TousAntiCovid et les données personnelles

Conférence ArmorHistel

Le 9 novembre 2021

Jean-Luc Godard & Didier Josse

Orange Solidarité Rennes

Fondation orange

sommaire

1. C’est quoi TousAntiCovid ?
2. L’enjeu des données personnelles dans TAC
3. La solution et les résultats
4. Les enseignements
5. Annexes
    1. La pandémie COVID-19
    2. Le protocole ROBERT
    3. RGPD: De quoi parle-t-on ?

C’est quoi « TousAntiCovid » ?

Contexte en Oct 2020

- Une pandémie **COVID-19** galopante
- Absence de vaccin
- **Tester – Alerter – Protéger**
- Faire appel au numérique pour le « **Contact Tracing** », Alerter et Informer

Les principes de la solution

- **Prévenir** tous ceux exposés au risque de contamination
- L’application ne doit **pas être obligatoire**
- L’anonymat des utilisateurs doit être **garanti**
- **Aucune donnée personnelle** ne doit être enregistrée
- Être un **centre de ressources** et d’information

Les bases techniques et organisationnelles

- Utilisation du « **Bluetooth** » pour le contact tracing (2m pendant au moins 5mn)
- Un projet de développement *StopCovid* sous tutelle de **l’INRIA** avec des experts de différents acteurs dont ANSSI, **Orange,** Dassault, CapGemini,…
- Développer une application « Souveraine » sous contrôle de la **CNIL et de l’ANSSI**
- S’inspirer des tests Bluetooth réalisés à l’Université d’Oxford et d’une application déployée à Singapour
- **Ne pas utiliser** la Géolocalisation (GPS) pour le Contact Tracing – Respect de la vie privée
- Une infrastructure technique **résiliente** et **hébergée en France**

L'enjeu des Données Personnelles dans TAC

Engagements

- Respect de la loi RGDP
- Pas de renseignement d'info personnelles pour utiliser l'application
- Une solution de Haut Niveau de Sécurité
- Principe de « Minimisation » des données utilisées

L'enjeu des données Personnelles

- **Finalité et traitement :** Alerter, Informer, Accompagner
- **Données Personnelles (DP) traitées sur serveur :** Clé authentification, identifiant unique aléatoire, historique proximité,…
- **DP en local :** attestations déplacement,
- **Destinataire des DP :** contacts à risque, INRIA

Gestion des données

- **Comment sont-elles échangées?**
  Bluetooth, pas de données GPS
- **Quelles données sont échangées?**
  via un pseudo-Identifiant renouvelé toutes les 15mn. Aucune information sur l'identité du contact et le lieu.
- **Où sont-elles hébergées ?**
  Sur le mobile pour le local.
  Serveur hébergé chez SecNumCloud (France)
- **Durée de conservation :**
  14 jours
- **Suppression des données**
  possibilité de supprimer les données sur mobile, sur serveur à partir de l'application.
- **Sécurité Informatique :** Procédures ANSSI

La solution et les résultats

Une organisation

- Multi partenaires sous le pilotage de **l'INRIA**
- Des organismes de contrôles pendant le développement : **ANSSI, CNIL**
- Des audits selon le protocole **ROBERT**
- Un cloisonnement des différentes fonctions

Une démarche volontaire et transparente

- Installation **volontaire** de TAC
- Les **codes sources** sont à disposition du public :
  - Vérification des engagements de respect des Données Personnelles
  - Confrontation avec la communauté scientifique pour identifier des possibles failles
- Des **tests de hacking** ont été menés sur la solution

Résultats au 3 nov

Les enseignements

Le respect de la vie privée et des données personnelles (RGDP) est **possible dans le digital** :

➡ Ce doit être une mesure forte de la Maitrise d'Ouvrage, au niveau de l'organisation de la Maitrise d'Œuvre, des partenaires, des contrôles menés avant, pendant et après la mise à disposition de la solution.

➡ La TRANSPARENCE est la clé essentielle du succès

➡ La **sécurité Informatique** n'est jamais figée : l'analyse permanente des risques et l'application des mesures de réduction de ces risques est un fondamental.

Le facteur humain reste un risque difficile à maitriser (exemple de pass sanitaires frauduleux divulgués) :

➡ Sensibilisations et contrôles des acteurs de toute la chaîne sont 2 actions essentielles à mener en permanence

Merci de votre attention

A vos Questions !

