

RASTREAMENTO DE CONTACTOS

Princípios para uma aplicação Nacional

v1.0 – 13 de Maio de 2020

Índice

Índice	2
Privacidade de raiz, e não uma questão de confiança	9
Vulnerabilidades e segurança	10
Sobre a eficácia do rastreamento de contactos digital	12
Literacia digital, maximizar a inclusão e visar o benefício de todos	16
Princípios para uma aplicação nacional	18
Ser eficaz para o propósito a que se propõe	18
Preservar a privacidade dos dados dos cidadãos	19
Ser robusta em termos de segurança	19
Ser escrutinável, aberta e passível de análise pública	20
Alcançar toda a população	21
Ser Integrada com os esforços nacionais de rastreamento de contatos, teste de diagnóstico e monitorização da COVID-19	21
Conjugar numa aplicação única funcionalidades complementares para controlo epidémico	22
Conclusões	23
Autoria	25
Referências	26

Introdução

O objetivo deste documento é **oferecer uma descrição acessível e rigorosa do rastreamento de contactos digital**, através de aplicações móveis, bem como clarificar questões do seu potencial impacto na privacidade dos cidadãos. Adicionalmente, são explorados aspectos relacionados com a sua eficácia, assim como aspectos de inclusão e literacia digital. Por fim, são apresentados **princípios orientadores** para o desenvolvimento de uma aplicação de rastreamento de contactos nacional, tendo em conta as várias questões examinadas ao longo do documento.

A propósito da luta contra a pandemia COVID-19, iniciou-se recentemente uma discussão difícil sobre o uso de aplicações móveis para esse fim. Nomeadamente sobre o uso de aplicações para fazer rastreamento de contactos (contact tracing) para que se possa conter as cadeias de transmissão de forma mais eficiente.



A discussão não se tem focado tanto na possível utilidade e funções de uma aplicação digital, sendo alimentada sobretudo pela, mais do que justificável, preocupação com eventuais riscos que ameaçam a privacidade dos cidadãos, e com a utilização dos seus dados para outros fins, ameaçando um direito consagrado na constituição portuguesa (art. 26, nº 1) [constpt26-1] e União Europeia [echr2012].

Esta discussão tem no entanto partido muitas vezes de premissas falsas: no epicentro das preocupações está a suposta inevitabilidade de haver um rastreamento dos dados de localização e movimentos dos cidadãos, bem como informação detalhada da sua saúde, pelo governo ou entidade que o represente; e a premissa de que só resta aos cidadãos confiar que não se utilizem estes dados para propósitos diferentes.

Estas premissas estão erradas pois existem formas descentralizadas de rastreamento de contactos que não colocam os dados dos cidadãos nas mãos de terceiros, não permitindo assim sequer a possibilidade de utilização desses dados para outros fins. E é assim que deve ser. Se para aplicações deste nível de sensibilidade, o cidadão tiver que confiar no governo ou outras instituições oficiais para não abusar dos seus dados, já se está a ir pelo caminho errado. Adicionalmente, as abordagens descentralizadas baseiam-se em detecção de proximidade, e não precisam da informação de geolocalização (Wi-fi ou GPS).

O conceito de rastreamento de contactos (manual) existe há longa data e é utilizado em grande parte do mundo.

O conceito de rastreamento de contactos (manual) existe há longa data e é utilizado em grande parte do mundo. Quando se descobre que alguém é positivo para uma infecção/doença, de epidemiologia relevante, as autoridades da saúde entrevistam a pessoa para fazer um levantamento de todos os contactos que a pessoa teve recentemente. Deste modo, é assegurado que estas pessoas são informadas para que possam tomar medidas e, mesmo que não apresentem sintomas, possam evitar que a infecção seja transmitida a um grupo mais alargado.

No contexto da pandemia que nos aflige hoje, alguns países asiáticos (China, Coreia do Sul, Taiwan, Singapura) utilizaram este conceito e

informatizaram-no, sob a forma de aplicações digitais. Infelizmente, algumas destas *apps* não foram implementadas com a privacidade em mente, e acabaram por descredibilizar o conceito de rastreamento de contactos (digital). Em alguns casos recolhiam dados geolocalizados, ou a matriz de contactos com casos positivos era processada centralmente, de uma forma que não protegia a identidade dos cidadãos.

Outras soluções usam Bluetooth para registar contactos com pessoas na proximidade, permitindo rastrear de forma mais eficiente os contactos tidos por casos positivos. Um exemplo disso é o projecto BlueTrace de Singapura.

