

LA CHRONIQUE DE  
GILLES DOWEK

# COMMUNIQUER TOUT EN RESTANT MASQUÉ

Dans le contexte du déconfinement, l'utilisation d'applications de traçage soulève des questions sur les moyens de protéger son identité.



Est-il possible d'échanger des informations sans avoir besoin de révéler son identité ou d'autres informations personnelles ?

**E**n mai dernier, l'organisation du déconfinement a suscité des débats sur les avantages et les inconvénients des « brigades sanitaires », des applications de traçage centralisées, décentralisées, etc. Ces discussions ont mis en lumière une question sur laquelle les informaticiens travaillent depuis longtemps : comment échanger de l'information sans dévoiler son identité ?

Imaginons par exemple que, pendant une épidémie, Alice et Bob se rencontrent et que, trois jours plus tard, Alice tombe malade. Comment peut-elle prévenir Bob pour qu'il s'isole, se fasse diagnostiquer et interrompe ainsi la chaîne de contamination ?

Une première approche consiste, pour Alice, à noter préalablement dans un carnet le numéro de téléphone de Bob et celui de toutes les personnes qu'elle rencontre afin de les prévenir si jamais elle tombe malade. Mais Bob ne veut pas nécessairement donner son numéro à Alice. Et s'il refuse, il ne sera pas prévenu. Un tel « algorithme », qui oblige à déclarer son identité à toutes les personnes que

l'on rencontre, est intrusif. Et il est peu efficace, car il est difficile de noter l'identité de toutes les personnes que l'on rencontre, surtout si elles ne coopèrent pas. C'est pourtant ainsi que procèdent en général les médecins pour éviter les épidémies : quand une personne tombe malade, un enquêteur cherche à identifier toutes les personnes avec qui elle a été en contact, pour leur proposer des soins.

## Il existe des protocoles respectueux de la vie privée

Pour éviter ces algorithmes intrusifs, les informaticiens en ont inventé d'autres, plus respectueux de la vie privée : par exemple, quand Alice et Bob se rencontrent, ils choisissent l'une et l'autre un pseudonyme, par exemple Xlthlx et Qfwfq, et communiquent à une tierce personne, Zoé, l'information que Xlthlx et Qfwfq se

sont rencontrés. Quand Alice tombe malade, elle indique à Zoé que la personne dont le pseudonyme est Xlthlx est malade et Zoé en déduit que la personne dont le pseudonyme est Qfwfq a été en contact avec une personne tombée malade depuis. Bob, tous les jours, demande à Zoé si Qfwfq a été en contact avec une personne malade.

Cet algorithme, dans lequel Zoé enregistre toutes les paires de pseudonymes à l'échelle d'un pays ou d'un continent, est dit « centralisé ». C'est approximativement ainsi que fonctionne le protocole ROBERT, qui est utilisé en particulier dans l'application de traçage StopCovid.

Mais il est aussi possible de se passer de Zoé. Bob peut lui-même noter qu'il a été en contact avec une personne dont le pseudonyme est Xlthlx et Alice peut prévenir le monde entier que la personne dont le pseudonyme est Xlthlx est malade, afin que Bob, parmi d'autres, sache qu'il a été en contact avec une personne malade.

Mais cet algorithme, dit « décentralisé », demande de rendre publique beaucoup d'informations, car tout un chacun doit savoir que la personne dont le pseudonyme est Xlthlx est malade, pour déterminer s'il a été en contact avec une personne tombée malade depuis ou non (dans l'algorithme centralisé, cette information n'est connue que d'Alice et de Zoé). C'est l'idée qui est derrière le protocole DP3T.

Dans les deux cas, Bob est prévenu sans avoir besoin de communiquer à Alice, ni à personne, son numéro de téléphone ou son nom. Ces protocoles sont donc peu intrusifs. Cependant, si une utilisation « normale » de ces protocoles est peu intrusive, ils présentent les uns et les autres de potentielles failles de sécurité.

L'épidémie de Covid-19 a fait émerger un domaine entier au sein de la théorie des protocoles et les chercheurs développent de nouveaux protocoles qui présenteront encore plus de garanties pour la vie privée, mais ils ne seront sans doute prêts que pour la prochaine épidémie... ■

**GILLES DOWEK** est chercheur à l'Inria, enseignant à l'École normale supérieure de Paris-Saclay et membre du Comité national pilote d'éthique du numérique.

