Nations Unies A/75/147

Assemblée générale

Distr. générale
27 juillet 2020

Français
Original : anglais

Soixante-quinzième session
Point 72 b) de l'ordre du jour provisoire*.
Promotion et protection des droits de l'homme : questions relatives aux droits de l'homme, y compris les divers moyens de mieux assurer l'exercice effectif des droits de l'homme et des libertés fondamentales

Droit à la vie privée

Note du Secrétaire général

Le Secrétaire général a l'honneur de transmettre à l'Assemblée générale le rapport établi par le Rapporteur spécial sur le droit à la vie privée du Conseil des droits de l'homme, Joseph A. Cannataci, en application de la résolution 28/16 du Conseil.

* A/75/150.

20-10082 (F) 140920 170920

Rapport du Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci

Résumé

Dans le présent rapport, le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, propose une évaluation préliminaire des aspects de la pandémie de maladie à coronavirus (COVID-19) liés à la vie privée. La base de données factuelles nécessaire pour déterminer avec certitude si les mesures de lutte contre la COVID-19 portant atteinte à la vie privée sont nécessaires et proportionnées dans une société démocratique n'est pas encore disponible. Le Rapporteur spécial examine deux aspects particuliers de l'incidence de la COVID-19 sur le droit à la vie privée : la protection des données et la surveillance.

La surveillance et la recherche des contacts liées à COVID-19 peuvent prendre différentes formes et peuvent être manuelles ou technologiques, anonymes ou non, consensuelles ou non. La situation suscite des inquiétudes lorsque des dispositifs de surveillance traditionnellement utilisés pour garantir la sécurité de l'État sont proposés ou déployés à la hâte à des fins de santé publique pour suivre les données relatives à la santé, en cas de pandémie.

Lorsqu'un État décide qu'une surveillance technologique est nécessaire pour faire face à la pandémie mondiale de COVID-19, il doit s'assurer, après avoir démontré qu'une telle mesure est à la fois nécessaire et proportionnée, qu'il a adopté une loi qui prévoit explicitement de telles mesures de surveillance. La loi doit comporter des garanties qui, si elles ne sont pas suffisamment détaillées, ne peuvent être considérées comme adéquates en droit international.

Un rapport plus détaillé sur le sujet est prévu pour 2021, lorsque davantage de données factuelles seront disponibles pour permettre une évaluation plus précise.

I. Introduction

1. Les aspects de la pandémie de maladie à coronavirus (COVID-19) liés au droit à la vie privée sont un sujet approprié et opportun à aborder dans le cadre du présent rapport à l'Assemblée générale, étant donné que les droits de l'homme, y compris le droit à la vie privée, sont gravement et généralement compromis par la pandémie. En effet, les mesures élaborées dans le respect des droits de l'homme et fondées sur ces derniers permettent d'obtenir de meilleurs résultats dans la lutte contre la pandémie, de garantir un accès aux soins de santé pour tous et de préserver la dignité humaine[1].

2. Certes, la priorité est de sauver des vies, mais la lutte contre la COVID-19 et le respect des droits de l'homme, y compris le droit à la vie privée, ne sont pas incompatibles. En effet, lorsque la population est convaincue que son droit à la vie privée, par exemple, est respecté, elle se sent davantage en confiance et prête à soutenir de manière proactive les mesures prises par l'État pour prévenir la propagation du virus. Les droits de l'homme peuvent permettre aux États de gagner la confiance de leurs citoyens.

3. Le présent rapport constitue une évaluation préliminaire dans la mesure où la base de données factuelles nécessaire pour déterminer avec certitude si les mesures de lutte contre la COVID-19 portant atteinte à la vie privée sont nécessaires et proportionnées dans une société démocratique n'est pas encore disponible. Un rapport plus détaillé est prévu pour la mi-2021, lorsque l'on disposera de 16 mois de données factuelles pour permettre une évaluation plus précise.

4. Dans le présent rapport, le Rapporteur spécial examine deux aspects particuliers de l'incidence de la COVID-19 sur le droit à la vie privée : la protection des données et la surveillance. Il reconnaît que les questions relatives à la vie privée sont beaucoup plus nombreuses pendant la pandémie, notamment celles qui concernent les enfants, le genre, le rôle des algorithmes, etc.

Points essentiels

5. Les préoccupations relatives à la protection de la vie privée soulevées par la COVID-19 ne sont pas apparues du jour au lendemain. Elles se sont manifestées dans un contexte où le Rapporteur spécial sur le droit à la vie privée se penchait déjà sur les problèmes liés à la protection de la vie privée, tels que la surveillance et la protection adéquate des données relatives à la santé.