Entretanto, na Europa e nos EUA, vários grupos iniciaram trabalho em versões de rastreamento de proximidade com maior ênfase na privacidade, alguns deles resultantes da fusão de projectos individuais. Entre os vários grupos Europeus destacam-se o PEPP-PT (Pan-European Privacy Preserving - Proximity Tracing), um grupo de académicos de várias universidades europeias; o DP-3T, também iniciado por académicos, que estando inicialmente integrados no PEPP-PT, saíram [tech0417] para defender uma abordagem descentralizada, mais exigente no que toca a privacidade dos dados. Entretanto a Google e a Apple avançaram com uma solução própria, inspirada no modelo DP-3T, e que será, tudo indica, a base de aplicações que sigam este modelo, uma vez que garantem o bom funcionamento num vasto grupo de *Smartphones* dos sistemas operativos Android e iOS. Há várias outras iniciativas relevantes também baseadas num modelo descentralizado: a TCN Coalition, um grupo de instituições americanas e europeias, das quais fazem parte os projetos CovidWatch, CoEpi e a Universidade Técnica de Munique; o PACT (Privacy Automated Contact Tracing, também conhecido como East Coast PACT), liderada pelas universidades norte-americanas MIT, ACLU, Brown, BU, e Weizmann Institute; e o Privacy-Sensitive Protocols and Mechanisms for Mobile Contact Tracing (também conhecida por West Coast PACT), do qual fazem parte da Universidade de Washington, a Universidade da Pennsylvania e a Microsoft.

Em Portugal sabe-se que está em curso o desenvolvimento de uma app/plataforma denominada de StayAway pelo INESC TEC, e existe ainda uma solução proprietária da empresa Hype Labs. Ainda não se sabem todos os detalhes sobre estas aplicações. Aguarda-se também mais detalhes por parte do governo em relação à futura plataforma.





De seguida será feita uma descrição simplificada e clara do funcionamento do rastreamento de contactos digital, após a qual serão analisados aspectos de privacidade e segurança. Posteriormente, é apresentada uma reflexão sobre aspectos de eficácia da técnica e sobre inclusão e literacia digital. Por fim, são apresentados princípios orientadores para o desenvolvimento e operação de uma aplicação de rastreamento de contactos digital para Portugal.

Funcionamento do rastreamento de contactos digital

As aplicações de rastreamento de contactos digitais permitem detectar via Bluetooth a proximidade de outros *Smartphones* com a mesma aplicação ativa, e trocam com estes senhas aleatórias que são únicas, geradas de forma a garantir que não podem ser facilmente forjadas, e que são efémeras, sendo alteradas ao fim de uns minutos. As senhas escutadas são guardadas por cada *Smartphone* juntamente com a data, duração do contacto e uma estimativa da proximidade mínima com esse contacto. A toda esta informação chamamos, no contexto destas aplicações, de *Contacto*. Mais nenhuma informação é trocada, não havendo qualquer partilha de informação que identifique os intervenientes, os seus *Smartphones* ou o local onde aconteceu o contacto.

Em propostas de rastreamento de contactos descentralizadas ([DP-3T](#), [Apple+Google](#), [TCN Coalition](#), [East](#) e [West](#) Coast PACT), a informação dos *Contactos* nunca sai dos *Smartphones*. As propostas assentes num modelo centralizado (PEPP-PT, BlueTrace) não protegem tanto a privacidade e enviam parte ou a totalidade dos *Contactos* para um servidor central onde se reúne a matriz de contactos de todos os utilizadores, para calcular o risco de cada contacto e notificar, a partir daí, os envolvidos. Esse modelo é potencialmente perigoso em termos da salvaguarda da privacidade dos utilizadores, algo absolutamente desnecessário.

Propostas Internacionais:

	 Google			
DP-3PT	Apple+google	TCN coalition	East Pact	West Pact

As soluções descentralizadas, consideradas mais seguras, calculam o risco de cada contacto directamente nos telemóveis. Para tal, permitem aos utilizadores diagnosticados com COVID-19, e sempre com o seu consentimento, comunicar as suas senhas dos últimos 14 dias às aplicações dos outros utilizadores, permitindo localmente no *Smartphone* verificar se houve algum contacto de risco de relevância médica (determinado através da proximidade e tempo de exposição). Esta comunicação é feita através de um servidor central, que com base na informação recebida não tem forma de perceber a matriz de contactos, ou seja, as senhas de cada utilizador que contactou o caso positivo nunca saem do *Smartphone* deste último, nem as senhas deste último saem dos *Smartphones* dos utilizadores que se cruzaram com o caso positivo.

Se o risco de contágio for relevante, a própria aplicação emite uma recomendação ao utilizador, podendo esta ser a de se isolar imediatamente, contactar os serviços de saúde, sugerir que faça um teste diagnóstico, ou outra medida que as autoridades venham a considerar mais eficazes na contenção do vírus.

O utilizador não necessita de ter acesso aos detalhes dos contactos tidos, como o dia em que este ocorreu ou quanto tempo esteve em contacto com o caso positivo. Tudo depende da fórmula de cálculo de risco. Se esta determinar que o risco é relevante, a App emite uma notificação mais, ou menos, genérica ao utilizador. Caso contrário, não há qualquer notificação.

O modelo DP-3T prevê já, sempre com o consentimento expresso do utilizador, a partilha anónima de informação de contactos com infectados com instituições saúde pública e centros de investigação epidemiológica, sem a identificação dos utilizadores. Estes centros poderão trabalhar modelos de propagação da doença que permitam identificar prováveis casos assintomáticos e desta forma conseguir complementar a informação da rede de saúde.

