos dados e recolha apenas para os fins específicos, somente durante o tempo estritamente necessário, com direito ao esquecimento, dentre outros.

Uma das previsões importantes no Regulamento é o consentimento do titular de dados, que passa a figurar como elemento principal para autorizar a coleta e tratamento de dados, devendo ser inequívoco e envolver sempre uma postura assertiva. Assim está previsto em seu art. 7º, a saber:

> Artigo 7.o
>
> Condições aplicáveis ao consentimento
>
> 1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
>
> 2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
>
> 3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.
>
> 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato. (UE, 2016).

Pontua-se, outrossim, quanto à aplicação extraterritorial, o art. 3º do Regulamento determina que as regras do RGPD são aplicáveis ao tratamento de dados pessoais efetuado no contexto das atividades do estabelecimento de um responsável pelo tratamento, ou das atividades de um subcontratante, situado no território da União Européia, independentemente de o tratamento em si ocorrer dentro ou fora da União. Isto é, o RGPD passa a ser aplicável não só às empresas sediadas na EU, como também a empresas cujas atividades estejam alicerçadas na utilização de dados pessoais na iaôão Européia.

A intenção do parlamento europeu foi, portanto, de garantir proteção ampla a todos os indivíduos que tiveram seus dados coletados de alguma forma por empresas ou instituições que realizam transferência de dados com organizações européias, fazendo com que as mesmas prestem contas nesse sentido.

Outra previsão que merece destaque é quanto ao poder concedido às autoridades fiscalizadoras para aplicar sanções a quem descumprir o Regulamento. Assim, as Autoridades de Proteção de Dados (*Data Protection Authorities)* ficam encarregadas de supervisionar a aplicação das regras (arts. 52 e ss da RGPD).

Ademais, cria-se a figura do Diretor de Proteção de Dados, o DPO (*Data Protection Officer),* que é o encarregado da proteção de dados (art. 37 da RGPD), que, dentre as funções elencadas no art. 39 do Regulamento, deve informar e aconselhar o responsável pelo tratamento, bem como controlar a conformidade com o regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros.

Não obstante as inovações trazidas pelo RGPD, este deve ser pensado quanto aos desafios específicos a nível tecnológico, no sentido de que muitas empresas podem ter dificuldades em responder ao texto do Regulamento em sua íntegra.

A dificuldade no cumprimento do RGPD reside, pois, no pilar tecnologia, conforme defendem Cordeiro e Gouveia, a saber:

> Uma das principais dificuldades das empresas, para assegurar os mecanismos de conformidade com o novo regulamento, é que dados pessoais como os números de identificação, emails, contactos telefónicos, cookies, endereços, etc. estão dispersos por diversos sistemas. As empresas terão de centralizar a gestão dos dados pessoais ou garantir que todos os sistemas estão conformes (tarefa que exige tempo, recursos e conhecimento para poder ser realizada). Estes objetivos podem ser alcançados com recurso a técnicas de encriptação, pseudonimização e a anonimização dos dados, que permitem trabalhar sobre os dados pessoais sem identificação do seu titular. Naturalmente, impõe-se um rigoroso controlo de acessos, deteção de falhas de segurança e respetiva comunicação em 72 horas à comissão nacional de proteção de dados (CORDEIRO; GOUVEIA, 2018, p. 4).

Nesse sentido, não há uma solução imediata e normalizada, devendo as empresas percorrer um caminho tortuoso, qual seja, um processo iterativo de otimização de processos e ajustes de mentalidades, que se repetirá sucessivamente até que procedimentos enraizados sejam repensados ou, ao menos, revistos (CORDEIRO; GOUVEIA, 2018, p. 4).

Diante desse cenário, deve-se buscar nos princípios da necessidade, do não estrangulamento tributário e da proporcionalidade formas de aplicação das normas previstas no Regulamento, visando a prudência das normas e a proteção dos destinatários na sua aplicação.

Pelo princípio da necessidade, tem-se que as normas e os procedimentos da sua aplicação sejam necessários, imprescindíveis para a proteção dos interesses e valores em causa. Assim, liga-se à proibição do estrangulamento tributário, que veda as limitações, imposições e encargos que impeçam ou dificultem seriamente uma atividade legítima ou a tornem desnecessariamente onerosas frente aos seus fins (CAMPOS; FOZ; GONÇALVES, 2019, p. 460).

Por fim, quanto ao princípio da proporcionalidade, tem-se que os meios utilizados na aplicação das normas devem ser os adequados ao fim que se pretende atingir, em íntima relação com os princípios citados anteriormente. É dizer, não há que se falar em meios excessivos, vexatórios ou ineficazes (CAMPOS; FOZ; GONÇALVES, 2019, p. 461).

Vejamos, pois, o seguinte exemplo:

> Se um cliente se dirige a um profissional liberal (médico, advogado, arquiteto, contabilista, etc.) com escassos clientes, pode e deve esperar dele serviços profissionais de qualidade (não confundamos a quantidade com a qualidade).Mas não deve esperar a utilização de infra-estruturas pesadas e caras, meios de recolha de dados, sua armazenagem e utilização com o mais elevado grau de segurança que seja possível obter. Um gabinete fechado, um armário também fechado e um computador dotado de sistemas de segurança razoáveis , são de esperar e serão normalmente suficientes.
>
> Se for exigido (não sendo exigível) o grau máximo de segurança – utilizado por exemplo por um banco ou uma empresa de transmissão de dados -tal implicará **duas consequências: o cliente não terá capacidade financeira de pagar os serviços onerados por esses custos, ficando com as suas necessidades insatisfeitas; os**

> **prestadores de serviços serão extremamente reduzidos – ficando limitados a alguns grupos com as consequentes e graves desvantagens sociais** (CAMPOS; FOZ. GONÇALVES, 2019, p. 461 **grifo nosso**).