6. Si la pandémie de COVID-19 a suscité de nombreux débats sur l'intérêt de la recherche des contacts et du recours aux technologies permettant de suivre des personnes et les points de contact de ces dernières, l'utilisation de l'information et des technologies n'est pas une nouveauté dans la gestion des urgences de santé publique. Ce qui est préoccupant, dans certains États, ce sont les informations concernant la façon dont la technologie est utilisée et le degré d'intrusion et de contrôle exercé sur la population – qui n'auront probablement qu'un effet limité sur la santé publique.

7. La COVID-19 est une maladie et, en tant que problème de santé :

a) Dans plusieurs États, les lois relatives à la santé publique prévoient depuis longtemps des mesures pouvant être prises pour lutter contre les maladies

[1] Voir ONU, COVID-19 et droits humains – Réagissons ensemble ! note de synthèse, avril 2020.

transmissibles, qui fournissent une norme au regard de laquelle il convient d'examiner les mesures spécifiques liées à la COVID-19 ;

b) Les conditions nécessaires à la prise en compte des informations personnelles et relatives à la santé dans le cadre de la pandémie de COVID-19 doivent être envisagées en tenant compte de l'approche générale de la société en matière de traitement des données relatives à la santé.

8. Les mesures portant atteinte à la vie privée déployées au nom de la lutte contre la COVID-19, y compris les dispositifs de surveillance, ne peuvent et ne doivent pas être considérées hors contexte. Elles doivent être examinées dans le cadre d'une politique holistique et exhaustive régissant la surveillance dans les États respectifs et en cohérence avec celle-ci.

9. En ce qui concerne l'utilisation des technologies modernes pour contrôler la propagation de la pandémie, de manière générale, la sous-discipline de l'ingénierie de la protection de la vie privée n'a pas obtenu l'attention qu'elle méritait.

10. Les recommandations précédemment formulées par le Rapporteur spécial, en particulier celles concernant la surveillance exercée par les États (A/HRC/37/62) et la protection des aspects liés à la vie privée des données relatives à la santé (A/74/277), fournissent des lignes directrices destinées à aider les États à faire face à la pandémie de COVID-19 tout en respectant leurs obligations en matière de droit international des droits de l'homme[2].

II. Protection et surveillance des données pendant la pandémie de COVID-19

11. Il semble opportun d'examiner brièvement les mesures de santé publique ordinaires antérieures à la COVID ayant trait aux maladies à déclaration obligatoire et aux maladies transmissibles.

12. Des lois et des procédures régissant les maladies transmissibles sont en place depuis des siècles, à l'instar des mesures de quarantaine strictes – et des hôpitaux de quarantaine – mis en place pour lutter contre certaines pandémies telles que la peste bubonique. Plus récemment, le rôle des États dans la mise en œuvre d'interventions et de mécanismes de santé publique a été illustré par le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord. Au terme d'une période de près de deux siècles, la perception de la santé publique a commencé à changer au Royaume-Uni, notamment grâce aux travaux de John Snow sur l'épidémie de choléra de 1854 à Broad Street et à une meilleure compréhension des risques de maladies transmises par l'eau. En 1939, un système d'inspecteurs de la santé fut mis en place au Royaume-Uni, dans certaines parties de l'Empire britannique et au-delà. Au niveau local, les inspecteurs de la santé veillaient à l'application des lois relatives à l'hygiène et à la salubrité – des raccordements aux égouts aux installations de lavage des mains dans les magasins. Ils étaient déjà en première ligne de la lutte contre les maladies transmissibles comme le choléra et la tuberculose avant le début de la Seconde Guerre mondiale, qui a donné lieu à certaines situations, notamment des logements surpeuplés et insalubres, où ces maladies contagieuses pouvaient se propager plus facilement. Les inspecteurs de la santé étaient normalement des fonctionnaires spécialement formés qui devaient – et

[2] Les annexes et l'exposé des motifs (y compris des versions complètes non éditées) de ces rapports sont disponibles à l'adresse suivante : www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

doivent toujours – respecter des règles strictes en matière d'établissement de rapports et de signalement, de sorte que les professionnels de la santé publique soient avertis de l'apparition de maladies infectieuses graves. Les praticiens prenaient alors des mesures pour maîtriser et éradiquer ces maladies transmissibles.