Algumas destas soluções prevêem ainda que o servidor central envie para cada uma das aplicações alterações à fórmula de risco por forma a calibrar as mesmas e adequá-las a avanços no entendimento epidemiológico da infecção.

Privacidade de raíz, e não uma questão de confiança

Estas soluções tecnológicas, quando implementadas de forma a preservar a privacidade, não permitem a utilização de dados para outros fins, pois em nenhum momento a informação de contactos, ou dados identificativos, é enviada para o governo ou entidade que o represente. Apenas são trocadas senhas que não têm qualquer significado e que são sempre guardadas localmente, no *Smartphone* do utilizador. O cruzamento de dados, mesmo sendo codificado ou pseudo-anonimizado, é sempre feito de forma descentralizada, localmente no *Smartphone* do utilizador. As pessoas são notificadas, quando for caso disso, pela própria aplicação a correr no seu *Smartphone*. Não há necessidade de qualquer partilha do contacto telefónico, morada, ou identidade da pessoa, e muito menos, coordenadas geolocalizadas, ou seja, o percurso ou localização das pessoas.



Estas medidas no desenho de raíz destas soluções colocam o cidadão numa situação de maior conforto, pois sabe que o próprio funcionamento da aplicação não possibilita o abuso dos dados, não tendo assim que confiar que seja respeitada a finalidade a que estes se destinam. No entanto, o potencial benefício no combate à pandemia está igualmente presente. Não sendo necessário ao utilizador abdicar da sua privacidade.

Vulnerabilidades e segurança

A solução ideal é, como referido acima, descentralizada e anónima. Mas será que mesmo assim é possível deduzir a identidade das pessoas em certas situações? Sim, em casos muito particulares. Por exemplo, se só esteve com uma pessoa nos últimos 15 dias, ambas utilizam a aplicação, e de repente é notificado para se isolar, isso revela que a outra pessoa foi diagnosticada com COVID-19. A este processo, que consiste em reverter a anonimização de dados com recurso a informação obtida externamente, chama-se deanonimização. No exemplo dado, a notificação automaticamente revela quem terá sido diagnosticado por exclusão de partes.

Uma defesa que é possível utilizar é introduzir mais informação por forma a não se conseguir fazer a reversão da anonimização. Numa aplicação que inclua outras abordagens para além do rastreamento de contactos, como o rastreamento de sintomas e estado de confinamento, aliado a informação de saúde na região, uma notificação pode provir de qualquer uma destas abordagens, sem deixar claro ao utilizador qual delas a originou. O rastreamento de sintomas pode gerar notificações relacionadas com os sintomas introduzidos directamente pelo utilizador, ou com base em estudos longitudinais/aleatórios da população, em que o teste pode ser aconselhado por amostragem e/ou em função da região julgada de risco. Com todas estas possibilidades, não seria evidente qual a origem da notificação, criando o benefício da dúvida. Estes são exemplos de como se pode combater a deanonimização num contexto integrado e útil.

Outra questão frequentemente levantada é a possibilidade de utilizadores declararem o estado de infectados sem realmente o estarem, provocando uma onda de isolamentos desnecessários e consequente descrédito do sistema. Esta situação em particular foi já amplamente discutida e muitas destas soluções prevêm que o utilizador apenas se possa declarar SARS-CoV2-Positivo se foi efectivamente testado e/ou se um médico formalmente autorizar esta situação. Recomenda-se no entanto cuidado na

análise de como este mecanismo é implementado, para garantir que se protege a identidade do utilizador.

É necessário também garantir que estas aplicações não criam o que em cibersegurança se chamam canais laterais (*side-channels*). Este tipo de vulnerabilidade ocorre quando apesar da confidencialidade utilizada num canal de comunicações, é ainda assim possível deduzir o que está a ser transmitido através da análise da informação disponível e do conhecimento de como funciona a aplicação. Por exemplo, através da simples observação, da parte de um atacante, da quantidade de tráfego emitido pela aplicação, que, apesar de cifrado, pode revelar a ação que está a ser executada pela App. Uma transmissão de uma certa duração e com determinadas características pode denunciar que um utilizador se encontra a transmitir o estado de infeção ao sistema. No enquadramento do DP-3T já se implementam medidas para impedir este tipo de ataques com recurso a análise de tráfego. Existem outros exemplos relacionados com tempos de resposta, ou com a utilização da memória no *smartphone*. Para garantir que este tipo de ataque não é possível é necessário uma análise cuidada da aplicação por parte de especialistas de segurança.

Sobre a eficácia do rastreamento de contactos digital

A grande proposta de valor deste tipo de aplicações é a notificação automática e recomendação mais rápida de isolamento e teste de potenciais infectados. Isso mesmo é sugerido num [artigo recente da revista Science Magazine](#) [Ferreti2020], que se refere às Apps Chinesa e Sul Coreana como exemplos de sucesso na supressão da doença. De 2 a 23 de Março a China reportou de forma sustentada menos do que 150 novos casos por dia, quando no pique da pandemia eram milhares por dia. Mas quanto dessa redução se deveu especificamente ao rastreamento de contactos digital?

