RAC: revista angolana de ciências | ISSN: 2664-259X

Aplicação para o Rastreio de Contactos de Infectados por Coronavírus em Angola

Aplicación para el Seguimiento de Contactos de Infectados por Coronavirus en Angola

Application for Digital Contact Tracing of Infected by Coronavirus in Angola

Lázaro Emílio Makili
ORCID: 0000-0002-7371-1407
Doutor. Professor Auxiliar. Universidade Katyavala Bwila. Benguela, Angola
lazaro.makili@ukb.ed.ao

José Valdemiro Caseiro
ORCID: 0000-0001-8112-6024
Licenciado. Assistente Estagiário. Universidade Katyavala Bwila. Benguela, Angola
jvcaseiro@hotmail.com

Elda Jael Paulo
ORCID: 0000-0002-2982-9803
Mestre. Professor Auxiliar. Universidade Katyavala Bwila. Benguela, Angola
elda.paulo@ukb.ed.ao

Arnaldo Luciano de Jesús Domingos
ORCID: 0000-0002-8283-2470
Licenciado. Assistente Estagiário. Universidade Katyavala Bwila. Benguela, Angola
luisfrancisco19962010@gmail.com

Abílio de Jesús Epalanga Anapaz
ORCID: 0000-0002-4504-9751
Licenciado. Assistente. Universidade Katyavala Bwila. Benguela, Angola
abilio.anapaz@ukb.ed.ao

Hermenegildo José Camenhe Severino
ORCID: 0000-0002-8982-8431
Mestre. Professor Auxiliar. Universidade Katyavala Bwila. Benguela, Angola
chermejose@yahoo.com.br

DATA DA RECEPÇÃO: Julho, 2021 | **DATA DA ACEITAÇÃO**: Outubro, 2021

Resumo

Nos últimos meses a humanidade confronta-se com um enorme desafio, a propagação do novo coronavírus. O surto foi classificado como uma pandemia e as medidas para a sua contenção encontram-se no topo das prioridades. Na presença de circulação local ou comunitária do vírus resulta importante para as estratégias de controlo a reconstituição da cadeia de contactos estabelecidos durante um período determinado pelos indivíduos infectados, pelos seus contactos e, algumas vezes, pelos suspeitos de contaminação ou casos de risco. Este procedimento é complexo, tem como suporte o recurso à memória das pessoas investigadas, exigindo um esforço considerável. A tecnologia pode constituir um auxiliar importante neste domínio, abrindo-se a questão de como os dispositivos tecnológicos actuais podem auxiliar no rastreio de contactos pretendido. Com este trabalho pretende-se desenvolver uma aplicação que efectue o rastreio digital dos contactos de indivíduos infectados por coronavírus no contexto angolano, emitindo alertas para as pessoas em risco, devido à exposição por proximidade a outros indivíduos infectados. A aplicação deverá correr sobre a plataforma *Android*, tendo como base modernos recursos de programação e implementará as mais estritas normas de protecção à privacidade e aos direitos individuais, adoptando-se um modelo descentralizado, baseado no protocolo DP3T. Como resultado implementou-se um protótipo de sistema integrado por duas componentes, uma aplicação móvel e um servidor de apoio. Nos testes efectuados verificou-se que o mesmo permite executar as funcionalidades básicas pretendidas.

Palavras-chave: coronavírus; COVID-19; aplicação; contactos; pandemia

Resumen

En los últimos meses, la humanidad se enfrenta a un enorme desafío, la propagación del nuevo coronavirus. El brote fue clasificado como una pandemia y las medidas para contenerlo constituyen una prioridad. Ante la presencia de circulación local o comunitaria del virus, es importante para las estrategias de control la reconstitución de la cadena de contactos establecida durante un período determinado por los individuos infectados, por sus contactos y, en ocasiones, por los sospechosos de contaminación o casos de riesgo. Este procedimiento es complejo y se apoya en el uso de la memoria de las personas investigadas, requiriéndose un esfuerzo considerable. La tecnología puede ayudar en este dominio, abriéndose la pregunta de ¿cómo los dispositivos tecnológicos actuales pueden ayudar en el rastreo de contactos deseado? El objetivo de este trabajo es desarrollar una aplicación que realice el rastreo digital de los contactos de personas infectadas en el contexto angoleño, emitiendo alertas a personas en riesgo por exposición por proximidad a otras personas infectadas. La aplicación

debe ejecutarse en la plataforma *Android*, se basa en modernos recursos de programación e implementará los más estrictos estándares de protección de la privacidad y los derechos individuales, adoptándose un modelo descentralizado, basado en el protocolo DP3T. Como resultado, se implementó un prototipo de sistema integrado por dos componentes, una aplicación móvil y un servidor de soporte. En las pruebas realizadas, se verificó que el mismo permite la ejecución de las funcionalidades básicas deseadas.

Palabras clave: coronavirus; COVID-19; aplicación; contactos; pandemia

Abstract

In recent months, humanity is faced with an enormous challenge, the spread of the new coronavirus. The outbreak was classified as a pandemic and measures to contain it has a high priority. In the presence of local or community circulation of the virus, it is important for control strategies to reconstitute the chain of contacts established during a period determined by the infected individuals, their contacts and, sometimes, those suspected of contamination or risk cases. This procedure is complex and is supported by the use of the investigated people's memory, requiring considerable effort. Technology can be an important aid in this domain, opening up the question of how current technological devices can help in the desired contact tracing. The aim of this work is to develop an application that performs digital contact tracing of individuals infected with coronavirus in the Angolan context, issuing alerts to people at risk due to proximity exposure to other infected individuals. The application will run on the Android platform, based on modern programming resources and will implement the strictest privacy and individual rights protection standards, adopting a decentralized model, based on the DP3T protocol. As a result, a prototype of a system integrated by two components, a mobile application and a support server, was implemented. In the tests carried out, it was verified that it allows the execution of the desired basic functionalities.

Key words: coronavirus; COVID-19; application; contact tracing; pandemic

INTRODUÇÃO

A propagação do novo coronavírus tem constituído um grande desafio em termos de saúde pública à escala global, tendo sido o surto considerado como uma pandemia pela Organização Mundial da Saúde (OMS). Milhões de pessoas já resultaram infectadas até ao momento, o que tem motivado a mobilização de toda a atenção e recursos por parte dos diferentes Estados.

A estratégia de controlo da propagação do vírus, na presença de circulação local ou comunitária, passa por um processo de investigação epidemiológica ao redor das pessoas declaradas infectadas ou suspeitas de infecção, em alguns casos. Para tal, existe a necessidade de reconstituir-se a cadeia de contactos estabelecidos pelos indivíduos de interesse durante um período determinado, e também pelos seus contactos, procedimento que faz parte das acções de investigação levadas a cabo em Angola neste domínio.