13. Du point de vue juridique, l'évolution des mesures de santé publique s'est donc traduite par la divulgation obligatoire aux autorités de santé publique de la découverte d'un certain type de maladie. C'est ce qu'on appelle une maladie à déclaration obligatoire.

14. La COVID-19 est une maladie à déclaration obligatoire. Dans un certain État Membre, il s'agit de la 66e maladie inscrite sur la liste des maladies à déclaration obligatoire. Par conséquent, 65 maladies avaient déjà été identifiées et signalées aux autorités nationales de santé publique.

15. Le transfert de données personnelles sensibles, lors de la déclaration d'une maladie transmissible, est une mesure ordinaire au niveau national, mais elle revêt également une dimension internationale. Bien qu'il ne constitue pas une mesure extraordinaire, le transfert de données de ce type peut conduire à des situations dans lesquelles des mesures extraordinaires sont invoquées.

16. Une fois informées de l'incidence d'une maladie, les autorités de santé publique se voient accorder par la loi un arsenal d'options et de mesures, allant de l'attentisme à la plus stricte des quarantaines. En d'autres termes, une fois qu'elles reçoivent des données de santé concernant un patient donné, elles sont censées prendre une décision éclairée sur ce qu'il convient de faire.

17. Dans la plupart des pays développés, les données personnelles relatives à la santé sont traitées de manière confidentielle et archivées en fonction des besoins, notamment le stockage à des fins épidémiologiques. Les autorités de santé publique ont pour objectif principal de recourir à l'épidémiologie pour prévenir et combattre les épidémies. Elles s'y sont employées – généralement avec succès – avant même l'ère des smartphones et de la COVID-19. En effet, il apparaît de plus en plus clairement que la plupart des pays développés qui ont agi de manière réfléchie et en temps utile avaient, à la mi-juillet 2020, réussi à lutter contre la COVID-19, voire à la maîtriser, en utilisant des méthodes établies de longue date et sans recourir aux technologies liées aux smartphones[3].

18. La recherche des contacts est l'outil classique utilisé par les organismes de santé publique pour enrayer la propagation des maladies transmissibles. Elle constitue une atteinte à la vie privée en ce qu'elle oblige le patient à révéler avec qui il a pu être en contact pendant une période donnée. De manière générale, dans la plupart des pays, il s'agit implicitement de l'un des cas exceptionnels où le droit à la vie privée n'a pas à être absolu. La nécessité d'arrêter la propagation d'une épidémie potentielle est l'un des rares cas où l'intérêt public est socialement considéré comme supérieur au droit à la vie privée ou, en définitive, à d'autres droits tels que la liberté de circulation et la liberté d'association. En bref, afin d'éviter la propagation du choléra ou de la tuberculose, par exemple, les autorités ont le droit : a) de savoir qui est atteint de la maladie ; et b) d'ordonner un isolement strict selon des règles sanitaires strictes, entre autres.

[3] Voir, par exemple, la Grèce et Malte ; si le/la principal(e) critère/mesure de succès ou d'échec correspondait au nombre de décès par million d'habitants, ces pays pourraient faire figure d'exemples de gestion réussie du virus, sans surveillance technologique.

19. Toutes les données factuelles disponibles laissent à pense qu'il n'existe actuellement aucune alternative ou solution de substitution raisonnable à la recherche des contacts qui permette d'arrêter la contagion, de la limiter et le plus souvent de la contenir. Il ne fait actuellement aucun doute que, chaque fois qu'elle est envisageable, la recherche des contacts fonctionne bien et que, bien qu'elle porte atteinte à la vie privée, elle peut être considérée comme une mesure nécessaire.

20. Les procédures manuelles de recherche des contacts strictes et portant atteinte à la vie privée peuvent également être considérées comme proportionnées à la nécessité de prévenir, de contenir ou de combattre un risque pour la santé publique tel qu'une épidémie. La nature et la quantité des informations personnelles requises et généralement collectées dans le cadre d'un exercice de recherche des contacts sont celles qui sont strictement nécessaires pour enrayer la propagation de la maladie en essayant d'identifier qui pourrait également avoir été infecté. Ainsi, par exemple, le support d'informations privées le plus exhaustif du patient – son smartphone – ne peut être consulté ou saisi dans le cadre d'un exercice traditionnel de recherche des contacts. Les autorités sanitaires, souvent accompagnées de policiers chargés de faire appliquer la loi sur la santé, téléphonent et/ou rendent visite aux personnes avec lesquelles la personne contaminée a pu être en contact et font appliquer la ligne de conduite prescrite – généralement un isolement pendant une période donnée.