RESEARCH ARTICLE

Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing

Luca Ferretti^{1,*}, Chris Wymant^{1,*}, Michelle Kendall¹, Lele Zhao¹, Anel Nurtay¹, Lucie Abeler-Dörner¹, Michael Parker², David...

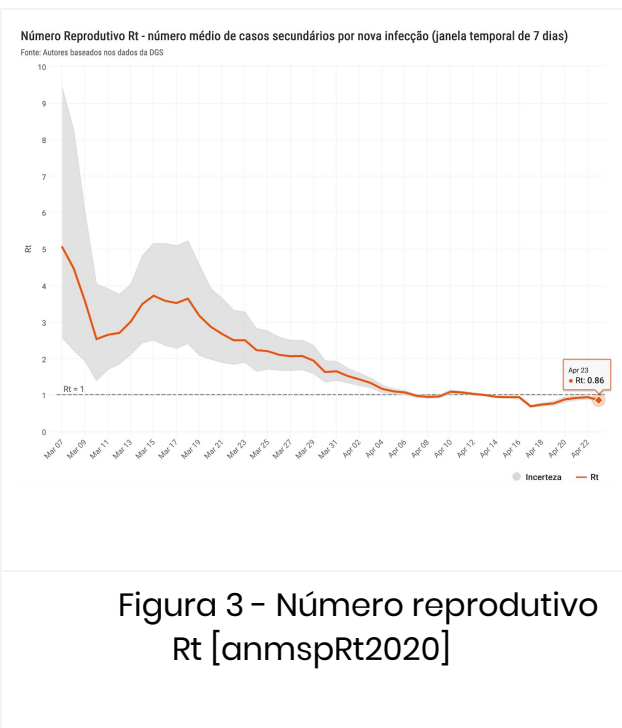
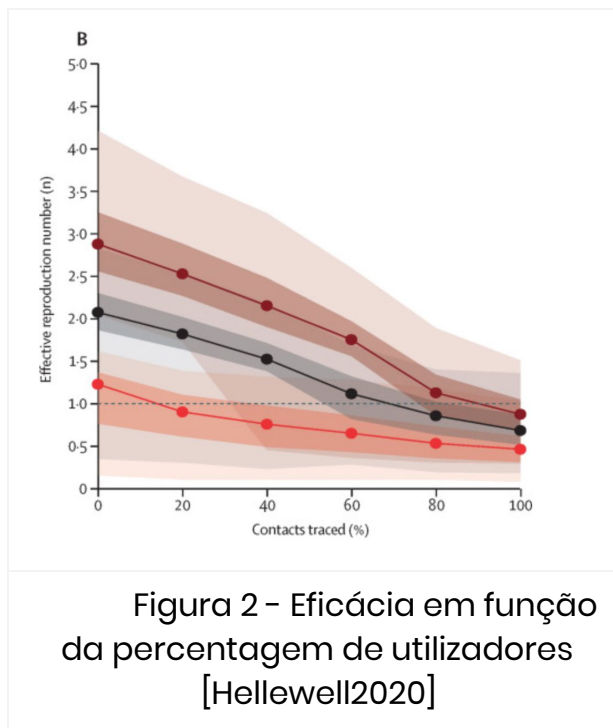
✦ See all authors and affiliations

Science 08 May 2020:
Vol. 368, Issue 6491, eabb6936
DOI: 10.1126/science.abb6936

[Science Magazine](#) [Ferreti2020]

Uma das questões que se têm colocado é que estas aplicações, se não forem utilizadas por uma percentagem elevada da população (> 60%), são inúteis e, pelo contrário, podem gerar uma falsa sensação de segurança aos seus utilizadores. A aplicação de Singapura tem sido frequentemente apresentada como exemplo de que estas aplicações de uso voluntário são pouco instaladas, contando apenas com 20% da população (1.1M) no fim de Abril. Não podemos contudo esquecer que esta aplicação não garante a privacidade dos contactos e tal apresenta-se como um forte desmotivador ao uso da aplicação.

Num outro [estudo](#) [Hellewell2020] modelou-se o rastreamento de contactos digital para estudar o seu impacto em função de diferentes taxas de utilização da aplicação por parte da população. Em epidemiologia, a velocidade de disseminação de uma doença é identificada como R (ou número reprodutivo), e representa o número médio de pessoas infectadas por um caso positivo. Entre Dezembro e Janeiro, o R do COVID-19 oscilou entre 1.4 e 3.8 [Riou2020]. Esta variação é ainda muito grande, mas estima-se que em Portugal no início de Maio, com o país a deixar o estado de emergência e a maior parte da sua população em quarentena, o R está abaixo de 1.0 [anmspRt2020] (Figura 3), limiar abaixo do qual o número de novos casos tende a reduzir-se até desaparecer. À medida que começamos a abrir o país, não havendo novas medidas, é expectável que o R suba. De acordo com o estudo [Hellewell2020], introduzindo rastreamento de contactos, e assumindo que o R subiria para 1.5, seria suficiente uma taxa de utilização da aplicação entre 20% e 30% da população para trazer o R novamente abaixo de 1.0. Em qualquer caso, este estudo sugere que, para qualquer valor de R , a utilização desta abordagem reduz sempre a disseminação, independentemente da taxa de utilização. Contudo este estudo não considera as taxas de falsos positivos e falsos negativos que a técnica poderá implicar, discutidas abaixo.