Vê-se, portanto, que ao aplicar o Regulamento, é essencial a utilização dos princípios basilares do Direito, de modo tal que possa ser atingido a finalidade pretendida pelo Regulamento, sem se tornar algo extremamente oneroso ao indivíduo.

Isto posto, feita a breve análise do Regulamento Geral de Proteção de Dados, resta imprescindível a compreensão do atual momento vivenciado pelo mundo, o da pandemia do novo coronavírus.

2 A Crise do Coronavírus

O ano de 2020 está sendo marcado pela grave crise provocada pela pandemia do novo coronavírus, batizado de COVID-19, o qual foi notificado pela primeira vez na província de Wuhan, na China, em 31 de dezembro de 2019. A COVID-19 é uma doença causada pelo coronavírus SARS-CoV-2, que apresenta um quadro clínico que varia de infecções assintomáticas a quadros respiratórios graves.

O cenário mundial ainda é de incertezas, considerando que, conforme a Organização Mundial da Saúde (OMS), a maioria dos pacientes com COVID-19 (cerca de 80%) podem ser assintomáticos e cerca de 20% dos casos podem requerer atendimento hospitalar por apresentarem dificuldade respiratória e desses casos aproximadamente 5% podem necessitar de suporte para o tratamento de insuficiência respiratória (suporte ventilatório).

Com superlotações em hospitais e falta de leitos em Unidades de Tratamento Intensivas (UTIs), a crise assola diversos países, com um número elevado de mortes diárias anunciadas em jornais, transformando vidas em meros números utilizados em índices de pesquisa da mortalidade do vírus.

Apesar de os sintomas da COVID-19 poderem variar de um simples resfriado até uma pneumonia severa, com os sintomas mais comuns sendo tosse, febre, coriza, dor de garganta e dificuldade para respirar, o que preocupa os governos é a superlotação dos hospitais, impossibilitando o atendimento adequado de todos e causando uma verdadeira crise na saúde pública.

Até a data de 02 de junho de 2020, a Universidade Johns Hopkins confirmou o total de casos mundial de 6.325.303 pessoas contaminadas pelo COVID-19, sendo que destas, 377.460 pessoas vieram a óbito em decorrência do vírus e 2.727.679 pessoas conseguiram se recuperar (JOHNS HOPKINS UNIVERSITY, 2020).

O epicentro da pandemia, que no início era na China e depois migrou para a Itália, hoje está nos Estados Unidos da América.

Os números divulgados pela Universidade Johns Hopkins de casos confirmados até o dia 02 de junho de 2020 eram de 1.820.523 nos Estado Unidos, 526.447 no Brasil, 423.186 na Russia, 279.391 no Reino Unido, 239.932 na Espanha e 233.515 na Itália (JOHNS HOPKINS UNIVERSITY, 2020).

Já o número de mortes confirmadas com a causa da morte o novo coronavírus até o dia 02 de junho de 2020 eram de 105.644 nos Estados Unidos, 39.451 no Reino Unido, 33.530 na Itália, 29.937 no Brasil, 28.836 na França e 27.127 na Espanha (JOHNS HOPKINS UNIVERSITY, 2020).

Por outro lado, o número de infectados recuperados confirmados até o dia 02 de junho de 2020 eram de 458.231 nos Estados Unidos, 211.080 no Brasil, 186.602 na Russia, 166.609 na Alemanha, 160.092 na Itália e 150.376 na Espanha (JOHNS HOPKINS UNIVERSITY, 2020).

Como exemplo a sobrecarga do sistema de saúde, tem-se a Itália, que sofreu com medidas progressivamente restritivas desde o começo do surto de casos do COVID-19 no país, conforme explica a *Human Rights Watch*:

> Na Itália, o governo impôs um confinamento, mas com maiores proteções aos direitos individuais. O governo italiano adotou medidas progressivamente restritivas desde o primeiro grande surto de casos COVID-19 no país no final de fevereiro. As autoridades inicialmente colocaram dez cidades na Lombardia e uma em Veneto sob quarentena estrita, proibindo os residentes de deixarem essas regiões. Ao mesmo tempo, escolas nas regiões afetadas foram fechadas. Citando uma onda de casos e uma sobrecarga cada vez mais insustentável para o sistema público de saúde, em 8 de março, o governo impôs uma série de novas medidas a uma grande parte do norte do país, implementando restrições muito mais severas à circulação e a liberdades fundamentais. No dia seguinte, as medidas foram aplicadas em todo o país. Outras medidas impostas incluem restrições a viagens, exceto por questões essenciais de saúde ou trabalho (mediante autodeclaração), fechamento de todos os centros culturais (cinemas, museus) e cancelamento de eventos esportivos e aglomerações públicas. Em 11 de março, o governo fechou todos os bares, restaurantes e comércios, exceto supermercados e farmácias (e algumas outras exceções) em todo o país. As pessoas que desobedecerem as restrições à circulação sem um motivo válido podem ser multadas em até 206 euros e enfrentar uma pena de prisão de três meses. Todas as escolas e universidades foram fechadas em todo o país. As pessoas foram autorizadas a sair para comprar itens essenciais, para fazer exercícios, para trabalhar (se não puderem realizar o trabalho em casa) e para tratar de cuidados de saúde (incluindo cuidados a um parente doente) (DIMENSÕES..., 2020).

