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 detecta que uma pessoa A está infectada 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 ineficiente 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 infectada a outra não infectada). 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 acesso 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 infecção 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 infectado 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 infectados 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 infecção 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 infectado 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 contatos de forma centralizada, rastreamento sem acesso à identidade das pessoas (n.o de telefone), proatividade 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 (Descentralizada)

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 infectado 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 infectados 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 contatos de forma descentralizada, rastreamento sem acesso à identidade das pessoas (n.o de telefone), proatividade 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

Uma resposta ao teste 2 de ASPI que os docentes consideram certa

Na análise das três aplicações não se considera se estas são ou não úteis para controlar o comportamento dos infectados, isto é, se eles respeitam ou não as regras do confinamento, nem considerações como “se eu estiver infectado e não puder sair de casa, então se não me ajudarem, eu e a minha família vamos morrer de fome”. A primeira questão é para outra categoria de aplicações, e a segunda, por hipótese, também não se considera, pois admite-se que se alguém estiver infectado e não puder trabalhar, então o doente e a família vão ser ajudados. Infelizmente esta hipótese é falsa, mas é mesmo assim introduzida para simplificar a discussão.

Resposta à questão 1

As 3 aplicações são compatíveis com o RGPD porque:

- São operadas por autoridades oficiais de saúde com o objetivo de ajudar a combater e compreender a evolução da pandemia Covid-19, sem qualquer outra motivação.
- São de adesão voluntária.
- Indicam quais os processamentos dos dados realizados, como e por quem.
- A recolha de dados é proporcional e não exagerada.
- Quando são guardados dados estes são anonimizados.
- Como os dados são apagados ao fim de 14 dias não é preciso política de apagar dados a pedido.
- Incluem uma política de consentimento clara.
- No caso de ser detectado um infectado este tem de dar autorização para os seus IDs serem inseridos no sistema.
- É claro que os IDs de um utilizador vão ficar armazenados no telemóvel dos utilizadores com que ele se cruzou. Logo, esses utilizadores também podem processar esses dados. Este aspeto faz com a aplicação S possa ferir o RGPD pois não há garantias sobre o que os outros utilizadores vão fazer com esses dados. Tem de estar na política de utilização que não podem fazer nada caso a aplicação não inclua meios para não dar acesso aos utilizadores aos dados sobre os contactos, o que é possível em qualquer caso.

Notas de correção - na resposta exige-se que se diga preto no branco se as aplicações estão ou não de acordo com o RGPD e se justifique a resposta. Podem frisar as condições necessárias de implementação que o garantem se tiverem dúvidas sobre a implementação proposta.

Resposta à questão 2

Resposta, do ponto de vista utilitarista, à pergunta “como avaliar a utilidade das aplicações de rastreamento dos contatos de um infetado com outras pessoas?”

Fator K ou faceta negativa de todas as (três) aplicações - a deteção de contactos diretos entre pessoas através de Bluetooth é sujeita a falsos positivos e negativos e não tem em consideração se as pessoas em questão estavam ou não a usar máscaras e se tomaram ou não outras precauções, como por exemplo o uso de separadores plásticos numa loja. Por outro lado, os grupos de risco são aqueles em que a adesão à aplicação deve ser menor.

Quantificar o valor do positivo e negativo é um exercício quase impossível. Tentemos a versão qualitativa.

Aplicação S

- **Positivo** - Permite ao profissional de saúde que fala com o infectado aumentar o número de pessoas a contactar dado que a pessoa infectada pode esquecer-se de situações ocorridas; portanto funciona como uma potencial ajuda ao recenseamento de mais contactos.
- **Menos positivo** - O fator K aplica-se mas existem hipóteses de minorar o mesmo através da intervenção do especialista que pode descartar a priori casos pouco prováveis e fala com as pessoas recenseadas pela aplicação.
- **Menos positivo** - Envolve e guarda muitos dados pessoais e se o serviço central puder ser atacado ou se tiver deficiências de desenho esses dados podem ser usados desrespeitando a privacidade e o consentimento dos utilizadores.

Pode ajudar os profissionais de saúde a recensearem alguns contactos suplementares de que o infectado se esqueceu, mas tem muitos perigos para a privacidade.

Aplicação C

- **Positivo -** Permite lançar alertas mas estes podem não ajudar e provocarem mais confusão.
- **Positivo -** Os perigos do ponto de vista da privacidade são muito limitados se não se tiver acesso aos telemóveis das pessoas.
- **Menos positivo -** O fator K aplica-se mas como a aplicação não tem intervenção humana o alertado fica numa situação complicada. Que deve fazer? Onde foi? Estava protegido? Fecha-se em casa? É fácil fazer testes?
- **Menos positivo** – Pode facilitar ataques (mas provavelmente limitados) à privacidade dos utilizadores.

Está por provar que seja efetiva a recensear contactos que conduzam a infetados sem sintomas e pode provocar confusão e alarmes injustificados, não parece ter perigos para a privacidade.

Aplicação D

- **Positivo -** Mesmos que a aplicação C.
- **Positivo -** Os perigos do ponto de vista da privacidade são provavelmente desprezáveis.
- **Menos positivo -** O fator K aplica-se mas como a aplicação não tem intervenção humana o alertado fica numa situação complicada. Que deve fazer? Onde foi? Estava protegido? Fecha-se em casa? É fácil fazer testes?

Está por provar que seja efetiva a recensear contactos que conduzam a infetados sem sintomas e pode provocar confusão e alarmes injustificados, não tem perigos para a privacidade.

Notas de correção – a correta análise dos aspetos positivos vale mais que os menos positivos. Se tiver erros na análise de uma das facetas (os positivos, ou os menos positivos) só pode ter 50% da cotação dessa parte.