Há duas questões centrais relativas à eficácia e falibilidade destes sistemas: a possibilidade de resultados chamados falsos negativos e falsos positivos. Resultados chamados falsos negativos, surgem por estas aplicações não poderem rastrear diretamente potenciais infecções via superfícies onde o vírus ficou depositado (contágios indirectos) nem poderem sinalizar contatos com indivíduos assintomáticos positivos mas não diagnosticados, que segundo [nature20] poderão ser até 60% de todos os indivíduos infectados, pelo menos, enquanto não aumentar a capacidade de realização de testes de diagnóstico e de presença de anticorpos.

Da mesma forma é complexo lidar com os potenciais resultados que chamamos falsos positivos, como a proximidade detectada a alguém do outro lado de uma janela ou uma parede fina, com quem efetivamente não houve contato. Outro exemplo interessante coloca-se na perspectiva de empresas. Se alguém for diagnosticado positivo, todos os trabalhadores a trabalhar no mesmo recinto, ao longo do mesmo tempo, irão com alta probabilidade ser notificados para se isolarem e a empresa, se não tiver a funcionar com equipas estanques, poderá ter que parar. Nas cidades e nos locais de maior concentração de pessoas (supermercados, restaurantes, transportes públicos) o número de falsos positivos será potencialmente elevado, o que poderá pôr em causa a utilidade da app. Um indivíduo infectado que use máscara e luvas também reduz drasticamente a sua taxa de infecção, dependendo da forma como as use e o tipo da máscara, podendo contudo os seus contactos serem marcados como de alto risco.

Não conhecemos à data estudos mais completos sobre rastreamento de contactos que meçam taxas de falsos positivos e de falsos negativos e o seu impacto na eficácia desta abordagem. Estes resultados surgirão em breve à medida que vários países introduzem estas soluções no terreno, possivelmente com testes controlados, e discussão subsequente.

Dentro deste grupo de trabalho foram discutidas várias formas de reduzir ou colmatar resultados falsos positivos no rastreamento de contactos digital:

- Não sendo aparentemente prático uma solução em que a aplicação possa restringir o alcance do sinal Bluetooth (20 a 30 metros) por falta

de suporte universal, a solução passaria então por afinar a fórmula de risco para desconsiderar contactos em função da sua proximidade. Ou seja, colocar os contactados a ignorar contactos que não tenham sido muito próximos (2-5 metros). Contudo, a estimativa habitualmente devolvida pela interface Bluetooth é muito falível, podendo-se trabalhar em soluções para melhorar a sua precisão, tais como o uso de filtros [Mackey2020] ou recorrendo a triangulação entre os dispositivos com a aplicação ativa.

- Programar na aplicação um estado de “estou só”, para que as pessoas quando estão, por exemplo, em à casa à noite, dentro de paredes, a aplicação não estar a registar contactos na vizinhança.
- Combinar a aplicação de rastreamento de contactos com o rastreamento de sintomas para incluir o histórico de sintomas no cálculo do risco de um contacto. Se o contacto foi há uma semana e a pessoa não tem sintomas, maior será a probabilidade de ser um falso positivo. A fórmula de risco pode também ponderar o actual risco da zona (código postal) onde a pessoa passar a maior parte do tempo. Não resolve todos os problemas relacionados com falso positivos, mas atenua, adicionando outra informação epidemiológica relevante.
- Considerar o rastreamento de contactos digital como um complemento do rastreamento de contactos manual. Tal sistema poderia funcionar desta forma: quando a aplicação notifica o utilizador, em vez de recomendar o teste diagnóstico pede para contactar uma linha, onde alguém irá fazer uma avaliação de risco e determinar se a pessoa deve mesmo ser testada e/ou iniciar isolamento ou não.

O impacto real do rastreamento de contactos digital nunca será determinístico ou garantido. Também por esse motivo, em momento algum, se deverá relaxar todas as outras medidas de contenção como uso da máscara, luvas e distanciamento social, apenas por existirem meios de rastreamento digital. Deve haver muito cuidado na comunicação sobre o rastreamento de contactos para evitar gerar excessos de confiança e comportamentos de risco.

Literacia digital, maximizar a inclusão e visar o benefício de todos

Uma característica importante que estas soluções devem ter é que possam ser inclusivas e potencialmente utilizadas por, ou pelo menos trazer benefício direto a, 100% da população. No entanto isso é utópico, pelo menos no sentido da possibilidade de todos os indivíduos poderem utilizar estes meios digitais hoje. Há uma percentagem importante da população portuguesa que não tem um Smartphone com Bluetooth e/ou ligação à Internet. Dos que os têm, a maioria terá um Smartphone Android ou iOS, mas nem todos. Como permitir aos restantes cidadãos participar? Uma solução poderia ser a distribuição de Smartphones baratos ou SmartWatches baratos mas funcionais. O modelo de financiamento destes dispositivos teria que ser discutido e acompanhado de medidas de introdução do seu funcionamento aos novos utilizadores, potencialmente às populações mais vulneráveis, com necessidade de isolamento e menor literacia digital. Estes dispositivos teriam também de ser robustos do ponto de vista de segurança.