O referido procedimento é complexo, dependendo essencialmente do recurso à memória das pessoas implicadas, sendo necessário elaborar um registo dos locais frequentados e das pessoas com as quais partilhou-se espaço durante um intervalo de tempo de catorze dias aproximadamente, o que é considerável. Mais ainda, as condições em que o referido exercício é requerido, marcadas pelo temor gerado pelo resultado positivo num teste ou por uma informação de suspeição, concorrem negativamente para o funcionamento adequado da memória pessoal dos indivíduos em causa.

Por outro lado, o processo de desconfinamento das pessoas e a retomada gradual da actividade económica e comercial associam-se a novos desafios neste âmbito. Uma característica deste processo é o aumento da mobilidade das pessoas, mobilidade que gradualmente tende a alcançar a escala nacional e até transfronteiriça, sendo expectável para cada indivíduo o aumento (i) da quantidade de contactos estabelecidos no período de interesse e (ii) da dispersão geográfica dos contactos estabelecidos, factores que tornam mais desafiante a investigação no domínio epidemiológico.

Estando alguns instrumentos tecnológicos actuais, como os telemóveis e *tablets*, presentes nas mais diferentes actividades desenvolvidas pela maior parte das pessoas, acompanhando-as no seu percurso durante a quase totalidade das horas do dia, os mesmos podem constituir um recurso auxiliar importante para o restabelecimento da cadeia de contactos pretendida.

Deste modo, a tecnologia pode tornar-se um factor importante neste domínio, deixando aberta a questão de como os dispositivos tecnológicos actuais, tais como os telemóveis e *tablets*, podem auxiliar no processo de rastreio necessário para o restabelecimento da cadeia de contactos pretendida.

O rastreio digital de contactos constitui uma alternativa importante, existindo a nível global um grande esforço no sentido da criação de condições para a sua implementação. Na literatura existem referências a diferentes projectos de apoio ao desenvolvimento de aplicações com este propósito, veja-se por exemplo (Troncoso, et al., 2020), (Bay, et al., 2020) ou (TCN Coalition, 2020), e a aplicações disponibilizadas por parte de diferentes países, por exemplo (Ahmed, et al., 2020) e (Martin, Karopoulos, Hernández-Ramos, Kambourakis, & Fovino, 2020).

Alinhados a esta tendência, este trabalho tem como objectivo desenvolver uma aplicação móvel, que auxilie no rastreio digital dos contactos de indivíduos infectados por coronavírus no contexto angolano, emitindo notificações de alerta para os indivíduos em risco devido à exposição por proximidade a outros indivíduos infectados.

A referida aplicação deverá correr sobre a plataforma *Android*, a qual dá suporte à maioria dos dispositivos móveis no nosso contexto, e terá como base de desenvolvimento modernos recursos disponíveis para a programação nesta plataforma. A mesma terá um carácter de adesão voluntária e não intrusivo, partilhando os dados registados exclusivamente por iniciativa do utilizador. Dessa forma, na mesma serão implementadas as mais estritas normas de protecção à privacidade e aos direitos fundamentais dos utentes.

Não obstante ser desenvolvida para *Android*, os princípios e estratégias utilizados poderão servir de base para o desenvolvimento de aplicações dirigidas a outras plataformas, como é o caso da iOS.

Este artigo espelha o esforço de desenvolvimento levado a cabo até ao momento, tendo em vista o objectivo traçado, retratando, entre outros aspectos, as principais decisões técnicas, os resultados obtidos e as dificuldades encontradas.

RASTREIO DIGITAL DE CONTACTOS

O uso da tecnologia como instrumento auxiliar na prevenção e combate à COVID – 19 é um problema emergente ao qual tem sido dedicado muita atenção nos últimos meses, pese embora haver até ao momento poucas publicações revistas por pares que tratam de estratégias para a sua implementação ou realizam análises ao redor da sua utilização.

Contudo, na imprensa, tanto comum como especializada, e em portais institucionais existem numerosos artigos que abordam o tema bem como relatos de aplicações disponibilizadas neste âmbito. Por exemplo, veja-se os artigos publicados pela ANGOP (2020), pelo Ministério da Saúde do Brasil (2020) ou por Adrian Kriesch (2020), que abordam a disponibilização de recursos tecnológicos, e por Karla Pequenino (2020) ou Joana Santos (2020), que abordam questões mais gerais acerca do assunto.

Por outro lado, começam a surgir os primeiros artigos revistos por pares, assim como *white papers* associados a projectos. Estes tratam a problemática em diferentes perspectivas tais como a revisão geral acerca das abordagens utilizadas (Ahmed, et al., 2020), (Martin, Karopoulos, Hernández-Ramos, Kambourakis, & Fovino, 2020), (Reichert, Brack, & Scheuermann, 2020), (Ming, et al., 2020), a análise da aplicabilidade e/ou aceitabilidade da introdução de recursos tecnológicos nesta área (Altmann, et al., 2020), (Walrave, Waeterloos, & Ponnet, 2020), (Jonker, et al.,

2020) ou detalhes acerca da implementação de projectos de desenvolvimento particulares (Troncoso, et al., 2020), (Bay, et al., 2020), (TCN Coalition, 2020), por exemplo.

As aplicações para plataformas móveis (*App*) constituem um segmento importante neste domínio e têm sido disponibilizadas com diferentes finalidades. As orientações respeitantes a aplicações móveis de apoio à luta contra a pandemia de COVID – 19 na perspectiva da protecção de dados, adoptada pela União Europeia (Comissão Europeia, 2020) fazem referência a diferentes funcionalidades associadas às referidas aplicações, como é o caso (i) do fornecimento de informações aos cidadãos, (ii) do controlo de sintomas e autoavaliação, (iii) do rastreio de contactos e alerta e (iv) da criação de fóruns de comunicação para médicos e pacientes em autoisolamento. Por outro lado, o Instituto Ada Lovelace refere-se num estudo (Ada Lovelace Institute, 2020) a três potenciais áreas para intervenção tecnológica: (a) aplicações de rastreio de sintomas, (b) aplicações de rastreio digital de contactos e (c) atribuição de certificados digitais de imunidade.

As aplicações de rastreio de contactos são peças de *software* para plataformas móveis que determinam quando um indivíduo esteve em contacto com outra pessoa infectada com COVID – 19 e notifica o indivíduo ou a autoridade de saúde pública para o fornecimento de orientações (Ada Lovelace Institute, 2020).

A importância deste tipo de ferramenta é reconhecida. O seu propósito é o de reduzir o número efectivo de reprodução de uma doença, no contexto de um surto epidémico, identificando os indivíduos expostos ao vírus através de uma pessoa infectada, contactando-os para que seja possível uma detecção precoce e se proporcione orientação personalizada e tratamento atempado (Bay, et al., 2020).