Diante deste triste cenário que se repete em diversos países, a Organização Mundial da Saúde (OMS) publicou diversas diretrizes para auxiliar os governos a lidar com a crise provocada pelo novo coronavírus.

Nesse contexto insere-se a Atualização da Estratégia frente ao COVID-19, publicada pela OMS em 14 de abril de 2020, que pretende ajudar a orientar a resposta de saúde pública ao COVID-19, a nível nacional e internacional, além de atualizar a estratégia global de resposta à pandemia mundial, complementando orientações técnicas já publicadas pela OMS (OMS, 2020).

O objetivo primordial exposto pela OMS é de que todos os países controlem a pandemia ao abrandar a transmissão e reduzir a mortalidade associada ao COVID-19.

A Atualização da Estratégia elenca, ainda, como objetivos estratégicos mundiais a mobilização de todos os setores e comunidades para garantir que cada setor do governo e da sociedade assuma a responsabilidade e participe na resposta e prevenção de casos. Ademais, devem-se controlar os casos esporádicos e grupos de casos, prevenindo a transmissão comunitária por meio da rápida detecção e

isolamento de todos os casos, bem como conter a transmissão comunitária mediante a prevenção do contágio e medidas de controle adequadas (OMS, 2020).

Por fim, a OMS cita ainda a redução da mortalidade e o desenvolvimento de vacinas e terapias seguras e eficazes a serem oferecidas de modo acessível e em grande escala como objetivos a serem cumpridos pelos governos (OMS, 2020).

Não obstante a profunda crise gerada no campo da saúde pública, a esfera econômica também foi afetada pela crise, considerando as oscilações nas bolsas de valores em todo o mundo, desemprego e com o impacto da própria crise na saúde pública.

Desse modo, não resta dúvidas que o novo coronavírus provocou, e ainda provoca uma mudança no cenário global, impactando diversos setores da sociedade e governos. Nesse contexto, o próprio cumprimento da Regulação Geral de Proteção de Dados merece ser repensado à luz desse cenário.

3 Os Impactos do Coronavírus: limitações ao cumprimento da RGPD

Com o desenvolvimento de novas tecnologias surgem questionamentos quanto a segurança das informações na era digital. Assim, é natural que pessoas físicas e jurídicas procurem meios de manter seus dados pessoais protegidos, evitando a exposição à ataques de hackers.

Considerando o contexto da pandemia mundial do novo coronavírus, a preocupação com a proteção de dados persiste, tendo em vista que dados relativos a saúde são considerados dados sensíveis, bem como que eventual vazamento de dados, de qualquer natureza, pode prejudicar ainda mais empresas, governos e indivíduos, trazendo mais instabilidade ao cenário mundial.

Pontua-se que, conforme noticiado pela própria Organização Mundial da Saúde, desde o início da pandemia da COVID-19 observou-se um aumento extraordinário do número de ataques informáticos contra o seu pessoal, bem como de esquemas de correio eletrônico contra o público em geral (*LA OMS...*, 2020), a saber:

> Cerca de 450 endereços de correio electrónico e palavras-passe activos da OMS foram divulgados esta semana na Internet, juntamente com os de milhares de outros que trabalharam na resposta ao novo coronavírus.
>
> A fuga destas credenciais não comprometeu os sistemas da OMS, uma vez que os dados não são recentes. No entanto, o ataque afectou um sistema de rede externa mais antigo utilizado pelo pessoal activo e reformado e pelos parceiros.
>
> A OMS está actualmente a trabalhar na migração dos sistemas afectados para um sistema de autenticação mais seguro.
>
> Os autores de fraudes que se fazem passar por pessoal da OMS através de correio electrónico estão também a dirigir-se cada vez mais ao público em geral, com a intenção de canalizar as doações para um fundo fictício e não para o verdadeiro Fundo de Resposta COVID-19. O número de ciberataques que a Organização recebeu até agora é mais de cinco vezes superior ao do mesmo período do ano passado.
>
> "Garantir a segurança da informação sanitária dos Estados-Membros e a privacidade dos utilizadores que interagem connosco é sempre uma prioridade para a OMS, mas ainda mais durante a pandemia da COVID-19. Agradecemos os alertas que recebemos

> dos Estados-Membros e do sector privado. Estamos todos juntos nesta luta", disse Bernardo Mariano, Director de Sistemas de Informação da OMS (*LA OMS...*, 2020, tradução nossa)[3]

Nesse sentido, a OMS disponibilizou uma Plataforma Clínica Mundial sobre a COVID-19 para que os Estados-Partes no Regulamento Sanitário Internacional (RSI) de 2005 possam compartilhar com a OMS informação e dados clínicos anonimizados sobre pacientes com infecção confirmada ou potencial do vírus.