# ABONNEZ-VOUS À POUR LA SCIENCE

3 FORMULES  
AU CHOIX

|                                                                                                           | FORMULE<br>PAPIER                          | FORMULE<br>PAPIER<br>+ HORS-SÉRIE           | FORMULE<br>INTÉGRALE                        |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------|---------------------------------------------|---------------------------------------------|
| Le magazine papier 12 numéros par an                                                                      | ✓                                          | ✓                                           | ✓                                           |
| Le magazine en version numérique 12 numéros par an                                                        |                                            |                                             | ✓                                           |
| Le hors-série papier 4 numéros par an                                                                     |                                            | ✓                                           | ✓                                           |
| Le hors-série en version numérique 4 numéros par an                                                       |                                            |                                             | ✓                                           |
| Accès à <a href="http://pouirlascience.fr">pouirlascience.fr</a><br>actus, dossiers, archives depuis 1996 |                                            |                                             | ✓                                           |
| <b>VOTRE TARIF D'ABONNEMENT</b>                                                                           | <b>59€</b><br>Au lieu de <del>82,80€</del> | <b>79€</b><br>Au lieu de <del>114,40€</del> | <b>99€</b><br>Au lieu de <del>174,40€</del> |
|                                                                                                           | <b>29 %</b><br>de réduction *              | <b>31 %</b><br>de réduction *               | <b>43 %</b><br>de réduction *               |

## BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à : Next2C – Service abonnements Pour La Science  
26 BD Président Wilson – CS 40032 – 67085 Strasbourg CEDEX – email : [pouirlascience@abopress.fr](mailto:pouirlascience@abopress.fr)

PAG20STD



**OUI, je m'abonne  
pour 1 an à  
POUR LA  
SCIENCE**

### 2 / J'indique mes coordonnées

☐ M. ☐ Mme

Nom : ..... Prénom : .....

Adresse : .....

Code postal : ..... Ville : .....

Téléphone : .....

Email : (indispensable pour la formule intégrale) .....

@ .....

J'accepte de recevoir les offres de Pour la Science ☐ OUI ☐ NON

### 3 / Je choisis mon mode de règlement

☐ Par chèque à l'ordre de Pour la Science

☐ Carte bancaire

N° : ..... Clé (Les 3 chiffres au dos de votre CB) : .....

Date d'expiration : ..... Clé (Les 3 chiffres au dos de votre CB) : .....

Signature obligatoire :

### 1 / Je choisis ma formule (merci de cocher)

☐ FORMULE  
PAPIER

• 12 n° du magazine papier

**59€**  
Au lieu de ~~82,80€~~

DIA59E

☐ FORMULE PAPIER  
+ HORS SÉRIE

• 12 n° du magazine papier  
• 4 Hors-série papier

**79€**  
Au lieu de ~~114,40€~~

PIA79E

☐ FORMULE  
INTÉGRALE

• 12 n° du magazine  
(papier et numérique)  
• 4 Hors-série  
(papier et numérique)  
• Accès illimité aux contenus en ligne

**99€**  
Au lieu de ~~174,40€~~

IIA99E

\* Réduction par rapport au prix de vente en kiosque et l'accès aux archives numériques. Durée d'abonnement : 1 an. Délai de livraison : dans le mois suivant l'enregistrement de votre règlement. Offre valable jusqu'au 31/03/2021 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site <https://boutique.pouirlascience.fr>. Photos non contractuelles.

Les informations que nous collectons dans ce bulletin d'abonnement nous aident à personnaliser et à améliorer les services que nous vous proposons. Nous les utiliserons pour gérer votre accès à l'intégralité de nos services, traiter vos commandes et paiements, et vous faire part notamment par newsletters de nos offres commerciales moyennant le respect de vos choix en la matière. Le responsable du traitement est la société Pour la Science. Vos données personnelles ne seront pas conservées au-delà de la durée nécessaire à la finalité de leur traitement. Pour la Science ne commercialise ni ne loue vos données à caractère personnel à des tiers. Les données collectées sont exclusivement destinées à Pour la Science. Nous vous invitons à prendre connaissance de notre charte de protection des données personnelles à l'adresse suivante : <https://rebrand.ly/charte-donnees-pls>. Conformément à la réglementation applicable (et notamment au Règlement 2016/679/UE dit « RGPD ») vous disposez des droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de vos données personnelles. Pour exercer ces droits (ou nous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à l'adresse [protection-donnees@pouirlascience.fr](mailto:protection-donnees@pouirlascience.fr).