21. Les pouvoirs permettant d'effectuer des perquisitions et des saisies sont depuis longtemps liés au droit à la vie privée. La santé publique est considérée comme une question d'intérêt commun tellement primordiale que, dans certains pays, les pouvoirs de perquisition et de saisie ordinaires (et non extraordinaires) d'une autorité de santé publique sont souvent plus importants que ceux de la police. Ils font rarement la une des journaux et la présomption en faveur de la santé publique est très présente. Ainsi, dans certains États, alors que la perquisition de locaux par la police nécessite souvent un mandat judiciaire ou exécutif, il n'en va pas de même si la perquisition doit être effectuée en vertu d'une loi de santé publique, même si le responsable de la santé doit parfois être accompagné d'un agent de police lors d'une telle perquisition.

A. Mesures extraordinaires

22. Dans la plupart des États, une loi accorde aux autorités de santé publique le pouvoir de prendre des mesures extraordinaires. Cette procédure s'inscrit normalement dans le cadre d'une urgence de santé publique, qui peut être soit nationale soit localisée, et qui doit être formellement déclarée pour que des mesures extraordinaires puissent être invoquées. Une « urgence de santé publique » est souvent définie de manière vague, voire pas du tout, et, dans certains pays, elle peut être définie dans la loi comme étant ce que le chef de l'autorité de santé publique décide. Les définitions de l'Organisation mondiale de la Santé (OMS), par exemple, donnent des indications à ce sujet.

23. Les pouvoirs d'urgence sanitaire sont énormes et peuvent, littéralement, inclure tout ce qui est imaginable [voir l'alinéa g) ci-après] et qui est « nécessaire pour réduire, supprimer ou éliminer toute menace pour la santé publique »[4]. L'autorité de santé publique peut :

a) Séparer ou isoler toute personne, quel que soit le lieu ;

[4] Malte, Loi sur la santé publique, chapitre 465 des Lois de Malte, art. 15.

b) Évacuer toute personne, quel que soit le lieu ;

c) Bloquer l'accès à n'importe quel lieu ;

d) Contrôler le mouvement de tout véhicule ;

e) Obliger toute personne à se soumettre à un examen médical ;

f) Ordonner que toute substance ou tout objet soit saisi, détruit ou éliminé ;

g) Ordonner toute autre mesure qu'elle juge appropriée.

24. Lorsqu'un État accorde à ses autorités de santé publique des pouvoirs aussi étendus en cas d'urgence de santé publique, il convient de se demander si l'accès régulier ou constant à l'appareil électronique d'une personne, tel qu'un smartphone, ou la surveillance des déplacements et des contacts d'un tiers par la géolocalisation d'un smartphone est une mesure nécessaire et proportionnée.

25. La question se pose également lorsque l'on constate que certains États n'ont pas attendu de traverser une urgence de santé publique pour établir une base juridique permettant d'accéder à l'appareil électronique d'une personne. En effet, dans certains pays, cette possibilité relève du pouvoir ordinaire (et non extraordinaire) des autorités sanitaires, qui peuvent « inspecter, extraire ou saisir tout fichier ou se procurer une copie de tout fichier pertinent pour la santé publique, quelle que soit la forme sous laquelle il est enregistré et, dans le cas où un fichier est conservé sur un ordinateur, lesdites autorités :

i) doivent avoir accès à tout ordinateur, à tout appareil ou matériel associé qui est ou a été ou aurait pu être utilisé en lien avec les fichiers, les inspecter et en vérifier leur fonctionnement ;

ii) peuvent obliger toute personne responsable de l'ordinateur, de l'appareil ou du matériel, ou autrement concernée par le fonctionnement de ceux-ci, à leur fournir l'assistance dont elles peuvent raisonnablement avoir besoin »[5].

26. Ces dispositions visent sans doute à fournir un accès ciblé dans une situation normale et non pas un accès à un large pourcentage ou à la totalité de la population d'un État tout entier, comme cela a été envisagé, testé et déployé à ce jour dans le cadre de la crise de la COVID-19.

B. Réglementation relative aux données de santé et à la vie privée

27. Les données liées à la COVID-19 sont des données relatives à la santé et constituent la première catégorie de données personnelles à bénéficier de niveaux de protection spéciaux. On peut considérer que la protection des données de santé fut le précurseur des règles et réglementations en matière de protection des données. Le serment d'Hippocrate – dont on pense qu'il a été prononcé entre le VIe et le IIIe siècle avant J.-C. – exige des médecins qu'ils préservent le secret et la confidentialité des informations médicales de leurs patients[6].