#Tous AntiCovid

Fondation orange

Annexes

1 - La Pandémie de COVID-19

2 – StopCovid. Pandémie de Covid-19

Dynamique de propagation du virus

Phase de propagation exponentielle. Quand R0 > 1

R0 = **taux de reproduction de base**

R0 : Nombre moyen de personnes qu'une personne déjà atteinte va contaminer

R0 > 1 → l'épidémie se propage
R0 < 1 → l'épidémie régresse

R0 = P*C*D

Fondation orange

2 – StopCovid. Pandémie de Covid-19

R0 = P*C*D

P : probabilité de contaminer quelqu'un. $0 < P < 1$

C : nombre de contacts/unité de temps

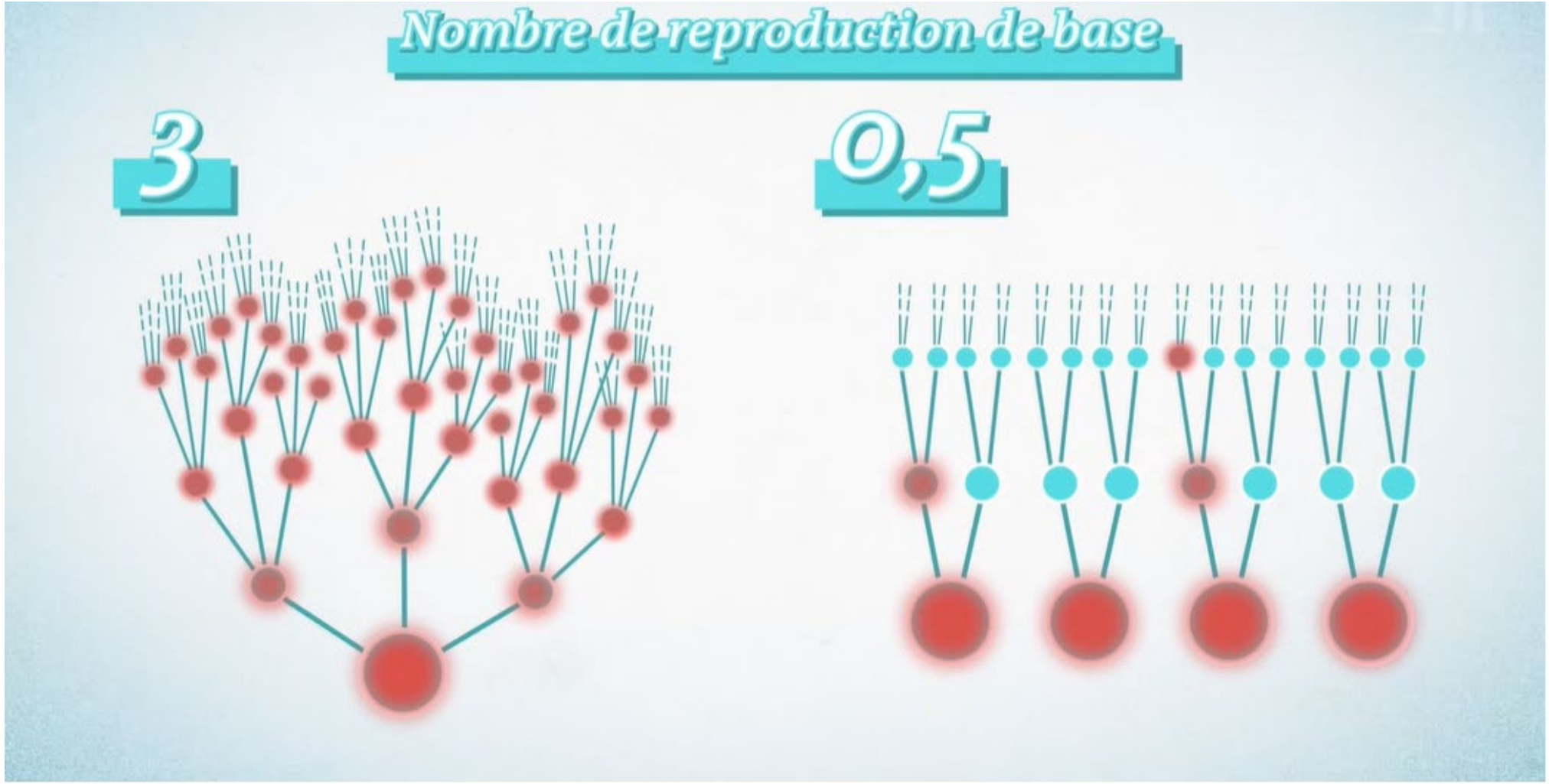
D : durée pendant laquelle on est contagieux (14 jours ?)