Em 2019, a percentagem da população com competências digitais básicas (ou superior) pouco passava os 50%

Mas ter um *Smartphone* está longe de ser o único problema. Em 2019, a percentagem da população com competências digitais básicas (ou superior) pouco passava os 50% [incpothum20]. O rastreamento de contatos digital, implica necessariamente a utilização de uma aplicação móvel por indivíduo, contudo, outras funcionalidades potencialmente providenciadas pela mesma App, como aconselhamento baseado em rastreamento de sintomas,

podem contemplar a possibilidade de inclusão por um terceiro, de indivíduos sem acesso a smartphones, como idosos e crianças.



Sendo a aplicação necessariamente opcional, haverá quem mesmo podendo, opte por não participar. É importante que não haja nenhum tipo de discriminação ou limitação, directa ou implícita relativamente a quem não usa a aplicação.

Outro aspecto a ter em conta é que pessoas suspeitas de infecção poderão ficar barradas de sair de casa e ir trabalhar. Isso poderá levar pessoas a não usarem a aplicação, optando por não saber

de forma a poderem ir trabalhar. Este factor não é único a estas aplicações, aplicando-se também a pessoas que têm sintomas mas optam por não contactar as autoridades.

Mesmo que a possibilidade de utilização destas aplicações tecnológicas por 100% dos cidadãos, possa ser hoje ainda uma utopia, a utilização das mesmas apenas por uma fração da população, poderá trazer benefício a todos.

Princípios para uma aplicação nacional

O sucesso de uma aplicação de rastreamento de contactos depende de vários factores, a começar pela sua eficácia, mas também aspectos de privacidade, segurança, credibilidade, percepção de risco, facilidade de utilização ou percentagem de utilização por parte dos portugueses, assim como o contexto de utilização destas Apps, e a sua integração com os sistemas de saúde, científicos e a economia.

A seguinte lista pondera estes aspectos e materializa-os em princípios orientadores para o desenvolvimento e operacionalização de uma aplicação de rastreamento de contactos para Portugal.

1. Ser eficaz para o propósito a que se propõe

É urgente **discutir abertamente e encontrar soluções para mitigar ou atenuar o problema de falsos positivos e falsos negativos**, nomeadamente no sentido de potenciar a eficácia do rastreamento de contactos digital em relação ao manual, no que diz respeito a estes problemas, além do factor de ampliação do número rastreamentos possível. Algumas ideias foram incluídas neste documento. Caso os falsos positivos e falsos negativos não sejam mitigados de forma significativa, a utilidade da solução poderá estar em causa, e assim, também, a sua taxa de utilização.

No âmbito do Regulamento Geral de Proteção de Dados (RGPD), é permitida a recolha de dados que sejam necessários para realizar um determinado objectivo que é contratualizado ou prometido a quem os cede. Se o propósito não é cumprido, então um dos princípios do RGPD não é respeitado.

Para ser eficaz no espaço Europeu, terá também de ser uma aplicação interoperável, ou seja que possa funcionar com apps de rastreamento de contactos de outros países, pelo menos, ao nível da União Europeia.

2. Preservar a privacidade dos dados dos cidadãos

Para tal propõe-se a utilização de um **modelo descentralizado**, em linha com o que o [DP-3T propõe](#). A solução deverá respeitar a 100% o **RGPD**, incluindo minimização da utilização de dados, e **expirando automaticamente** os dados à medida que perdem a sua utilidade. No final da pandemia a aplicação deverá remover a totalidade dos dados. A solução deverá respeitar também a **constituição portuguesa**. E terá ainda que merecer um **parecer positivo** da Comissão Nacional de Proteção de Dados (CNPd), o que incluirá, entre outras, a necessidade de a aplicação **não ser de uso obrigatório**.

Terá que ser **robusta** em relação a ataques de **deanonimização** e não expor *side-channels*. Aspectos de privacidade deverão ser alvo de uma **auditoria independente**.

Uma avaliação de impacto na privacidade (PIA) deverá também ser realizada por uma entidade independente.

3. Ser robusta em termos de segurança

Do ponto de vista da segurança, a solução deve ser sujeita a uma **auditoria independente** e mostrar robustez. Deverá também ser **resiliente** a ataques **à integridade** do código no próprio dispositivo, devendo o código da aplicação ser protegido com tecnologia específica para o efeito (tecnologia *tamper-resistant*, que abranja também protecção contra ataques de exfiltração de dados, quer por via de adulteração do código como por inspecção da memória da aplicação enquanto esta se encontra em funcionamento).

A Open Web Application Security Project ([OWASP](#)) é uma organização sem fins lucrativos, respeitada internacionalmente e movida por voluntários, que se dedica à divulgação de boas práticas de segurança aplicacional. A aplicação deverá seguir as recomendações gerais do [OWASP Mobile Security Testing Guide](#), tais como, o uso de assinaturas digitais do código (*Code Signing*), para reduzir o risco de publicação de uma versão adulterada da aplicação, seja nas *appstores* oficiais ou noutras - e apenas confiar em comunicações encriptadas com um par de chaves digitais pré-definido (*Certificate Pinning*), uma prática comum recomendada para reduzir o risco de ataques que comprometam a confidencialidade das comunicações (*Man-in-the-Middle*, MITM).