28. Toute situation médicale génère inévitablement des données personnelles qui doivent être traitées selon les normes juridiques et éthiques les plus strictes. Le débat sur le droit à la vie privée aux États-Unis d'Amérique, en 1973, a débouché sur les

[5] Ibid., art. 6, 1), c).

[6] Institute of Medicine, Health Data in the Information Age: Use, Disclosure, and Privacy (Washington, D.C., National Academies Press, 1994)

premiers principes relatifs aux données de santé, tandis qu'en Europe, la toute première recommandation du Conseil de l'Europe sur la protection des données, en 1980, concernait les données médicales et a précédé la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) de janvier 1981. La recommandation du Conseil a depuis lors été révisée à deux reprises (en 1997 et en 2019).

29. La numérisation des données a entraîné une croissance significative du volume de données de santé traitées et a permis de disposer de profils de patients plus complets. Elle a non seulement abouti à une amélioration de la qualité des données et facilité le partage des données entre les professionnels de la santé, augmentant ainsi le potentiel d'amélioration de la prestation des soins de santé.

30. La personne à laquelle les données se rapportent présente manifestement un intérêt pour ces données et pour leur contrôle. Les parents de cette personne, les tiers ayant une relation transactionnelle avec elle et d'autres parties prenantes indirectes, telles que la communauté de la personne, le grand public et les chercheurs médicaux, ont également un intérêt pour les données de cette personne. Ces intérêts sont divers, variés et inégaux, et il convient par conséquent de prendre diverses dispositions spécifiques pour garantir le respect que mérite le droit à la vie privée, conformément à l'article 12 de la Déclaration universelle des droits de l'homme.

31. Le nombre de parties prenantes indirectes intéressées par les données relatives à la santé augmente de manière exponentielle depuis quelques années, et cette croissance se traduit également par des tensions entre les différentes parties prenantes, ce qui entraîne des problèmes juridiques et éthiques de plus en plus complexes.

32. Le règlement général sur la protection des données[7] de l'Union européenne et la Convention 108[8] du Conseil de l'Europe reconnaissent tous deux les données relatives à la santé comme étant une « catégorie spéciale de données ». Aux termes de la Convention, le traitement des données relatives à la santé n'est autorisé que si des garanties appropriées sont prévues par la loi. Bien que le règlement envisage davantage de scénarios selon lesquels les données relatives à la santé peuvent être traitées, le traitement de ces dernières, par opposition aux données personnelles plus générales, reste soumis à des restrictions plus strictes. Le règlement permet aux États membres de l'Union européenne de « maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé[9] ».

33. En mars 2019, le Comité des Ministres du Conseil de l'Europe a adopté la Recommandation CM/Rec(2019)2 sur la protection des données relatives à la santé[10]. Celle-ci contient un ensemble de principes destinés à protéger les données relatives à la santé, intégrant à la fois les dispositions de la Convention 108 et les ajouts introduits dans la version modernisée de la Convention de 2018 pour la protection des personnes à l'égard du traitement des données à caractère personnel, connue sous le

[7] Union européenne, Règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 2016, art. 9(1).

[8] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), 1981, art.6.

[9] Union européenne, Règlement général sur la protection des données, art. 9(4).

[10] Voir https://edoc.coe.int/fr/droit-international/7968-protection-des-donnees-relatives-a-la-sante-recommandation-cmrec20192.html

nom de Convention 108+, qui devaient permettre à la Convention de répondre aux nouveaux défis de l'ère numérique[11].

34. En octobre 2019, le Rapporteur spécial a officiellement présenté à l'Assemblée générale la Recommandation sur la protection et l'utilisation de données de santé (A/74/277, annexe), laquelle reconnaît le caractère sensible et la grande valeur commerciale des données relatives à la santé, et fournit une base de référence internationale commune pour les normes minimales de protection des données relatives à la santé[12]. La Recommandation vise à compléter les réglementations et recommandations existantes, tout en tenant compte de la hausse du traitement numérisé des données de santé de la population. Elle aborde la question des lacunes et des incertitudes engendrées par le déploiement des dossiers médicaux électroniques, des applications mobiles, du marketing ciblé, de l'accès des employeurs et des assureurs aux données relatives à la santé, ainsi que des besoins de protection des données propres à certaines catégories de personnes, telles que les personnes handicapées et les réfugiés.