Stratégie pour stopper la propagation de l'épidémie :
→ R0 < 1
→ faire décroitre P, faire décroitre C

faire décroitre P → gestes « barrière »
faire décroitre C → confinement

2 – StopCovid. Pandémie de Covid-19

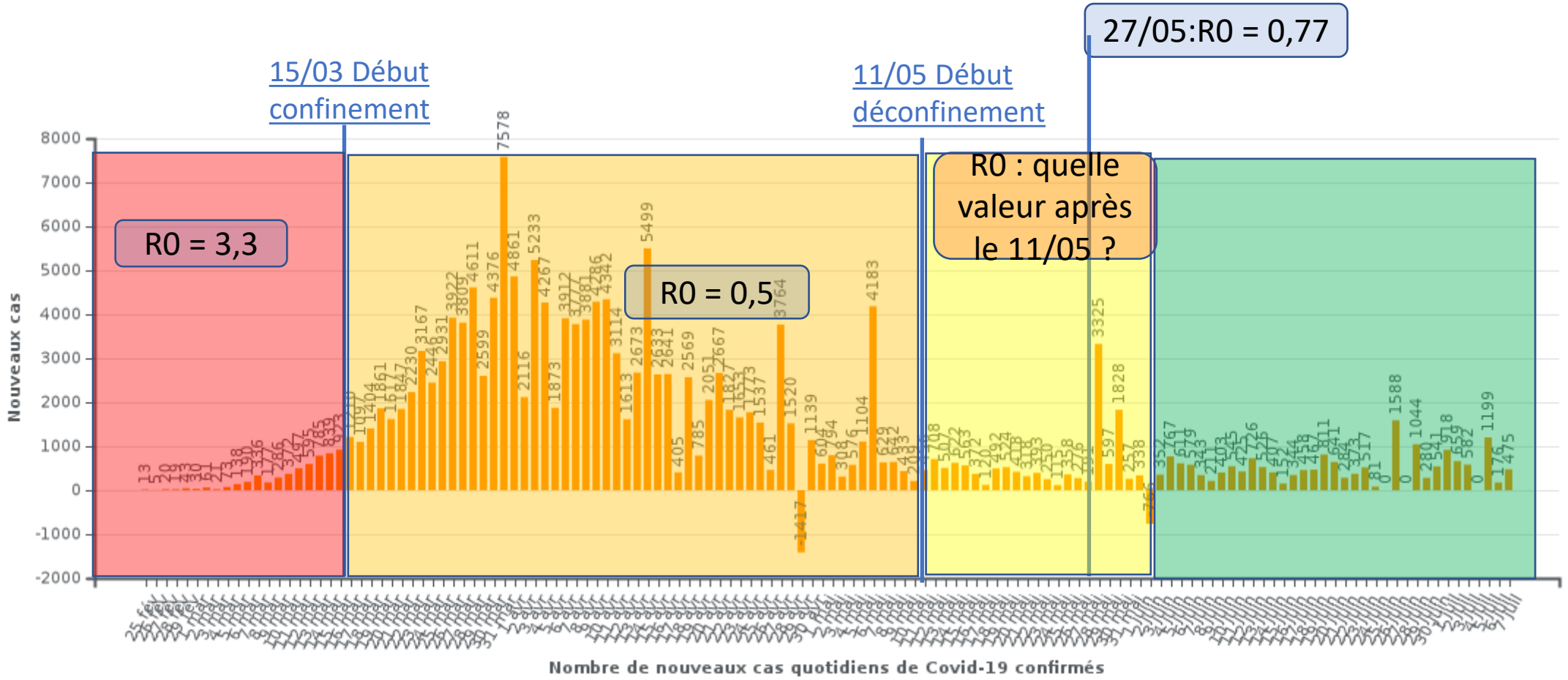
Chaine de contamination du virus en fonction de R0



Source : https://www.lemonde.fr/sante/video/2020/03/21/confinement-comment-la-distanciation-sociale-peut-eviter-des-morts_6033968_1651302.html