A preocupação com o armazenamento de dados foi exposta da seguinte maneira no documento publicado pela OMS na Plataforma Clínica Mundial sobre a COVID-19:

> Os dados COVID-19 anónimos serão armazenados na Plataforma de Dados COVID-19, que é uma plataforma electrónica segura, protegida por senha, com acesso restrito, alojada por um fornecedor externo em nome da OMS. A OMS e o fornecedor celebraram acordos contratuais nos termos dos quais o fornecedor exige, nomeadamente: i) proteger a confidencialidade dos dados anónimos sobre a COVID-19 e impedir a sua divulgação ii) abster-se de utilizar os dados COVID-19 anónimos para outros fins que não o fornecimento de serviços de alojamento da OMS, em conformidade com os acordos contratuais; e iii) aplicar e manter medidas de segurança técnicas e organizacionais para proteger a segurança da COVID-19 Dados Anónimos e a Plataforma de Dados COVID-19. Em conformidade com o artigo 11.4 do RSI (2005), a OMS não os dados anónimos COVID-19 disponíveis para outros Estados Partes até ao momento em que pela primeira vez qualquer das condições estabelecidas no n.º 2 do referido artigo 11. afectadas. De acordo com o artigo 11º acima mencionado, a OMS não colocará à disposição do público dados anônimos sobre a COVID-19 até serem disponibilizadas aos Estados Partes, e desde que tenham sido divulgadas outras informações sobre a epidemia de COVID-19 e há necessidade de divulgar informação autorizada e independente a este respeito (*LA OMS...,* 2020) [4]

---

[3] Esta semana se han filtrado en internet cerca de 450 direcciones y contraseñas de correos electrónicos activos de la OMS, junto con las de otros miles de personas que trabajan en la respuesta al nuevo coronavirus.

La filtración de esas credenciales no ha puesto en peligro los sistemas de la OMS, ya que los datos no son recientes. Sin embargo, el ataque sí ha afectado a un sistema de red externa más antiguo, utilizado por personal en activo y jubilado, así como por asociados.

La OMS está trabajando en estos momentos en la migración de los sistemas afectados hacia un sistema de autenticación más seguro.

Los estafadores que se hacen pasar por personal de la OMS a través de correos electrónicos se están dirigiendo también, cada vez más, contra el público en general, con intención de canalizar donaciones a un fondo ficticio y no al auténtico Fondo de Respuesta a la COVID-19. El número de ciberataques que ha recibido la Organización hasta ahora es más de cinco veces mayor al sufrido en el mismo periodo del año pasado.

«Garantizar la seguridad de la información sanitaria de los Estados Miembros y la privacidad de los usuarios que interactúan con nosotros es una prioridad para la OMS en todo momento, pero aún más durante la pandemia de COVID-19. Agradecemos las alertas que recibimos de los Estados Miembros y del sector privado. Estamos todos juntos en esta lucha», ha dicho Bernardo Mariano, Director de Sistemas de Información de la OMS (*LA OMS...,* 2020).

[4] Los Datos Anonimizados sobre la COVID-19 se guardarán en la Plataforma de Datos sobre la COVID-19, que es una plataforma electrónica segura de acceso restringido protegida por contraseña, alojada por un proveedor externo en nombre de la OMS. La OMS y dicho proveedor han celebrado acuerdos contractuales en virtud de los cuales el proveedor se obliga, entre otros: i) a proteger la confidencialidad de los Datos Anonimizados sobre la COVID-19 e impedir su revelación no

Desse modo, ao menos no campo teórico, os dados anônimos relativos aos COVID-19 receberão uma proteção especial, contando com uma plataforma eletrônica segura, de maneira tal a proteger a confidencialidade dos dados.

Ressalta-se que os dados sobre saúde são particularmente sensíveis, de modo que a publicação de informações online pode causar risos significativos para as pessoas afetadas, bem como para pessoas já inseridas num sistema de vulnerabilidade e marginalização na sociedade. Assim, garantias legais baseadas em uma perspectiva de direitos deveriam orientar o uso e a gestão de informações pessoais de saúde (DIMENSÕES..., 2020).

Nesse aspecto, a Comissão Européia de Proteção de Dados (EDPB) divulgou em março de 2020 a declaração de seu Presidente sobre o processamento de dados pessoais no contexto do surto da COVID-19, no qual deixa claro que a proteção de dados seguindo o RGPD não dificulta as medidas tomadas na luta contra o vírus, senão vejamos:

> Governos, organizações públicas e privadas em toda a Europa estão a tomar medidas para conter e mitigar a COVID-19. Isto pode envolver o processamento de diferentes tipos de dados pessoais.
>
> Andrea Jelinek, presidente do Conselho Europeu de Protecção de Dados (EDPB), afirmou: "Protecção de dados as regras (como o GDPR) não dificultam as medidas tomadas na luta contra o coronavírus pandemia. No entanto, gostaria de sublinhar que, mesmo nestes tempos excepcionais, os dados, o responsável pelo tratamento deve assegurar a protecção dos dados pessoais das pessoas em causa. Por conseguinte, há que ter em conta um certo número de considerações para garantir o tratamento lícito de dados pessoais".
>
> O GDPR é uma legislação ampla e prevê também as regras a aplicar ao processamento de dados pessoais num contexto como o que se refere à COVID-19. De facto, o GDPR fornece pelos motivos jurídicos que permitem aos empregadores e às autoridades de saúde pública competentes processar dados pessoais no contexto de epidemias, sem a necessidade de obter o consentimento do pessoa em causa. Isto aplica-se, por exemplo, quando o tratamento de dados pessoais é necessário para a empregadores por razões de interesse público na área da saúde pública ou para proteger interesses vitais (artigos 6º e 9º do PIBR) ou para cumprir outra obrigação legal (EDBP, 2020a, tradução nossa).[5]

