Teste 2 de ASPI

(Teste para fazer em casa e em grupo)

Introdução ao problema objeto das perguntas

Durante a atual crise provocada pelo Covid-19, quando se deteta que uma pessoa A está infetada pelo vírus, é essencial proceder a um inquérito para saber com que outras pessoas A contactou recentemente de forma continuada (esteve na sua proximidade tempo significativo). Essas pessoas deverão ser contactadas para se analisar as suas características (se são de risco por exemplo), se apresentam sintomas, etc. para decidir que ações tomar (se as mesmas devem ser isoladas, feitos testes, etc.) com o objetivo final de limitar a propagação do vírus.

Naturalmente, este processo, realizado manualmente, é inefeciente e lento. Pôr a tecnologia ao serviço do mesmo, de forma a torná-lo mais eficiente, é importante. Por isso foram desenvolvidas diversas soluções tecnológicas baseadas na utilização de smartphones para tentar tornar mais eficaz o processo.

Considere a seguir três dessas aplicações: uma, semelhante à desenvolvida pelo Governo de Singapura (S) e duas outras "teóricas", desenvolvidas na Europa, uma das quais dita Centralizada (C), e outra dita Descentralizada (D).

Vamos admitir por hipótese que todas as aplicações usam a tecnologia Bluetooth para que dois smartphones detetem se estão na proximidade um do outro (por hipótese a menos de 2 metros e durante pelo menos 10 minutos – o que seria uma situação que poderia propiciar a passagem do vírus de uma pessoa infetada a outra não infetada). Existem duas hipóteses de os dois smartphones registarem a identidade um do outro nessa situação.

No primeiro caso, cada smartphone memoriza um identificador único do outro. Esse identificador caracteriza inequivocamente cada smartphone . Chamemos a esta solução: proximidade com base em IDs únicos.

Na segunda hipótese, cada smartphone gera um ID (número) aleatório e, caso dois smartphones se encontrem em proximidade, eles trocam entre si os IDs aleatórios. Para reforçar o anonimato, estes IDs são gerados e alterados por cada smartphone, de forma independente, de meia em meia hora. Chamemos a esta solução: proximidade com base em IDs aleatórios.

Nota: a Apple e a Google desenvolveram uma API que dá a cesso a uma implementação semelhante à descrita nesta segunda hipótese, e que permite a uma aplicação aceder aos pares de IDs aleatórios correspondentes aos encontros que o smartphone teve nos últimos 14 a 16 dias. Encontros mais antigos são esquecidos. Se tiver curiosidade, consulte a bibliografia no fim.

As descrições que se seguem são versões hipotéticas e simplificadas das verdadeiras aplicações que estão, ou vão estar, disponíveis. Todas as aplicações têm em comum o facto de serem geridas pelos Governos através das respetivas Autoridades de Saúde, serem de

instalação e uso voluntário, e serem transparentes, na medida em que existe, não só consentimento dos utilizadores, como ampla informação sobre o seu funcionamento. O código fonte das aplicações a correrem nos smartphones é também público.

Descrição da aplicação S (Singapura)

Quando o utilizador instala a aplicação S, a mesma regista num servidor central o número de telefone do utilizador e o ID único do seu smartphone. Depois, o sistema de operação do smartphone, mesmo que o mesmo esteja bloqueado, vai monitorando e registando os eventos de proximidade com outros smartphones, e regista os IDs únicos daqueles com que tem encontros.

Periodicamente, os smartphones com a aplicação instalada contactam o servidor central e registam nele os encontros que tiveram ultimamente, através dos IDs únicos que caracterizam esses encontros.

Se for diagnosticada a infeção por Covid-19 de uma pessoa a usar a aplicação, sob sua autorização, os profissionais de saúde têm acesso imediato aos IDs, e, portanto, aos telefones das pessoas com as quais o infetado se encontrou ultimamente, e essas pessoas podem ser avisadas automaticamente desse contato.

A aplicação e o servidor central são geridos pelo Governo, em quem as pessoas em Singapura confiam, e os dados sobre encontros são apagados ao fim de 14 a 16 dias. No entanto, uma versão anonimizada desses dados é guardada para estudos sobre a evolução da pandemia.

Verificou-se que apenas 20% das pessoas instalaram a aplicação e que houve necessidade de continuar a usar uma grande quantidade de rastreadores humanos que entrevistavam todos os infetados e os seus contactos (ou pelo menos aqueles de que eles se lembravam). Constatou-se também que, entre o grupo de risco (maiores que 65 anos), apenas 50% tinham smartphone e apenas 20% destes instalaram a aplicação.

Resumo: a solução S é baseada em proximidade com base em IDs únicos não anonimizados, rastreamento dos contatos de forma centralizada, rastreamento com acesso à identidade das pessoas (n.º de telefone) e anonimização da informação sobre encontros para estudo posterior da evolução da pandemia.

Descrição da aplicação C (Centralizada)

Esta aplicação é usada em vários países da UE. É bastante parecida com a aplicação S, mas tem uma diferença essencial: utiliza identificadores de proximidade aleatórios e não existe registo central de qualquer relação entre os identificadores aleatórios e números de telefone ou nomes de pessoas. Tudo é anónimo.

Ou seja, cada encontro de smartphones é caracterizado por um par de números aleatórios que é registado por estes. Periodicamente, a aplicação passa ao servidor central os encontros que teve, ou seja, os pares de números aleatórios que os caracterizam.