Deverão ser criados mecanismos que permitam a rápida detecção e eliminação de **aplicações falsas** (*fake apps*).

Estabelecendo-se a necessidade deste tipo de aplicações de forma sazonal ou periódica, idealmente, esta aplicação deverá ser operada por uma entidade com capacidade para **gestão de sistemas com altos requisitos de segurança**. Nomeadamente deverá ter ou procurar obter certificações como ISO 27001 ou SOC/SOC2, que promovem uma profissionalização da organização no que toca aos seus processos de segurança.

4. Ser escrutinável, aberta e passível de análise pública

O desenvolvimento e operacionalização desta aplicação deverá ser feita de forma **transparente**, permitindo aos cidadãos ganharem confiança na aplicação. Uma medida absolutamente essencial é disponibilizar como **código aberto** todo o código da aplicação, bem como de todos os componentes de que depende.

5. Alcançar toda a população

Esta aplicação deverá chegar idealmente a **todos os Portugueses**. Sabemos que isso não é fácil, uma vez que nem toda a população tem equipamentos compatíveis ou os sabe utilizar. Foram dadas algumas sugestões nesse sentido neste documento.

É também uma tarefa monumental garantir o bom funcionamento da aplicação na vasta diversidade de dispositivos que existem no mercado. Uma grande ajuda nesse sentido será fazer **uso da API da Google e da Apple** para rastreamento de contactos, assegurando através desta o bom funcionamento da parte mais complexa da aplicação em todos os dispositivos Android e IOS.

A aplicação deverá ser **simples e agradável de usar**, devendo ser desenvolvida como o **produto** digital que será, com foco na usabilidade, com atenção ao *feedback* dos utilizadores, e com estrutura de suporte profissionalizada.

Do ponto de vista da engenharia, a **infraestrutura** deverá ser **dimensionada** para suportar toda a população portuguesa e com **alta disponibilidade e resiliência a falhas**.

6. Ser Integrada com os esforços nacionais de rastreamento de contatos, teste de diagnóstico e monitorização da COVID-19

É necessária uma verdadeira integração e trabalho coordenado e conjunto, em tempo real, com os vários esforços nacionais, especialmente os esforços de rastreamento contatos manual, realização de testes diagnóstico e controle da epidemia por parte do Ministério da Saúde (nomeadamente DGS, SPMS e as ARS), Ministério da Ciência e os vários ministérios com a tutela correspondente a diferentes aspectos da retoma sócio-económica e a populações mais vulneráveis, assim como os setores privado e social.

Uma aplicação não vem substituir estes esforços, mas sim procurar amplificá-los, assim como a colaboração e coordenação entre eles, de forma integrada.

7. Conjugar numa aplicação única funcionalidades complementares para controlo epidémico

Existem vários tipos de aplicações de controlo epidémico, como por exemplo soluções digitais de rastreamento de sintomas e do estado de confinamento da população, com provas dadas já no combate a COVID-19 [Rossman2020]. Estas aplicações deveriam ser **estrategicamente conjugadas numa aplicação só**, não só para evitar fragmentação, mas também para explorar sinergias entre as várias técnicas, e para facilitar a vida ao cidadão, multiplicando assim os incentivos ao uso destas apps.

Adicionalmente, a API que a Apple e a Google estão a desenvolver estará apenas disponível para uma aplicação por país [aplgoo20], por forma a não incentivar a fragmentação da oferta de aplicações, algo que pode ser prejudicial à eficácia das aplicações.

Conclusões

Neste documento apresentamos um conjunto de princípios orientadores para o desenvolvimento de uma aplicação de rastreamento de contactos para Portugal. Existem soluções que permitem a segurança e privacidade dos dados dos cidadãos, sem a criação de bases de dados centralizadas contendo dados sensíveis. O rastreamento de contactos digital carece ainda de validação científica quanto à sua eficácia. O problema relativo à sua eficácia, nomeadamente, a existência de falsos positivos e de falsos negativos, deverá ser quantificado e atenuado. **É necessário um trabalho conjunto, por parte dos diferentes ministérios do governo, da sociedade civil, das empresas, e do setor social** no sentido de ultrapassar estes problemas e desenvolver uma aplicação de rastreamento de contactos, unida a outras funcionalidades já comprovadas, como o rastreamento de sintomas, e integrada com os sistemas existentes de controle epidémico, que impacte positivamente a luta contra a COVID-19 e que auxilie a nossa saída gradual do confinamento.

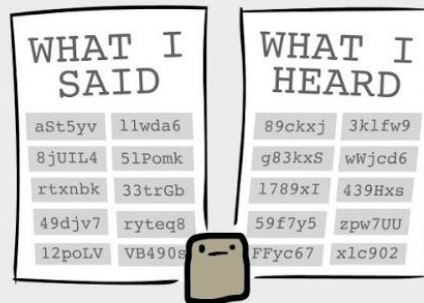
HOW PRIVACY-FIRST CONTACT TRACING WORKS



Alice's phone broadcasts a random message every few minutes.