2 – StopCovid. Pandémie de Covid-19

Evolution du virus en France en fonction de R0



Source : https://fr.wikipedia.org/wiki/Pand%C3%A9mie_de_Covid-19_en_France#Cas_recens%C3%A9s_positifs_au_SARS-CoV-2

Fondation orange

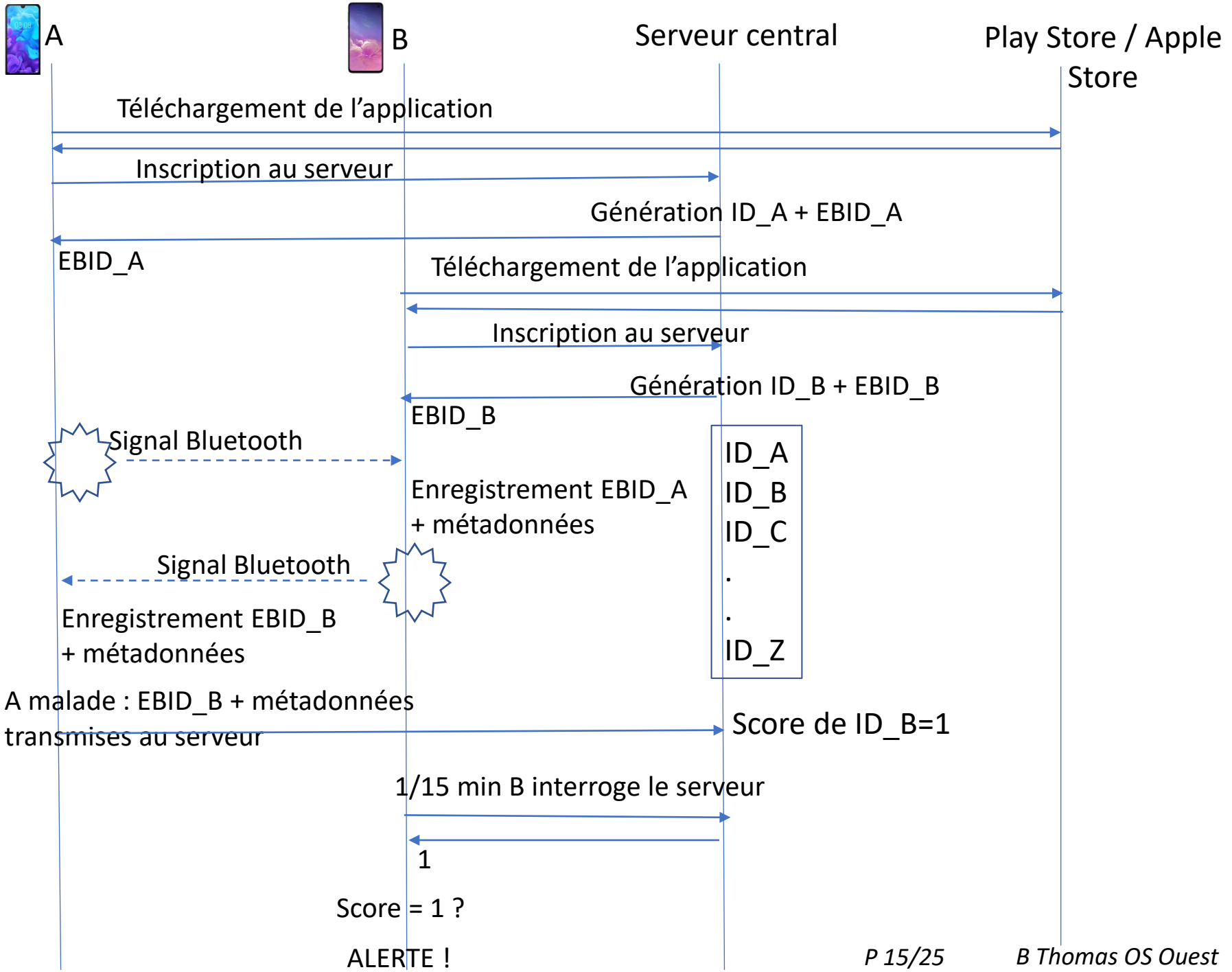
Annexes

2 - Le protocole ROBERT

Principe du traçage par BlueTooth Protocole Robert (France/INRIA)