Ao analisar a importância deste tipo de aplicação, Servick (2020) afirma que a sua atractividade deve-se em parte ao carácter furtivo da disseminação do coronavírus, uma vez que indivíduos infectados podem transmitir o vírus durante dias antes de desenvolver qualquer sintoma e que os investigadores do sistema de saúde pública podem necessitar de outros dias mais para a identificação de um caso e a sua confirmação através de um teste. No referido artigo apresenta-se, também, uma análise crítica às expectativas geradas ao redor do uso de semelhante tecnologia, referindo-se a opiniões de diversos especialistas.

É igualmente destacável que com base em recursos tecnológicos é possível implementar estratégias de definição da população alvo para a realização de testes, através da denominada testagem inteligente. Da mesma maneira, no caso de aplicações baseadas em tecnologias de localização, é possível definir estratégias de desinfecção de locais relacionados à ocorrência de casos positivos (Hart, et al., 2020). As mencionadas estratégias podem servir de complemento às

estratégias de rastreio habitualmente utilizadas, ampliando as probabilidades de sucesso na detecção precoce de casos.

Vários países disponibilizaram aplicações de rastreio de contactos, na sua maioria desenvolvidas com o suporte dos respectivos sistemas nacionais de saúde. Como exemplos disso podem ser mencionados a Singapura, Austrália, China, Bulgária e Estónia, de entre outros. Por outro lado, existe actualmente uma corrida para o seu desenvolvimento, sendo expectável o lançamento de diferentes aplicações nos próximos dias.

A este respeito, O'Neal, Ryan-Mosley e Johnson (2020) apontam que não existe um repositório central de informação que permite a comparação entre as diferentes *Apps* e encontrar respostas para uma série de perguntas pertinentes sobre as mesmas, por exemplo quais são os dados colectados, com quem são partilhados ou como será usada a referida informação no futuro. Apontam igualmente que não existe uma abordagem padronizada seguida pelos desenvolvedores e legisladores, o que conduz a que cidadãos de diferentes países sejam confrontados com diferentes níveis de segurança e transparência.

Em função disso os referidos autores tratam de reunir numa base de dados diferentes esforços realizados a nível global no domínio do desenvolvimento de aplicações de rastreio de contactos, reunindo até ao momento referências a quarenta e sete delas, já lançadas ou em fase de desenvolvimento. Na mesma inclui-se, acerca de cada aplicação, detalhes como o que são, como funcionam e que regras e processos foram implementados nelas.

Ahmed *et al.* (2020) referem-se a dezasseis *Apps* e protocolos propostos, desenvolvidos e implantados em vários países. Os autores analisam aos mesmos, categorizando-os de acordo à arquitectura base utilizada em cada um, destacando as principais características associadas a cada *App* ou protocolo. Por outro lado, seguindo a mesma lógica, Martin *et al*. (2020) referem-se a vinte e duas *Apps* disponibilizadas por países europeus descrevendo as correspondentes características.

PRINCIPAIS ARQUITECTURAS E TECNOLOGIAS

Diferentes arquitecturas e tecnologias têm sido propostas como base para o desenvolvimento das aplicações de rastreio de contactos, havendo na literatura várias análises das suas vantagens relativas no que concerne a aspectos de segurança e privacidade (Ahmed, et al., 2020), (Reichert, Brack, & Scheuermann, 2020), (Servick, 2020), (Hart, et al., 2020).

Desde o ponto de vista da arquitectura, estas aplicações são usualmente integradas em sistemas que permitem combinar as funcionalidades executadas ao nível dos dispositivos móveis com as intervenções das autoridades reguladoras dos

sistemas de saúde pública, através do uso de servidores centrais, sendo definidos protocolos que permitem a comunicação entre os diferentes subsistemas.

As arquitecturas propostas implementam diferentes modelos de escalonamento das funcionalidades executadas numa e noutra plataforma, destacando em maior ou menor medida o papel jogado por cada componente no sistema. Entre as referidas funcionalidades encontram-se a geração das senhas partilhadas pelos dispositivos, o seu armazenamento, a realização da análise do risco de exposição entre os diferentes contactos e a emissão de notificações.

Nesta óptica, diferentes autores consideram a existência de três grandes abordagens, cada uma com as suas vantagens relativas, as arquitecturas centralizada, descentralizada e híbrida (Ahmed, et al., 2020), (Servick, 2020), (Hart, et al., 2020).

De igual forma, diferentes tecnologias têm sido referidas como potenciais para o desenvolvimento das aplicações de rastreio. Autores como Ahmed et al. (2020), O'Neill, Ryan-Mosley e Johnson (2020) ou Li e Guo (2020) mencionam várias delas, estabelecendo uma relação entre as diversas *Apps* lançadas ou protocolos desenvolvidos e as tecnologias base de suporte aos mesmos. Entre as referidas tecnologias destacam-se a de *localização*, *Bluetooth Low Energy (BLE)* e os *códigos QR*.

PRINCÍPIOS GERAIS

Um debate importante acerca das aplicações de rastreio de contactos tem a ver com o seu potencial invasivo, sendo consentâneo que o seu uso inadequado representa um perigo para a privacidade e os direitos civis dos cidadãos.

Nessa base várias instituições têm feito pronunciamentos e recomendações estabelecendo o que se deve ter em conta como boas práticas para o seu desenvolvimento e utilização. Como exemplos dessas organizações pode-se mencionar a União Americana de Liberdades Civis (ACLU, abreviatura do inglês, *American Civil Liberties Union*) (Gillmor, 2020), o Observatório para os Direitos Humanos, associado a um conjunto de mais de cem organizações (Human Rights Watch, 2020), o Instituto Ada Lovelace (2020) e a Comissão Europeia (2020).

Os diferentes países têm feito uso da sua autonomia ao adoptar aplicações do género e, por isso, os exemplos de aplicações existentes têm tido em conta as referidas recomendações em diferentes medidas.

Não obstante, o seguimento das normas de protecção à privacidade e direitos civis tem tido ampla aceitação o que tem resultado na incorporação ao processo de desenvolvimento de diversos conceitos como (i) a voluntariedade do uso das aplicações, (ii) a voluntariedade da partilha de dados com as entidades

reguladoras, (iii) a minimização dos dados colectados ou (iv) a anonimização das fichas de contacto partilhadas pelos dispositivos (Comissão Europeia, 2020), (Comité Europeu para a Proteção de Dados, 2020).

A implementação destes conceitos tem servido de princípios orientadores para o desenvolvimento de diferentes protocolos que para além dos aspectos relacionados à segurança e privacidade têm tido em vista a possibilidade de interoperatividade dos sistemas desenvolvidos em diferentes países. Neste âmbito, é notória a preferência pelos protocolos baseados em *Bluetooth* que, na opinião de diversos autores, têm sido considerados menos propensos a invasões e com maiores garantias de segurança, sendo, por isso, utilizados na maioria das aplicações referidas (Ahmed, et al., 2020), (O'Neal, Ryan-Mosley, & Johnson, 2020).