autorizada; ii) a abstenerse de utilizar los Datos Anonimizados sobre la COVID-19 para fines que no sean la prestación de servicios de alojamiento a la OMS de conformidad con los acuerdos contractuales; y iii) a aplicar y mantener las oportunas medidas de seguridad técnica y organizativa para proteger la seguridad de los Datos Anonimizados sobre la COVID-19 y de la Plataforma de Datos sobre la COVID-19. De conformidad con el párrafo 4 del artículo 11 del RSI (2005), la OMS no pondrá los Datos Anonimizados sobre la COVID-19 a disposición de los demás Estados Partes hasta el momento en que se cumpla por primera vez alguna de las condiciones estipuladas en el párrafo 2 de dicho artículo 11, y previa consulta con los países afectados. Según lo establecido en el citado artículo 11, la OMS no pondrá a disposición del público los Datos Anonimizados sobre la COVID-19 hasta que estos no se hayan puesto a disposición de los Estados Partes, y siempre que se haya difundido públicamente otra información sobre la epidemia de COVID-19 y sea necesario difundir información autorizada e independiente al respecto (*LA OMS...*, 2020).

[5] Governments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19. This can involve the processing of different types of personal data. Andrea Jelinek, Chair of the European Data Protection Board (EDPB), said: “Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into

Isto posto, cabe observar como alguns países membros da União Européia estão a tratar da proteção de dados pessoais, conforme previsto no Regulamento Geral de Proteção de Dados.

3.1 Casos Específicos

3.1.1 Portugal

Em Portugal a Comissão Nacional de Proteção de Dados (CNPD) tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, respeitando os direitos e garantias consagradas na Constituição portuguesa e na lei. É uma entidade administrativa independente com poderes de autoridade, funcionando junto da Assembleia da República.

Os elementos normativos que tratam da proteção de dados em Portugal são a Lei 58/2019, que é a lei nacional de execução do Regulamento (UE) 2016/679 (PORTUGAL, 2019a), a Lei 59/2019 que trata da proteção de dados para os tratamentos efetuados por autoridades competentes para a detecção, prevenção e investigação e repressão de infrações penais e para a execução de sanções penais (PORTUGAL, 2019b).

Em seu sitio eletrônico, o CNPD divulga diversas diretrizes a respeito da COVID-19, dentre elas a Diretriz n. 4/2020, que trata da utilização de dados de localização e ferramentas de *contact tracing* no contexto atual da pandemia, aprovada pelo Comitê Europeu para a Proteção de Dados.

Trata-se, pois, de orientações que elucidam as condições e princípios para a utilização proporcionada dos dados de localização e dos instrumentos de localização, com a finalidade de utilizar dados de localização para apoiar a resposta à pandemia, modelando a propagação do vírus, bem como de rastreamento de contatos para notificar os indivíduos de que estiveram próximos de alguém que foi confirmado como portador do vírus, visando quebrar as cadeias de contaminação (CNPD, 2020).

Cabe destacar que na introdução da Diretriz n. 4/2020, em seus itens 7 e 8 é expõem a relação do RGPD com as medidas de proteção diante da pandemia do COVID-19, a saber:

> 7 O CEPD salienta que o RGPD e a Diretiva 2002/58/CE (Diretiva «ePrivacy») contêm regras específicas que permitem a utilização de dados anónimos ou pessoais para apoiar as autoridades públicas e outros intervenientes a nível nacional e da UE na monitorização e na disseminação do vírus SARS-CoV2.2
>
> 8 A este respeito, o CEPD já tomou posição sobre a utilização de tais aplicações de rastreamento de contacto dever ser voluntária e não dever depender do rastreamento

account to guarantee the lawful processing of personal data." The GDPR is a broad legislation and also provides for the rules to apply to the processing of personal data in a context such as the one relating to COVID-19. Indeed, the GDPR provides for the legal grounds to enable the employers and the competent public health authorities to process personal data in the context of epidemics, without the need to obtain the consent of the data subject. This applies for instance when the processing of personal data is necessary for the employers for reasons of public interest in the area of public health or to protect vital interests (Art. 6 and 9 of the GDPR) or to comply with another legal obligation (EDBP, 2020a).

> de movimentos individuais, mas sim de informações de proximidade sobre os utilizadores (EDPB, 2020b).

Seguindo a tendência de outros países, será lançado no final de junho o aplicativo português "*Stayaway"* de rastreio de contatos de infecção. O app tem a pretensão de ser um método que permite detectar e interromper cadeias de transmissão do novo coronavírus (CALHEIROS, 2020).

Por trás da iniciativa está o INESC TEC, junto as *startups spinoff* Keyruptive e a UBIrider, em parceria com o Instituto de Saúde Pública da Universidade do Porto (ISPUP), que envolve também Ordem dos Médicos, Direção-Geral da Saúde e Ministério da Saúde.