Se for diagnosticada a infeção por Covid-19 de uma pessoa a usar a aplicação, sob sua autorização, os profissionais de saúde têm acesso imediato aos IDs usados nos últimos 14 a 16 dias pelo smartphone do doente, e registam esses números no servidor. Este, pode identificar todos os pares de números aleatórios em que um dos números é um dos IDs aleatórios do doente e que representam encontros que este teve.

Periodicamente, cada smartphone contacta o servidor central, faz o upload dos últimos encontros que teve, e faz o download dos encontros em que os seus IDs figuram em encontros com infetados nos últimos 14 a 16 dias. Se esse conjunto não for vazio, o utilizador é avisado de que teve um encontro com um infetado e é aconselhado a contactar os serviços de saúde.

A aplicação e o servidor central são geridos pelo Governo. Os dados sobre encontros são apagados ao fim de 14 a 16 dias, mas uma versão anonimizada desses dados é guardada para estudos sobre a evolução da pandemia. Repare-se que o servidor central não consegue relacionar IDs aleatórios com doentes concretos (exceto saber os que correspondem a infetados) e nem sequer consegue correlacionar entre si todos os IDs do mesmo smartphone, nomeadamente os carregados em sessões distintas.

Não existem ainda dados sobre a popularidade ou eficácia da aplicação.

Resumo: a solução C é baseada em proximidade com base em IDs aleatórios, rastreamento dos contactos de forma centralizada, rastreamento sem acesso à identidade das pessoas (n.º de telefone), pro-atividade de quem contactou com infetados para contacto com os serviços de saúde, e anonimização da informação sobre encontros para estudo posterior da evolução da pandemia.

Descrição da aplicação D (Decentralizada)

Esta aplicação é usada em vários países da UE. É parecida com a aplicação C, mas tem uma diferença essencial: o servidor central apenas tem os IDs aleatórios de smartphones de pessoas infetadas (que autorizaram que esses IDs lá sejam colocados).

É cada smartphone que memoriza os pares de IDs aleatórios correspondentes aos encontros que este teve nos últimos 14 a 16 dias. No servidor só são registados os IDs usados nos últimos 14 a 16 dias pelos smartphones de cada infetado. Periodicamente, cada smartphone vai ao servidor e faz o download dos IDs dos infetados. Nessa altura compara com os pares que tem registados localmente, e se em algum desses pares figurarem IDs de infetados, alerta o utilizador para que este teve um encontro com um infetado e é portanto aconselhável contactar os serviços de saúde.

A aplicação e o servidor central são geridos pelo Governo, e os dados sobre os IDs dos infetados são apagados ao fim de 14 a 16 dias. Nessa altura toda a informação é apagada pois não acrescenta nenhum valor a qualquer estudo sobre a evolução da epidemia.

Não existem ainda dados sobre a popularidade ou eficácia da aplicação.

Resumo: a solução D é baseada em proximidade com base em IDs aleatórios, rastreamento dos contactos de forma descentralizada, rastreamento sem acesso à identidade das pessoas (n.º de telefone), pro-atividade de quem contactou com infetados para contacto com os serviços de saúde, e não fornece informação para estudos posteriores sobre a evolução da pandemia.

Questões a que devem responder

Respondam às 5 questões abaixo.

1) Respeito, formal ou não, do RGPD por cada uma das aplicações. Compare-as entre si deste ponto de vista.
2) Contribuição real de cada aplicação para ajudar o rastreamento de contactos com infetados (visão da parte boa de uma análise "utilitarista"). Compare-as entre si deste ponto de vista.
3) Contribuição real de cada aplicação para ajudar ao estudo da evolução da pandemia no tempo (visão da parte boa de uma análise "utilitarista"). Compare-as entre si deste ponto de vista.
4) Análise à luz da teoria ética designada "Kantianismo" ou análise à luz da teoria ética designada "Contrato social" as 3 aplicações.
5) Qual das 3 soluções acham preferível e porquê.

Podem escrever 3 (de preferência) ou no máximo 4 páginas no seguinte formato: fonte Arial, 11pt, espaçamento e meio, contendo a resposta a cada uma das 5 questões (numerem cada uma das respostas – i.e. "**Resposta à questão x**").

Cada uma das 5 respostas será avaliada com base no estilo e clareza do texto (30%) assim como com base na solidez da argumentação (70%). Por exemplo, se usarem tabelas para melhorar a clareza, isso pode ser favorável.

A resposta ao teste deve ser elaborada em grupo, pelo mesmo grupo que fez o desenvolvimento do trabalho anterior.

Prazo de entrega da resposta ao tese: 27 de Maio, até às 23:59

Penalizações por entregas com atraso: 0,5 valores por dia até um máximo de 6 dias de atraso (2 de Junho, 23:59). Submissões posteriores não são aceites.

Bibliografia para o caso de quererem aprofundar o problema

Podem consultar esta base de dados pública da MIT Technological Review que tem imensos dados sobre as aplicações que estão a ser usadas ou desenvolvidas
https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit#gid=0

Artigo sobre a aplicação usada em Singapura
https://www.straitstimes.com/singapore/coronavirus-singapore-develops-smartphone-app-for-efficient-contact-tracing

Documento com as recomendações da união europeia
https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Sobre a técnica de IDs aleatórios na base da solução Apple+Google:
https://en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing

Um artigo que tenta mostrar que estas aplicações não são tão eficazes quanto se julga
https://www.politico.eu/article/coronavirus-smartphone-apps-alone-wont-help-curb-the-pandemic-artificial-intelligence-experts-warn/?mc_cid=79d40d9ee7 HYPERLINK