A continuação abordam-se alguns exemplos de protocolos, sendo referidos de forma particular os protocolos baseados em *Bluetooth*, pelas razões já referidas.

SUPORTE AO DESENVOLVIMENTO

Para a implementação do rastreio têm sido propostos e desenvolvidos diversos protocolos com base nas tecnologias e arquitecturas anteriormente mencionadas. Como exemplos de protocolos propostos pode-se mencionar o *BlueTrace* (Bay, et al., 2020), (OpenTrace, 2020), *Temporary Contact Numbers* (TCN) (LF Public Health, 2020), (TCN Coalition, 2020), *Decentralized Privacy-Preserving Proximity Tracing* (DP-3T) (Troncoso, et al., 2020), (DP-3T, 2020), *Google and Apple Exposure Notification* (GAEN) (Google, Inc., 2020) e o *DESIRE* (Castelluccia, et al., 2020).

Para facilitar o desenvolvimento de aplicações diversos recursos têm sido disponibilizados para uso gratuito e com código aberto, na maioria dos casos. Os mesmos têm sido referidos por várias publicações que resumem vários protocolos propostos, relacionando-os às correspondentes arquitecturas e descrevendo, igualmente, algumas aplicações desenvolvidas com base nos referidos protocolos.

Os referidos recursos podem ser enquadrados em várias categorias, tais como Interfaces de Programação de Aplicações (API, abreviatura do inglês *Application Programming Interface*) para manejo das funcionalidades incluídas nos protocolos (Ahmed, et al., 2020), (Martin, Karopoulos, Hernández-Ramos, Kambourakis, & Fovino, 2020), código de referência para o desenvolvimento de aplicações disponibilizado pelos projectos proponentes dos protocolos (DP-3T, 2020), (OpenTrace, 2020), (Google, Inc., 2020) e código de aplicações lançadas por diversos países (Covid Watch, 2020), (DP-3T, 2020), (Deutsche Telekom and SAP Deutschland, 2020).

MATERIAIS E MÉTODOS

Nesta secção faz-se uma abordagem às decisões fundamentais que servem de base ao desenvolvimento da aplicação. As referidas decisões estão relacionadas à adopção de uma arquitectura para o sistema, à escolha de um protocolo, ao desenho geral do sistema e à estratégia a utilizar para o teste da aplicação.

ARQUITECTURA E TECNOLOGIA ADOPTADAS

Actualmente emergem na literatura discussões acerca das vantagens relativas das várias arquitecturas propostas. As referidas discussões centram-se essencialmente em aspectos relacionados à preservação da segurança e privacidade dos utilizadores e nas contramedidas a adoptar para a mitigação das possíveis ameaças. Não existe um consenso generalizado quanto à preferibilidade de uma arquitectura em particular e, por conseguinte, recomendações específicas que conduzam à selecção de uma arquitectura específica, havendo desafios particulares associados a cada uma das opções. Discussões do género podem ser vistas nas referências (Ahmed, et al., 2020) e (Vaudenay, 2020), por exemplo.

No que concerne às tecnologias de base, as discussões gravitam igualmente ao redor dos aspectos de segurança e privacidade, associados a aspectos relativos ao potencial de co-localização dos utilizadores inerente a cada uma delas. Neste caso, é notória a tendência para a adopção do BLE, destacando-se por exemplo a sua utilização em 57% das *App* analisadas por Li e Guo (2020).

Com base nas observações anteriores, para o desenvolvimento desta aplicação adoptou-se uma arquitectura descentralizada baseada em BLE. Este tipo de arquitectura delega as funcionalidades fundamentais do sistema para os dispositivos móveis dos utilizadores, evitando a existência de um centro único propenso a ataques ou falhas massivos. Também permite minorar um dos grandes temores da parte dos potenciais utilizadores que tem a ver com o abuso dos dados recolhidos durante o rastreio por parte de estruturas centralizadas, tais como governos ou grandes empresas.

Por outro lado, a tecnologia baseada em BLE possui um grande potencial para o registo de contactos e a estimação da distância, sendo superior a outras como o GPS no caso de contactos de proximidade. É de considerar igualmente o facto de esta permitir em maior medida a anonimização dos dados de proximidade, sendo menos propensa a violações de privacidade.

As Figuras 1 e 2 ilustram a ideia básica subjacente ao funcionamento da arquitectura adoptada, nas perspectivas dos dois utilizadores genéricos suportados pela aplicação.

Ao estarem próximas duas pessoas, os seus dispositivos intercambiam (ou seja, enviam e recebem) de forma anónima chaves encriptadas através das suas

interfaces de *Bluetooth*. As referidas chaves, tanto as enviadas como as recebidas, são armazenadas em cada um dos dispositivos.

Ao infectar-se uma delas, uma vez confirmado com um teste, decide, voluntariamente, partilhar o seu estado, recebendo para tal uma autorização por parte da autoridade sanitária. Com essa autorização a pessoa carrega as chaves emitidas pelo seu dispositivo nos últimos 14 dias para um servidor central. Este disponibiliza para a generalidade dos utilizadores do sistema as chaves partilhadas por todos os utilizadores infectados.

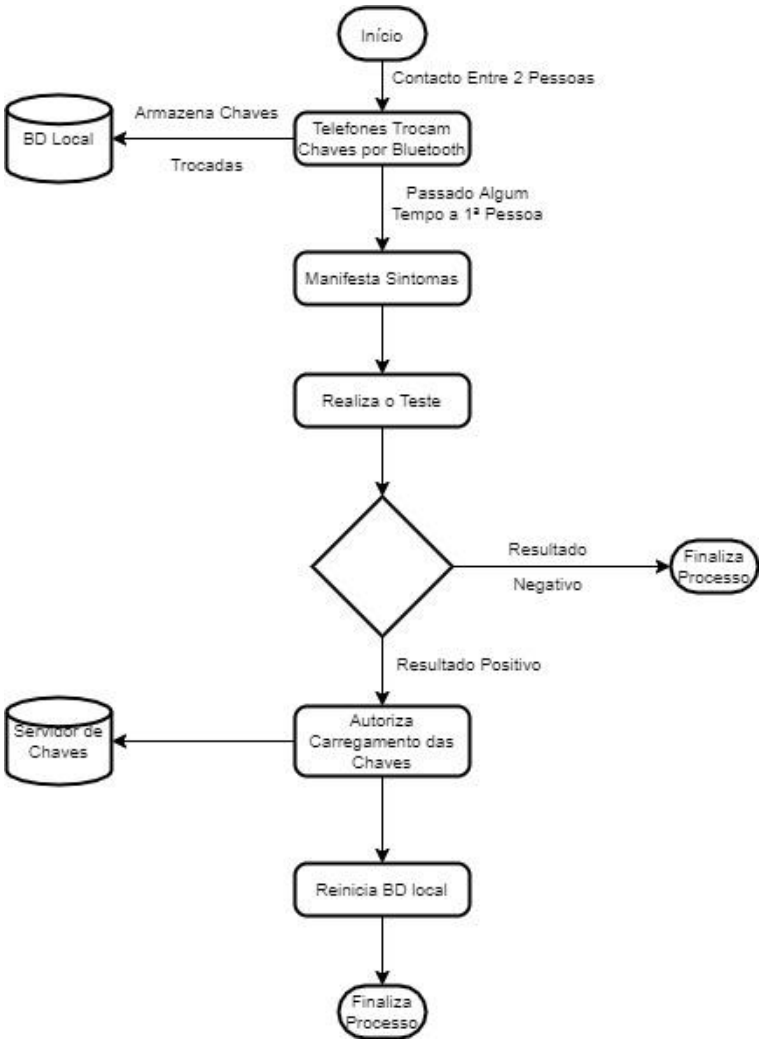

Figura 1: processo de rastreio de contactos por proximidade; perspectiva do utilizador 1