No entanto, o que preocupa é a proteção de dados de um projeto que quer conter a doença sem comprometer a privacidade de cada um, garantindo o anonimato, senão vejamos:

> **A grande diferença das aplicações que estão a ser criadas para cada país é saber se usam uma abordagem centralizada ou descentralizada.** Na centralizada, a app comunica todos os dados do utilizador (registo de contacto, localização de GPS) para um servidor central, onde são feitos os cálculos de risco de contacto, notificação, entre outros benefícios da app. Na opinião de Francisco Maia, o maior senão desta abordagem – apesar de existir mais informação centralizada que permite uma maior análise e previsão – é incorrer num problema de invasão de privacidade e de proteção de dados. Este é o caminho que tanto a França como o Reino Unido estão a seguir, gerando mais uma polémica no meio da crise sanitária. **Tal como a Suíça, a Itália e a Espanha também Portugal está a desenvolver uma abordagem descentralizada, em que "não existe recolha de nenhum tipo de dado pessoal" a quem utilizar a Stayaway.** A pessoa não terá de partilhar a sua localização ou o seu nome, nada. Tudo é feito com a geração de *beacons* (números aleatórios) e os dados dessas observações nunca saem do telemóvel. A única altura em que há um dado que sai do telemóvel é quando alguém, em caso de ser diagnosticado com Covid-19 e de forma voluntária, envia para o servidor central os seus números aleatórios e o código fornecido pelas autoridades de saúde pública. Isso faz com que todos os outros números aleatórios que estiveram em contacto com o infetado recebam um alerta, sem nunca se saber quem é o contacto dessa cadeia (CALHEIROS, 2020).

Desse modo, apesar da pandemia provocada pelo novo coronavírus, a preocupação reside na proteção de dados pessoais, evitando-se a invasão da privacidade dos usuários. É dizer, ainda que num cenário de crise, o Regulamento Geral de Proteção de Dados não deve ser esquecido.

3.1.2 Espanha

Na Espanha, a Agência Espanhola de Proteção de Dados é a autoridade pública independente responsável por garantir a privacidade e a proteção de dados dos cidadãos.

No campo normativo, tem-se a Lei Orgânica 3/2018, de 5 de dezembro, sobre Proteção de Dados Pessoais e garantia de direitos digitais. O objetivo da lei, conforme seu artigo primeiro é adaptar o sistema jurídico espanhol ao Regulamento (UE) 2016/679, relativo à proteção de pessoas singulares no que diz respeito ao tratamento de seus dados. Assim, o direito fundamental das pessoas singulares à proteção de dados pessoais, protegido pelo artigo 18.4 da Constituição Espanhola,

será exercido em conformidade com as disposições do Regulamento (UE) 2016/679 e desta lei orgânica (ESPANHA, 2018).

Considerando a atual propagação do vírus COVID-19, a Agência Espanhola de Proteção de Dados (AEPD) publicou um relatório no qual analisa o processamento de dados pessoais em relação a situação ora vivenciada.

De acordo com o relatório, a RGPD reconhece explicitamente em seu Considerando 46 como base legal para o tratamento legal de dados pessoais em casos excepcionais, como o controle de epidemias e sua disseminação, a missão realizada no interesse público (art. 6.1.e) ou o interesses vitais da parte interessada ou de outras pessoas físicas (art. 6.1.d), apesar de haver outras bases, como, por exemplo, o cumprimento de uma obrigação legal (para o empregador na prevenção de riscos ocupacionais de seu pessoal). Assim, essas bases legais permitem o processamento de dados sem o consentimento das pessoas afetadas (AEPD, 2020).

O relatório destaca, ainda, que o processamento de dados pessoais, mesmo nessas situações de emergência sanitária, deve continuar sendo tratado de acordo com os regulamentos de proteção de dados pessoais (RGPD e Lei Orgânica 3/2018 sobre Proteção de Dados Pessoais e garantia direitos digitais), uma vez que essas regras previam essa eventualidade, à qual seus princípios se aplicam e, entre eles, o tratamento de dados pessoais com legalidade, lealdade e transparência, limitação da finalidade (neste caso, salvaguardar os interesses das pessoas nessa situação de pandemia), o princípio da precisão e o princípio da minimização de dados (AEPD, 2020).

Dessa forma, os dados processados devem ser exclusivamente aqueles limitados aos necessários para a finalidade pretendida, sem que esse tratamento seja estendido a outros dados pessoais que não sejam estritamente necessários para essa finalidade (AEPD, 2020).

Após a divulgação do aplicativo *Stop Covid* na França, o governo da Catalunha lançou o aplicativo *Stop Covid19 Cat*, a fim de rastrear e identificar contatos por *Bluetooth* e alertar os usuários se eles tiverem passado mais de 15 minutos a menos de um metro de distância de alguém que teve teste positivo para coronavírus, a saber:

> O STOP COVID19 CAT permite-lhe monitorizar e monitorizar os seus sintomas através da aplicação. O utilizador pode controlar a evolução dos sintomas e seguir as indicações e dicas em cada situação.
>
> O cidadão pode realizar o seu teste sintomático através de um teste ao qual tem acesso através do registo no Código de Identificação Pessoal (CIP) do cartão de saúde. Esta autenticação e prova de possível diagnóstico está ligada ao Histórico Clínico Digital do utilizador, aspecto que permite aos profissionais de saúde realizar um acompanhamento personalizado dos cuidados e considerar outros dados clínicos relevantes do paciente. Em caso de diagnóstico positivo, a pessoa recebe conselhos e protocolos de actuação dos profissionais de saúde.
>
> A aplicação STOP COVID 19 tem diferentes funcionalidades de elevada utilidade para as autoridades de saúde e para a cidadania, porque permite:
> Promover e reforçar o confinamento voluntário.
>
> Descongestionar os serviços de cuidados cara-a-cara.
>
> Desmontar o número de telefone de contacto para outras emergências médicas.