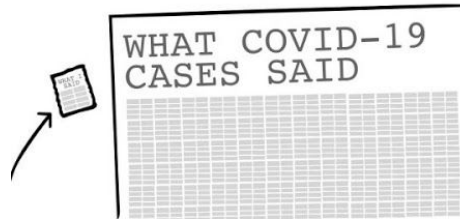
Alice sits next to Bob. Their phones exchange messages.



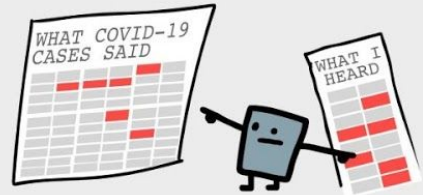
Both phones remember what they said & heard in the past 14 days.



If Alice gets Covid-19, she sends *her* messages to a hospital.



Because the messages are random, no info's revealed to the hospital...



...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!



If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.



And *that's* how contact tracing can protect our health *and* privacy!

by Nicky Case (ncase.me), CC0/public domain, feel free to re-post anywhere!

Autoria

Este documento é resultado do grupo de trabalho 1App4PT, resultando de uma cooperação entre as equipas da [Covidografia.pt](https://covidografia.pt) e da [CovidApp.pt](https://covidapp.pt) (não confundir com a aplicação da Hype Labs, também ela apelidada de CovidApp), contando ainda com o apoio do movimento [tech4COVID19](https://tech4COVID19.org).



covidografia



CovidApp



#tech4COVID19

Contactos: +351.917331552 – info@lapp4.pt

Referências

- **[constpt26-1]** Constituição Portuguesa – Artigo 26º – Nº 1 –
<https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx#art26>
- **[echr2012]** European Charter Of Human Rights,
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>
- **[Ferreti2020]** L. Ferreti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. A.-Dorner, “Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing”, Revista Science, 31 Março 2020,
<https://science.sciencemag.org/content/early/2020/04/09/science.abb6936>, acessado em 25 de Abril de 2020
- **[Hellewell2020]** Hellewell, Joel, Sam Abbott, Amy Gimma, Nikos I. Bosse, Christopher I. Jarvis, Timothy W. Russell, James D. Munday et al. “Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts.” The Lancet Global Health (2020),
[https://www.thelancet.com/journals/langlo/article/PIIS2214-109X\(20\)30074-7/fulltext](https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(20)30074-7/fulltext), acessado em 25 de Abril de 2020
- **[anmspRt2020]** Mapa Epidemiológico Portugal,
<https://www.anmsp.pt/covid19-mapa>, acessado em 25 de Abril de 2020
- **[nature20]** Nature – Covert coronavirus infections could be seeding new outbreaks, <https://www.nature.com/articles/d41586-020-00822-x>, 20 de Março de 2020, acessado em 25 de Abril de 2020
- **[incpothum20]** Indicadores de potencial humano na população portuguesa,
<http://observatorio.incode2030.gov.pt/indicadores/indicadores-potencial-humano/>

- **[uerecom20]** Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626, 8 de Abril de 2020, acessado a 12 de Maio de 2020
- **[cnil2020]** Publication de l'avis de la CNIL sur le projet d'application mobile StopCovid, <https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid>, 26 de Abril de 2020, acessado a 2 de Maio de 2020
- **[Riou2020]** Riou, Julien; Althaus, Christian L. (2020). "Pattern of early human-to-human transmission of Wuhan 2019 novel coronavirus (2019-nCoV), December 2019 to January 2020". *Eurosurveillance*. 25 (4). doi:10.2807/1560-7917.ES.2020.25.4.2000058. PMC 7001239. PMID 32019669.
- **[Mackey2020]** Mackey, A., Spachos, P., Song, L., & Plataniotis, K. (2020). Improving BLE Beacon Proximity Estimation Accuracy through Bayesian Filtering. *arXiv preprint arXiv:2001.02396*. <https://arxiv.org/pdf/2001.02396.pdf>
- **[tech0417]** Europe's PEPP-PT COVID-19 contacts tracing standard push could be squaring up for a fight with Apple and Google, <https://techcrunch.com/2020/04/17/europes-pepp-pt-covid-19-contacts-tracing-standard-push-could-be-squaring-up-for-a-fight-with-apple-and-google/>, 17 de Abril de 2020, acessado em 4 de Maio de 2020
- **[aplgoo20]** Apple, Google Covid-19 Tool to Be Limited to One App Per Country, <https://www.bloomberg.com/news/articles/2020-05-04/apple-google-covid-19-tool-to-be-limited-to-one-app-per-country>, acessado em 11 de Maio de 2020
- **[Rossman2020]** Rossman, Hagai, et al. "A framework for identifying regional outbreak and spread of COVID-19 from one-minute population-wide surveys". *Nature* 9 de Abril de 2020 <https://www.nature.com/articles/s41591-020-0857-9>