Enquanto isso, o dispositivo do segundo utilizador vai descarregando periodicamente (por exemplo, uma vez ao dia) as actualizações das chaves disponibilizadas pelo servidor central, sem ter referência alguma acerca de qual foi o dispositivo emissor. Uma vez descarregadas, o dispositivo compara as chaves com as recebidas, que se encontram armazenadas localmente, e, ao haver coincidência, calcula os índices de risco de infecção, com base no tempo de exposição e na proximidade relativamente aos contactos registados. Caso o índice

supere um valor determinado emite-se uma notificação para o utilizador com instruções sobre como proceder em função da sua exposição.

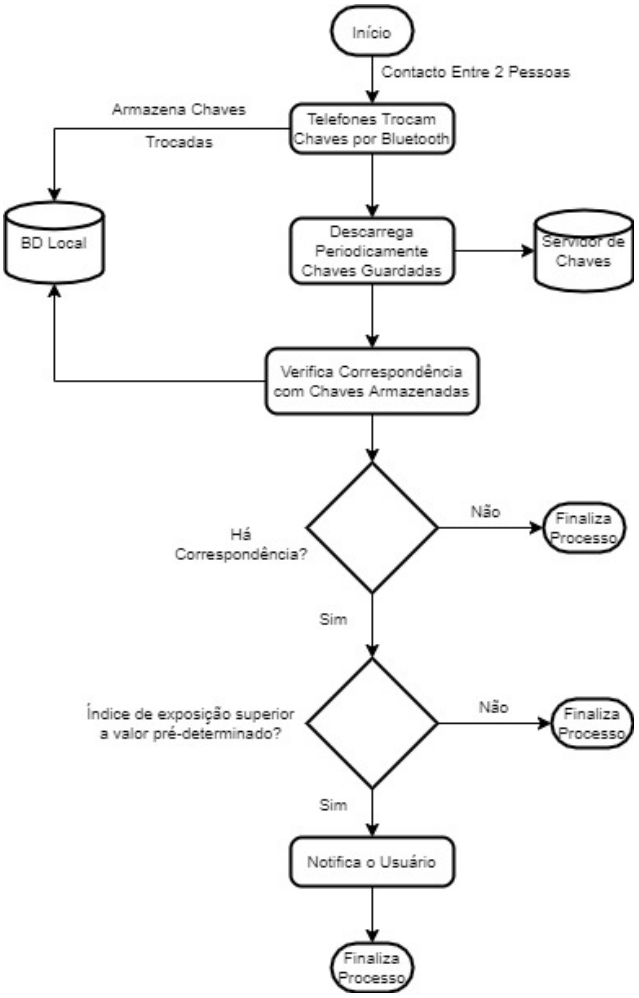

Figura 2: processo de rastreio de contactos por proximidade; perspectiva do utilizador 2

MATERIAL DE SUPORTE

Existem vários protocolos que implementam arquitecturas descentralizadas baseadas em BLE. Para a selecção de um pesam vários factores tais como a disponibilização da API para utilização livre e em formato aberto, a existência de código de referência para o auxílio ao desenvolvimento e a existência de documentação clara.

O protocolo GAEN, desenvolvido por iniciativa conjunta das multinacionais Google Inc. e Apple Inc., constitui um candidato digno de realce, estando a ocorrer nos últimos meses a migração de alguns projectos para a utilização deste.

A seu favor pende o facto de estas empresas serem as produtoras dos sistemas operativos utilizados pela maioria dos dispositivos móveis, garantindo a inclusão de

suporte ao rastreio ao nível dos sistemas operativos, o que permite melhor desempenho da aplicação no que concerne ao manejo das funcionalidades dos dispositivos implicadas no rastreio. Por outro lado, possui documentação de auxílio bem organizada e orientações de suporte ao desenvolvimento claras.

Não obstante, o código relativo às funcionalidades de rastreio é proprietário, não sendo disponibilizado de forma aberta, o que impossibilita a sua submissão e análise por escrutínio público.

A correspondente API está disponível apenas para as entidades governamentais gestoras dos Sistemas Nacionais de Saúde. Em função disso, a utilização do código, assim como o registo das aplicações derivadas nas respectivas lojas de *software*, só é possível caso se assine um convênio entre os gestores do sistema de saúde e as referidas empresas, sendo feito ao abrigo deste o licenciamento e registo dos grupos encarregados do desenvolvimento das aplicações.

Este requisito é imposto até no caso de versões de teste, facto que impossibilitou a utilização deste protocolo para o desenvolvimento do protótipo.

Como alternativa, para o desenvolvimento utilizou-se o protocolo DP-3T. Este possui igualmente uma considerável documentação de suporte e código de referência disponibilizado para utilização livre e em formato aberto. Por outro lado foi desenvolvido numa perspectiva europeia tendo por isso um forte substracto de integração e portabilidade entre sistemas desenvolvidos por diferentes países.

A correspondente API é igualmente disponibilizada para utilização livre e em formato aberto. Não obstante, as suas versões mais recentes fazem uso de algumas funcionalidades e recursos implementados pelo protocolo GAEN, o que limita o acesso pelos condicionalismos já referidos anteriormente.

Por esta razão, ao desenvolver este protótipo fez-se uso da versão 0.2.6 da API, a designada versão pré-standard, disponibilizada antes da inclusão dos recursos implementados pelo protocolo GAEN (DP-3T, 2020).

ANÁLISE E DESENHO

O sistema é composto por três peças fundamentais, uma aplicação móvel, um servidor de chaves e outro de autenticação. Na Figura 3 apresenta-se o diagrama de componentes que ilustra o relacionamento estabelecido entre os mesmos.