> Prestar informações verdadeiras e fiáveis aos cidadãos.
> Proporcionar cuidados de saúde e aconselhamento à distância.
> Monitorizar e avaliar os sintomas dos cidadãos auto-avaliados através do teste e activar o Serviço de Emergência Médica.
>
> Sempre que o utilizador der o seu consentimento, as autoridades sanitárias podem também acompanhar a evolução da SRA Cov-2 por geolocalização. Isto facilita a tomada de decisões focalizadas e em tempo real pelas autoridades competentes, fornecendo dados sobre o território com base em utilizadores activos (*THE CATALAN...*, 2020, tradução nossa).[6]

Nota-se, pois, que a preocupação com as medidas de combate ao novo coronavírus deve coincidir com as orientações da AEPD, de modo a proteger os dados pessoais dos usuários do aplicativo.

O que ocorre, ao menos no campo teórico, é a convergência entre os aplicativos de rastreio e as normas previstas no RGPD.

3.1.3 Itália

A referência na proteção de dados pessoais na Itália é o Garante para a proteção de dados pessoais, que é uma autoridade administrativa independente estabelecida pela chamada Lei de Privacidade n. 675/1996, então regida pelo Código referente à proteção de dados pessoais (196/2003), alterada pelo Decreto Legistlativo n. 101/2018, que confirmou que o Garante é a autoridade de supervisão também designada para a aplicação do Regulamento Geral sobre a Proteção de Dados pessoais (UE) 2016/679.

---

[6] STOP COVID19 CAT allows you to monitor and monitor your symptoms through the application. The user can control the evolution of the symptoms and follow the directions and tips in each situation.

Citizens can perform their symptomatic test through a test that is accessed by registering with the Personal Identification Code (CIP) of the health card. This authentication and proof of possible diagnosis is linked to the user's Digital Clinical History, an aspect that allows healthcare professionals to carry out personalized care monitoring and consider other relevant patient clinical data. In case of a positive diagnosis, the person receives advice and protocols of action from healthcare professionals.

The STOP COVID 19 application has different functionalities of high utility for the health authorities and the citizenship, because it allows:

Promote and enhance voluntary confinement.

Decongestant face-to-face care services.

Disassemble the contact telephone number for other medical emergencies.

Provide truthful and reliable information to citizens.

Provides remote health care and advice.

Monitor and evaluate the symptoms of self-assessed citizens by means of the test and activate the Medical Emergency Service.

Whenever the user gives their consent, the health authorities can also track the evolution of Cov-2 SARS by geolocation. This facilitates focused and real-time decision-making by competent authorities, providing data on the territory based on active users (*THE CATALAN...*, 2020).

Após se tornar o epicentro da pandemia do novo coronavírus, foi lançado na Itália o aplicativo *Immuni*, que permite avisar os utilizadores que tenham tido uma exposição ao risco do COVID-19. O aplicativo funciona só com notificações, com a maioria dos dados anonimizados, sem solicitar nome, apelido, número de telefone, e-mail, etc.

O *app Immuni* exige o consentimento para notificar o usuário, depois há a possibilidade de a plataforma comunicar com o cidadão sem pôr em causa a sua identidade. Na prática, para proteger a privacidade, cada telefone está associado a um código aleatório, que muda várias vezes por hora (D'ELIA, 2020).[7]

Assim como já foi explorado anteriormente, a preocupação reside em conciliar as medidas de combate ao vírus com a proteção de dados pessoais, sendo este um direito previsto no Regulamento adotado em toda União Européia.

Discute-se, portanto, que os direitos previstos no Regulamento não devem ser esquecidos frente ao novo cenário mundial, devendo-se proceder com prudência na adoção de medidas de proteção contra o vírus, principalmente no que diz respeito a aplicativos que coletam diversos dados pessoais.

Considerações Finais

Ao longo do artigo discutiu-se acerca do cumprimento das normas previstas no RGPD tendo em vista a atual pandemia do novo coronavírus. Para tanto, proporcionou-se uma visão geral do Regulamento 2016/679 (UE), com enfoque nos desafios tecnológicos enfrentados para adequação às normas, bem como a necessidade de se atentar ao dispositivo legal sob a ótica do princípio da proporcionalidade.

Após, foi exposto o atual panorama mundial da pandemia do novo coronavírus, com a dificuldade dos governos de fazerem-se valer de medidas de combate ao vírus e o exponencial e preocupante número de mortos e infectados pelo COVID-19. Ademais, deu-se enfoque às recomendações da Organização Mundial da Saúde.

Nesse contexto, foi exposta a preocupação com recentes vazamentos de dados pessoais, considerando que os dados referentes à saúde são dados sensíveis, objeto de maior proteção pelo RGPD.

A fim de aproximar o leitor com a realidade de alguns países membros da União Européia, foram analisadas a situação de Portugal, Espanha e Itália frente a pandemia e como tais países estão lidando com os novos aplicativos usados para rastreio e notificação de infectados, alertando os usuários de eventual risco de contágio.

[7] A questo punto Immuni richiede il consenso per la notifica, quindi la possibilità per la piattaforma di comunicare con il cittadino senza però metterne in gioco l'identità. In pratica ad ogni telefono viene associato un codice casuale, che cambia più volte ogni ora per tutelare la privacy. Anche in questo caso dopo un tocco sul tasto "abilita" compare un pop-ip che richiede nuovamente un tocco sul tasto "consenti" (D'ELIA, 2020).