ROBust and privacy-presERving proximity Tracing

- Téléchargement d'une application sur le mobile.
- Inscription à un serveur central (3DS Outscale, filiale de Dassault). *Utilisation Captcha*.
- Le serveur central génère et stocke un identifiant anonyme pour ce mobile. Il génère aussi des sous-identifiants éphémères (EBID) qu'il communique au mobile.(renouvelés toutes les 15 min)
- Chaque fois que le mobile A est en contact (pendant au moins 15 minutes à moins d'un mètre) avec un autre mobile B qui possède aussi l'application, A envoie son identifiant (EBID_A) à B qui l'enregistre. B fait la même chose et envoie son identifiant (EBID_B) à A qui l'enregistre. Echange aussi de la puissance et de la durée du signal.(Métadonnées)
- Après quelques jours, le mobile de A a enregistré plusieurs identifiants éphémères.
- A tombe malade, consulte un médecin qui diagnostique la Covid-19 → A se déclare « malade » sur l'application.→ L'application transmet les identifiants contacts (EBID) des 14 derniers jours au serveur central.
- Le serveur central calcule le « score » de B et met à jour son état à potentiellement infecté.
- B consulte le serveur central et lui demande son état. (Consultation toutes les 15 min)
- Le serveur répond 1 s'il est infecté, 0 sinon.
- Si la réponse est 1, l'application génère un message d'alerte sur le smartphone de B

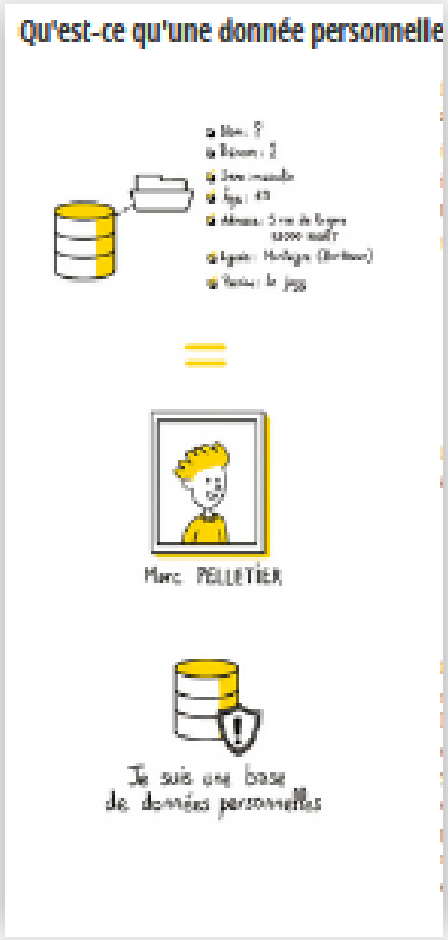


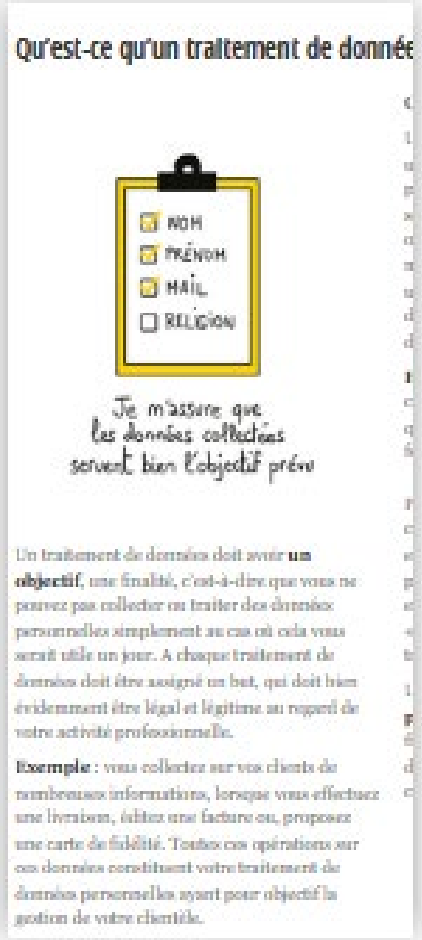
Protocole Robert

Annexes

3 - Le Règlement Général sur la Protection des Données - RGPD

RGDP – De quoi parle-t-on ?





Fondation orange

Orange Solidarité Ouest

Fondation