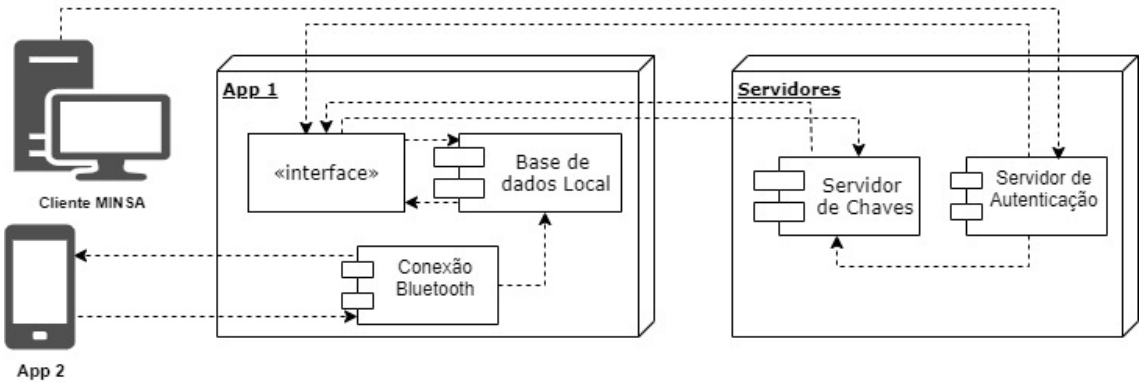

Figura 3: diagrama de componentes do sistema

Na arquitectura adoptada as funcionalidades fundamentais são implementadas ao nível da aplicação móvel. Destacam-se entre as referidas funcionalidades:

- Geração das chaves aleatórias.
- Manejo da emissão e recepção de chaves através da interface de BLE.
- Armazenamento local das chaves partilhadas e submissão das mesmas para o servidor, quando necessário.
- Pesquisa e descarga periódicas de chaves disponibilizadas pelo servidor.
- Cálculo dos índices de exposição dos usuários.
- Emissão de notificações para os utilizadores, caso o índice de exposição seja superior a um nível determinado.

Os servidores são utilizados como mecanismos de suporte ao funcionamento do sistema. O servidor de chaves é utilizado como plataforma de comunicação entre as aplicações instaladas em diferentes dispositivos móveis, permitindo o intercâmbio das chaves correspondentes aos utilizadores infectados. O servidor de autenticação é gerido pela autoridade de saúde e serve de mecanismo de controlo durante o processo de carregamento das chaves para o servidor, de forma tal que este acto possa ser levado a cabo apenas por utilizadores autorizados e com testes positivos confirmados. As principais funcionalidades implementadas nos referidos servidores são descritas a continuação.

Servidor de chaves:

- Armazenamento das chaves disponibilizadas pelos utilizadores diagnosticados positivamente.
- Distribuição das chaves com diagnóstico confirmado para os dispositivos móveis.

Servidor de autenticação:

- Geração de códigos de verificação e disponibilização aos utilizadores que pretendem carregar as suas chaves para o servidor.
- Fornecimento ao servidor de chaves de códigos de autenticação válidos para carregamento dos dados.

METODOLOGIA DE TESTE

O teste efectuado tem como objectivo a verificação da execução das funcionalidades essenciais do Sistema durante um ciclo de execução.

O mesmo consiste, primeiro, em observar as alterações ocorridas nos registos do estado interno da aplicação. Através destes pode-se controlar a quantidade de chaves partilhadas, o estado da emissão e recepção das chaves e da notificação como exposto à infecção ou não, por exemplo.

Em segundo lugar, realizar simulações do processo de comunicação com o servidor de chaves e emissão de notificações por parte da aplicação. Para tal, declara-se uma infecção a partir de um dos dispositivos e carrega-se os correspondentes dados para o servidor de chaves. Os demais dispositivos descarregam os dados a partir do servidor e faz-se a observação das alterações ocorridas nos estados das correspondentes aplicações.

RESULTADOS

Como resultado do trabalho, desenvolveu-se um protótipo do sistema o qual integra funcionalidades associadas à aplicação móvel e ao servidor de chaves.

A aplicação móvel corre em ambiente *Android*, tendo sido testada na sua versão 10.0. Desenvolveu-se para a mesma uma interface e para o rastreio usou-se o protocolo DP3T, recorrendo-se à versão pré-standard, 0.2.6, da correspondente biblioteca. A Figura 4 mostra o ecrã principal da referida interface.

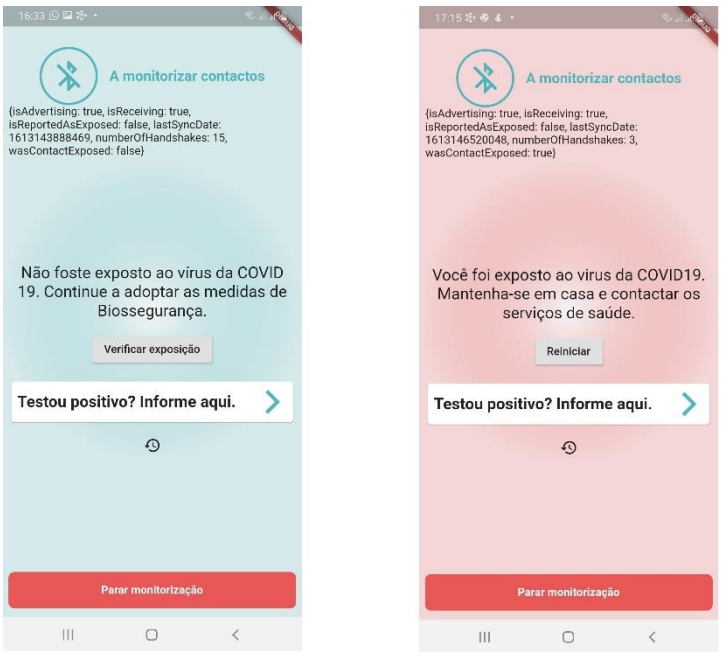

Figura 4: ecrã principal da aplicação. À esquerda: em funcionamento normal; à direita: após a recepção de uma notificação de risco de contágio

Para o armazenamento das chaves emitidas pelos utilizadores diagnosticados positivamente utilizou-se um servidor baseado na nuvem, o que facilita a sua disponibilidade. Na sua programação usou-se o *framework* Laravel e a linguagem PHP nas suas versões 8.0 e 7.2, respectivamente.

Realizou-se um teste em pequena escala, com um conjunto de quatro dispositivos móveis de diferentes marcas e modelos, usando todos a versão 10.0 do sistema operativo *Android*. Nestes, verificou-se o funcionamento de um ciclo básico de execução do sistema, desde a geração e partilha de chaves até à emissão de notificações para o utilizador, passando pela carga e descarga de dados para o servidor, tendo decorrido todo o processo de forma regular.

DISCUSSÃO

A documentação de referência para o desenvolvimento de aplicações, por exemplo a disponibilizada pela Google (Google, Inc., 2021) e pelo projecto Corona Warn (Deutsche Telekom AG and SAP SE, 2021), menciona a três componentes fundamentais dos sistemas de rastreio de contactos. O protótipo desenvolvido integra duas dessas componentes, a aplicação móvel e o servidor de chaves, não tendo sido implementadas, ainda, as funcionalidades relativas à terceira componente, o servidor de autenticação.