Desse modo, o presente artigo pretendeu responder a questão de como é possível harmonizar o cumprimento do Regulamento Geral de Proteção de Dados pessoais e as medidas de combate ao vírus em meio a pandemia do COVID-19.

Referências

AEPD. N/REF: 0017/2020. Gabinete Jurídico. Agencia Española de Protección de Datos. Madrid, 2020. Disponível em: <https://www.aepd.es/es/documento/2020-0017.pdf>. Acesso em: 04 jun. 2020.

CALHEIROS, Sónia. Covid-19: Apple e Google já testam a aplicação portuguesa Stayaway. Publicado em 02 jun. 2020. **Visão.** Portugal. Disponível em: <https://visao.sapo.pt/atualidade/sociedade/2020-06-02-covid-19-apple-e-google-ja-testam-a-aplicacao-portuguesa-stayaway/>. Acesso em: 03 jun. 2020.

CAMPOS Diogo Leite de; FOZ, Teresa; GONÇALVES, Nuno. **Estrutura Jurídica do Regulamento Geral de Proteção de Dados (RGPD) em Direito Portugês**. RJLB, ano 5 (2019), nº 1. Disponível em: <http://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0457_0463.pdf>. Acesso em: 01 jun. 2020.

CORDEIRO, Sivério Brunhoso; GOUVEIA, Luis Borges. **Regulamento Geral de Proteção de Dados (RGPD):** o novo pesadelo das empresas? Relatório Interno TRS 07/2018. Tecnologia, Redes e Sociedade. Maio, 2018. Disponível em: <https://bdigital.ufp.pt/bitstream/10284/6714/1/RI_trs_07_2018.pdf>. Acesso em: 01 jun. 2020.

D'ELIA, Dario. App Immuni, la prova: come funziona, dove scaricarla e come configurarla. **La Repubblica.** Roma, Itália. Publicado em 01 jun. 2020. Disponível em: <https://www.repubblica.it/tecnologia/2020/06/01/news/app_immuni_e_scaricabile_sullo_store_di_google_e_apple_cosa_bisogna_avere-258204188/>. Acesso em: 03 jun. 2020.

DIMENSÕES DE DIREITOS HUMANOS NA RESPOSTA À COVID-19. *Human Rights Watch*. Publicado em 22 mar. 2020. Disponível em: <https://www.hrw.org/pt/news/2020/03/23/339654>. Acesso em: 02 jun. 2020.

EDPB. *Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak*. Bruxelas, 16 de março de 2020. Comite Europeu para a Proteção de Dados. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/news/edpb_covid-19_20200316_press_statement_en.pdf>. Acesso em: 04 jun. 2020.

EDPB. **Diretrizes n.º 4/2020 sobre a utilização de dados de localização e ferramentas de *contact tracing* no contexto do surto de COVID-19**. Adotado em 21 de abril de 2020. Comitê Europeu para a Proteção de Dados. Disponível em: <https://www.cnpd.pt/home/orientacoes/Diretrizes_4-

2020_contact_tracing_covid_with_annex_en_PT.pdf>. Acesso em: 03 jun. 2020.

ESPANHA. *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Disponível em: <https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf>. Acesso em: 04 jun. 2020.

JOHNS HOPKINS UNIVERSITY. *COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU*). Coronavirus resource center. 2020. Disponível em: <https://coronavirus.jhu.edu/map.html>. Acesso em: 02 jun. 2020.

LA OMS informa de que el número de ciberataques se ha multiplicado por cinco y llama a aumentar la vigilancia. Publicado em 23 de abril de 2020. Comunicado de imprensa. Organização Mundial da Saúde. Disponível em: <https://www.who.int/es/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-v>. Acesso em: 03 jun. 2020.

PORTUGAL. **Lei n.º 58 de 8 de agosto de 2019**. Diário da República, 1ª série. Disponível em: <https://www.cnpd.pt/home/legis/nacional/Lei_58_2019.pdf>. Acesso em: 03 jun. 2020.

PORTUGAL. **Lei nº 59 de 8 de agosto de 2019**. Diário da República, 1ª série. Disponível em: <https://www.cnpd.pt/home/legis/nacional/Lei_59_2019.pdf>. Acesso em: 03 jun. 2020.

UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?uri=CELEX:32016R0679&from=EN>. Acesso em: 27 maio 2020.

OCDE. **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.** Organização para a Cooperação e Desenvolvimento Econômicos. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 01 jun. 2020.

OMS. *Actualización de la Estrategia Frente a la Covid-19.* Publicado em 14 de abril de 2020. Organização Mundial da Saúde, Genebra, Suíça. Disponível em: <https://www.who.int/docs/default-source/coronaviruse/covid-strategy-update-14april2020_es.pdf?sfvrsn=86c0929d_10>. Acesso em: 02 jun. 2020.

THE CATALAN Health System makes it available to the international community to stop the expansion of the COV-2 SARS coronavirus. The Global Connector. 27th april 2020. Disponível em: <https://echalliance.com/the-catalan-health-system-makes-it-available-to-the-international-community-to-stop-the-expansion-of-the-cov-2-sars-coronavirus/>. Acesso em: 04 jun. 2020.