Resposta à questão 3

Análise do ponto de vista do progresso no estudo da evolução da pandemia. Repare-se que mesmo sem as aplicações, o recenseamento dos infectados é sempre feito (manualmente) e mesmo com as aplicações continua a sê-lo. Quantificar o valor do positivo e negativo é novamente um exercício quase impossível a não ser nos casos em que não há fatores negativos.

Aplicação S

- **Positivo -** Permite estudos mais profundos sobre a forma como a pandemia se propaga, em particular a intervenção do profissional de saúde pode servir para assinalar pessoas a contactar que depois se verifica estarem infetadas. Isso pode ser muito útil. Permite estudar relações e quantas pessoas um infetado infectou mais.
- **Menos positivo -** Envolve e guarda muitos dados pessoais e se o serviço central puder ser atacado ou se tiver deficiências de desenho, esses dados podem ser usados desrespeitando a privacidade e o consentimento dos utilizadores.

Permite estudar melhor como a pandemia se propaga mas tem muitos perigos de privacidade. Quais pesam mais? Depende provavelmente da gravidade da situação concreta e da opinião dos profissionais de saúde. Numa situação em que a defesa da privacidade é para privilegiar é de rejeitar.

Aplicação C

- **Positivo -** Os estudos que permite sobre a forma como a pandemia se propaga são mais limitados devido a os identificadores serem aleatórios e mudarem e por isso não devem ser contabilizados como muito positivos.
- **Menos positivo -** Facilita ataques (mas provavelmente limitados) à privacidade dos utilizadores.

É duvidoso que ajude a recensear de forma clara a evolução da pandemia e como os infetados propagam a doença mas como não tem perigos de privacidade relevantes pode ser considerada positiva.

Aplicação D

Não deve servir para grande coisa do ponto de vista do estudo da evolução da pandemia mas, os perigos do ponto de vista da privacidade são provavelmente desprezáveis. Do ponto de vista do estudo da propagação é provavelmente neutra, sem positivo, nem negativo.

Notas de correção – a correta análise dos aspetos positivos vale mais que os menos positivos. Se tiver erros na análise de uma das facetas (os positivos, ou os menos positivos) só pode ter 50% da cotação dessa parte.

Resposta à questão 4

Análise do ponto de vista do Kantianismo.

Se universalizarmos o ato de colaborar numa base voluntária com as autoridades de saúde, tal não parece encerrar nenhuma contradição. Logo, do ponto de vista do primeiro imperativo categórico não se detetam contra indicações éticas. Só se as aplicações fossem obrigatórias é que isso seria discutível.

As autoridades de saúde podem estar a tratar as pessoas como meio para o fim de limitar a expansão da pandemia? Não, pois a colaboração dos infetados para o estudo é voluntária e com base em esclarecimento (até poderia ser objeto de um pedido suplementar de consentimento). Adicionalmente, o alerta dos potenciais infetados é do interesse deles. O segundo imperativo categórico só pode ser posto em causa se existirem ataques à privacidade e os dados das pessoas forem usados para outros fins que não os enunciados.

Análise do ponto de vista da teoria do Contrato Social

As pessoas devem colaborar com a Sociedade e obedecer a normas que maximizam o bem de todos, desde que essa colaboração não implique prejuízos desproporcionais e que não são exigidos aos outros. Logo, acreditando que a aplicação é útil à sociedade (e

eventualmente ao próprio) e que não tem inconvenientes para o utilizador, é de participar e usar a aplicação.

A hipótese de vir a ser prejudicado mais do que os outros membros da Sociedade está relacionada com os problemas de privacidade. Quem não aderir tem a certeza de não poder ser prejudicado.

O direito à privacidade é um direito cautelar, logo não é obrigatório. No entanto, como em ambos os casos a adesão é voluntária e tudo é explicado, não é possível argumentar que qualquer uma das aplicações não é ética.

Notas de correção – analisar se a teoria ética escolhida é aplicada de forma coerente com a sua forma de abordar o conceito “ser eticamente recomendada a adoção da aplicação”.

Resposta à questão 5

Um resumo potencialmente simplista é o seguinte: a aplicação que mais se pode revelar útil é simultaneamente a mesma que encerra mais problemas de privacidade - a aplicação S. As aplicações C e D parecem ser ambas de utilidade mais limitada que a S, mas também não encerram problemas graves de privacidade. Tudo indica que os problemas de privacidade da aplicação D são inexistentes.

Em conclusão, talvez seja de dar uma hipótese à aplicação D para ganhar experiência.

As potenciais vantagens de C em relação a D relacionadas com eventuais estudos não se devem valorizar pois a forma como os IDs são gerados vai conduzir a contagens sobrevalorizadas nos encontros (quaisquer dois tuplos distintos não correspondem necessariamente a diferentes encontros e dois encontros entre as mesmas duas pessoas podem ser contabilizados como encontros distintos). Por outro lado, sempre que uma pessoa infectada é detectada, pode-se sempre perguntar-lhe se foi alertada por uma aplicação o que permite ir recolhendo dados sobre a sua eficácia.

No entanto, se os profissionais de saúde estiverem absolutamente convencidos que a aplicação S é mesmo muito importante, e a situação pública for desesperada, talvez seja mesmo de optar pela aplicação S mas com cuidados muito redobrados em torno do servidor, da sua segurança e da forma como é acedido e controlado.

Tudo indica que atualmente os profissionais de saúde não estão muito convencidos da bondade da utilidade de qualquer uma das aplicações.

Notas de correção – todas as opções são aceitáveis, analisar apenas se a opção escolhida é justificada de forma consistente e não existem erros nos argumentos apresentados.