Das funcionalidades previstas nas referidas fontes para a aplicação móvel foram executadas as básicas, tais como a geração, intercâmbio e armazenamento das chaves via BLE. Outras funcionalidades, como a carga descarga de dados do servidor de chaves, foram implementadas de forma a serem despoletadas por

iniciativa do utilizador, deixando-se para uma fase posterior do desenvolvimento a sua automatização.

Como núcleo do sistema usou-se uma versão relativamente antiga da API DP3T (DP-3T, 2020). Isto deveu-se a que as versões mais recentes desta fazem recurso a funções disponibilizadas pela iniciativa conjunta da Google, Inc. e Apple, Inc. cujo acesso é limitado às equipas de desenvolvimento autorizadas pelos Sistemas Nacionais de Saúde, mediante protocolo estabelecido com as referidas empresas (Apple, Inc., 2021).

Este facto constitui um factor limitativo no caso desta equipa, não sendo possível usar versões mais actualizadas da API, versões nas quais eventualmente terão sido implementadas diversas inovações e correcções ao protocolo, relativamente à utilizada neste caso.

No protótipo, implementou-se igualmente as funcionalidades associadas ao servidor de chaves consideradas essenciais, de entre as descritas na documentação de referência (Google, Inc., 2021), (Deutsche Telekom AG and SAP SE, 2021). A recepção/disponibilização de chaves pelo servidor é feita por demanda directa da aplicação móvel, sendo, em ambos os casos, o processo despoletado por uma intervenção do utilizador. O referido servidor foi usado apenas como mecanismo de partilha e sincronização de dados entre os diferentes utilizadores do sistema. Até ao momento não foram implementadas no mesmo outras funcionalidades, tais como a automatização da geração e disponibilização de ficheiros de actualização, a limpeza das chaves antigas e os mecanismos de segurança de acesso.

Durante o teste, a aplicação foi instalada e executada com sucesso em todos os dispositivos utilizados, sendo possível a aferição da execução do ciclo básico de funcionamento do sistema.

Verificou-se a actividade de registo da partilha de chaves em três dos dispositivos, não sendo a mesma observada num deles. Não foi possível identificar as razões que estão na base desta falha, podendo estas estar associadas ao dispositivo em questão ou à programação do protocolo ou da aplicação. A actualização da biblioteca de sistema utilizada constitui, desde o ponto de vista dos autores, a primeira alternativa na tentativa de solução do problema, sendo considerada entre os próximos passos no processo de desenvolvimento. Por outro lado, a realização de testes com uma maior quantidade de dispositivos ajudaria a aferir se se trata de uma falha do dispositivo.

CONCLUSÕES

Neste artigo apresenta-se o esforço de desenvolvimento, para o contexto angolano, de uma aplicação de rastreio de contactos de indivíduos infectados pela COVID – 19.

Desenvolveu-se um protótipo de sistema, integrado por uma aplicação móvel e um servidor de chaves, no qual foram implementadas funcionalidades básicas que permitem a execução de um ciclo do funcionamento do sistema.

A aplicação móvel corre sobre ambiente *Android*, tendo sido testada na versão 10.0. Para o desenvolvimento da aplicação utilizou-se o protocolo DP3T, sendo usada a versão pré-standard, 0.2.6, da API.

Para implementação do servidor de chaves usou-se o *framework* Laravel e a linguagem PHP, nas suas versões 8.0 e 7.2, respectivamente.

O teste efectuado, com quatro dispositivos, permitiu verificar o funcionamento da aplicação, através da sua execução por um ciclo completo.

Como principais dificuldades associadas ao desenvolvimento aponta-se, por um lado, a falta de um acordo que permita o acesso desta equipa a versões mais actuais das APIs disponibilizadas para protocolos bem documentados, como é o caso do DP3T e GAEN, acesso que poderia constituir uma mais-valia para o processo de desenvolvimento e para a fiabilidade do sistema a obter.

Por outro lado, é de ressaltar a exiguidade em termos de dispositivos móveis para o teste da aplicação, o que fez com que este fosse realizado com uma quantidade limitada de dispositivos, em termos de marcas e versões do sistema operativo.

Como passos para o futuro considera-se o aprimoramento do protótipo no sentido da implementação de funcionalidades relativas ao serviço de autenticação do carregamento de chaves para o servidor, a automatização da pesquisa de actualizações das chaves disponibilizadas pelo servidor, por parte da aplicação móvel, e a automatização da gestão das chaves armazenadas no servidor de chaves.

Também, considera-se a realização de um teste em maior escala, com maior abrangência e diversidade em termos de marcas, modelos e versões dos sistemas operativos dos dispositivos móveis.

AGRADECIMENTOS

Os autores expressam os seus sinceros agradecimentos ao Dr. Albano Ferreira e ao Eng. Abdul Santos, entidades que desde o primeiro momento deram o seu apoio incondicional abrindo caminhos na busca de parcerias que pudessem potenciar ao projecto. Aos mesmos o nosso muito obrigado.

REFERÊNCIAS

Ada Lovelace Institute. (2020). *Exit through the App Store? A rapid evidence review of the technical considerations and societal implications of using technology to transition from the COVID-19 crisis.* London: Ada Lovelace Institute. Obtido de https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-app-store/

Ahmed, N., Michelin, R., Xue, W., Ruj, S., Malaney, R., Kanhere, S., . . . Jha, S. (2020). A Survey of COVID-19 Contact Tracing Apps. *IEEE Access, 8*, 134577 - 134601. doi:10.1109/ACCESS.2020.3010226

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., . . . Abeler, J. (2020). Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study. *JMIR mHealth uHealth, 8(8): e19857*. doi:10.2196/19857

ANGOP. (8 de Abril de 2020). COVID-19: Estudante cria aplicativo de autodiagnóstico. *Portal ANGOP*. Obtido de www.portalangop.co.ao

Apple and Google. (2020). *Exposure Notifications: Using technology to help public health authorities fight COVID-19*. (Google) Obtido em 21 de Novembro de 2020, de COVID - 19 Infromation & Resources: https://www.google.com/covid19/exposurenotifications/

Apple, Inc. (2021). *Exposure Notification APIs Addendum.* Obtido em 13 de 10 de 2021, de Apple Developer: https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf

Bay, J., Kek, J., Tan, A., Hau, C. S., Yongquan, L., Tan, J., & Quy, T. A. (2020). BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *White Paper*. Obtido de https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

Castelluccia, C., Bielova, N., Boutet, A., Cunche, M., Lauradoux, C., Métayer, D., & Roca, V. (2020). *Desire: A third way for a european exposure notification system leveraging the best of centralized and decentralized systems.* hal-02570382 . Obtido de https://hal.inria.fr/hal-02570382/document

Comissão Europeia. (17 de Abril de 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*. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN

Comité Europeu para a Proteção de Dados. (21 de Abril de 2020). *Diretrizes 4/2020 sobre a utilização de dados de localização e meios de rastreio de contactos no contexto do surto de COVID-19.* Obtido de Portal Comité Europeu para a Proteção de Dados: https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_pt

Covid Watch. (2020). *Covid Watch*. (GitHub, Inc) Obtido em 21 de Novembro de 2020, de https://github.com/covidwatchorg

Deutsche Telekom AG and SAP SE. (2021). *Documentation*. Obtido em 13 de 10 de 2021, de Corona Warn App: https://github.com/corona-warn-app/cwa-documentation

Deutsche Telekom and SAP Deutschland. (2020). *Corona-Warn-App*. (GitHub, Inc) Obtido em 21 de Novembro de 2020, de https://github.com/corona-warn-app

DP-3T. (2020). *DP-3T/dp3t-android-ch*. (GitHub, Inc) Obtido em 21 de Novembro de 2020, de https://github.com/DP-3T/dp3t-app-android-ch

DP-3T. (2020). *DP^3T Decentralized Privacy-Preserving Proximity Tracing*. (The GitHub, Inc) Obtido em 20 de Novembro de 2020, de https://github.com/DP-3T

DP-3T. (2020). *DP3T SDK for Android*. (GitHub, Inc.) Obtido em 20 de Novembro de 2020, de https://github.com/DP-3T/dp3t-sdk-android/tree/prestandard

Gillmor, D. K. (2020). *ACLU Principles for Technology-Assisted Contact-Tracing.* ACLU. Obtido de https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing

Google, Inc. (2020). *Google/exposure-notifications-server*. (GitHub, Inc) Obtido em 21 de Novembro de 2020, de https://github.com/google/exposure-notifications-server

Google, Inc. (3 de 6 de 2021). *Exposure Notifications API*. Obtido em 13 de 10 de 2021, de Google API for Exposure Notifications: https://developers.google.com/android/exposure-notifications/exposure-notifications-api#architecture

Hart, V., Siddarth, D., Cantrell, B., Tretikov, L., Eckersley, P., Langford, J., . . . Weyl, G. (2020). *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks.* Harvard: Edmond J. Safra Center for Ethics - Harvard University. Obtido de https://ethics.harvard.edu/outpacing-virus

Human Rights Watch. (2 de April de 2020). *Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights*. Obtido de Human Rights Watch Portal: https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight

Jonker, M., de Bekker-Grob, E., Veldwijk, J., Goossens, L., Bour, S., & Rutten-Van Mölken, M. (2020). COVID-19 Contact Tracing Apps: Predicted Uptake in the Netherlands Based on a Discrete Choice Experiment. *JMIR Mhealth Uhealth, 8(10): e20741*. doi:10.2196/20741

Kriesch, A. (15 de Maio de 2020). Covid-19: África do Sul cria app que rastreia o vírus. *SAPO Notícias*. Obtido de https://noticias.sapo.ao/tecnologia/artigos/covid-19-africa-do-sul-cria-app-que-rastreia-o-virus

LF Public Health. (2020). *TCN Coalition and LFPH have merged*. (The Linux Foundation) Obtido em 20 de Novembro de 2020, de https://www.lfph.io/tcn-coalition/

Li, J., & Guo, X. (2020). *Covid-19 contact-tracing apps: a survey on the global deployment and challenges.* Obtido em 17 de 11 de 2020, de https://arxiv.org/abs/2005.03599

Martin, T., Karopoulos, G., Hernández-Ramos, J. L., Kambourakis, G., & Fovino, I. N. (2020). Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps. *Wireless Communications and Mobile Computing, 2020*(Article ID 8851429). doi:https://doi.org/10.1155/2020/8851429

Ming, L. C., Untong, N., Aliudin, N. A., Osili, N., Kifli, N., Tan, C. S., . . . Goh, H. P. (2020). Mobile Health Apps on COVID-19 Launched in the Early Days of the Pandemic: Content Analysis and Review. *JMIR Mhealth Uhealth, 8(9): e19796*. doi:10.2196/19796

Ministério da Saúde de Portugal. (2020). *StayAway Covid*. (INESC TEC) Obtido em 21 de Novembro de 2020, de https://stayawaycovid.pt/

Ministério da Saúde do Brasil. (31 de Março de 2020). *Aplicativo Coronavírus SUS agora envia mensagens de alertas aos usuários*. Obtido em 27 de Maio de 2020, de Ministério da Saúde: https://www.saude.gov.br/noticias/agencia-saude/46628-aplicativo-coronavirus-sus-agora-envia-mensagens-de-alertas-aos-usuarios

O'Neal, P. H., Ryan-Mosley, T., & Johnson, B. (19 de Novembro de 2020). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. Obtido de https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

OpenTrace. (2020). *OpenTrace*. (GitHub, Inc) Obtido em 20 de Novembro de 2020, de https://github.com/opentrace-community

Pequenino, K. (16 de Abril de 2020). "Apps" para monitorizar covid-19 na EU não podem revelar identidade dos doentes. *Público*. Obtido de https://www.publico.pt/2020/04/16/tecnologia/noticia/apps-monitorizar-covid19-ue-nao-podem-revelar-identidade-doentes-1912599

Reichert, L., Brack, S., & Scheuermann, B. (2020). *A Survey of Automatic Contact Tracing Approaches Using Bluetooth Low Energy*. Cryptology ePrint Archive. Obtido de https://eprint.iacr.org/2020/672

Santos, J. R. (29 de Abril de 2020). Covid-19. Como vai funcionar a app de rastreamento de contactos em Portugal? *RTP Notícias*. Obtido de https://www.rtp.pt/noticias/pais/covid-19-como-vai-funcionar-a-app-de-rastreamento-de-contactos-em-portugal_es1224356

Servick, K. (21 de Maio de 2020). COVID - 19 contact tracing apps are coming to a phone near you. How will we know whether they work? *Science*. Obtido de https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how

TCN Coalition. (2020). *TCN Protocol*. (GitHub, Inc) Obtido em 20 de Novembro de 2020, de https://github.com/TCNCoalition/TCN

Troncoso, C., Payer, M., Hubaux, J.-P., Salathé, M., Larus, J., Bugnion, E., . . . Wiegand, T. (2020). Decentralized Privacy-Preserving Proximity Tracing. *White Paper*.

Vaudenay, S. (2020). *Centralized or decentralized? The contact tracing dilemma.* Cryptology ePrint Archive: Report 2020/531. Obtido de http://eprint.iacr.org/2020/531

Walrave, M., Waeterloos, C., & Ponnet, K. (2020). Adoption of a Contact Tracing App for Containing COVID-19: A Health Belief Model Approach. *JMIR Public Health and Surveillance, 6(3):e20572*.