35. La Recommandation montre comment les garanties en matière de protection des données ont évolué au fil du temps pour suivre les progrès de la société et de la technologie. Chaque fois que des crises internationales ont éclaté – sans oublier celles causées par des pandémies mondiales – les règles et recommandations existantes ont été mises à l'épreuve. Les motifs de santé publique ont toujours fourni, et fournissent encore, une base juridique légitime pour le traitement des données à caractère personnel et des données relatives à la santé dans le but de combattre et de contenir la propagation d'une pandémie. La Recommandation précise que le traitement des données relatives à la santé est légitime lorsqu'il est effectué dans l'intérêt public et que des garanties adéquates, notamment sous la forme de dispositions de sécurité et de mesures institutionnelles, sont mises en place[13].

36. Les données relatives à la santé de la population sont devenues un outil essentiel utilisé par les gouvernements et les scientifiques du monde entier aux fins de la lutte contre la propagation de la COVID-19. Un certain nombre de gouvernements, et souvent leurs services répressifs respectifs, traitent des données relatives à la santé (parfois en les combinant avec d'autres métadonnées personnelles[14], telles que des données de géolocalisation) en vue de faire respecter les obligations de quarantaine ou d'auto-isolement et d'alimenter la recherche visant à définir les mesures restrictives nécessaires en matière d'interaction sociale, entre autres. Dans certains cas, les entités ayant accès à ces données personnelles sensibles sont des acteurs indirects récemment apparus, et leur brusque irruption se fait parfois au détriment de politiques cohérentes qui protègent le droit à la vie privée et l'intégrité des données relatives à la santé.

---

[11] Conseil de l'Europe, « Protection des données relatives à la santé : le Conseil de l'Europe publie de nouvelles lignes directrices », communiqué de presse (mars 2019). Disponible à l'adresse suivante : https://www.coe.int/fr/web/portal/-/health-related-data-council-of-europe-issues-new-guidelines

[12] A/74/277, annexe, par. 4.1 c).

[13] Ibid., par.4.1 f).

[14] Privacy International définit les métadonnées comme « tout ensemble de données qui décrit d'autres données telles que la date et l'horaire d'un message électronique, le nom de l'expéditeur, le nom d'un destinataire, la localisation de l'appareil, etc., et fournit des informations y relatives ». Voir « Extraordinary powers need extraordinary protection », 20 mars 2020. Disponible à l'adresse suivante : https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections.

37. Dans le cadre de la lutte contre la pandémie de COVID-19, les gouvernements et les entreprises technologiques traitent les données relatives à la santé en utilisant la technologie pour suivre les personnes dont le test de dépistage de la maladie s'est révélé positif et, par extension, toutes les personnes avec lesquelles celles-ci ont pu entrer en contact. Cette extension technologique du processus traditionnel de recherche des contacts repose bien souvent sur le traitement des données générées par les téléphones portables. Cette approche a été testée aux fins du contrôle de précédentes crises pandémiques, par exemple, en 2014, dans la gestion de la propagation du virus Ebola en Afrique de l'Ouest, et en 2015, dans la lutte contre le syndrome respiratoire du Moyen-Orient (MERS)[15]. Aujourd'hui plus que jamais, et compte tenu notamment de la généralisation de l'utilisation des téléphones portables, cette méthode de recherche des contacts peut permettre aux États et à leurs autorités de santé publique respectives de contrôler avec succès le risque suscité par les pandémies telles que la COVID-19, ainsi que de surveiller la propagation et l'évolution à long terme d'une maladie. Le traitement des données relatives à la santé des personnes devrait faire l'objet d'une réglementation appropriée, inspirée de la Recommandation du Rapporteur spécial sur la protection et l'utilisation des données de santé, et qui devrait être inscrite dans la législation nationale des États.

38. La Recommandation fournit les orientations nécessaires aux États qui choisissent de légiférer en faveur d'un traitement sécurisé des données relatives à la santé, même dans des scénarios mondiaux sans précédent tels que celui de la COVID-19. Chaque partie prenante indirecte est incluse dans le champ d'application de la Recommandation, étant donné que celle-ci n'est pas seulement applicable aux professionnels de la santé et aux médecins, mais englobe plutôt le « traitement des données de santé dans tous les secteurs de la société, public et privé compris[16] ». Conformément à ladite Recommandation, tous les responsables du contrôle et du traitement des données sont tenus de prendre toutes les mesures appropriées pour s'acquitter de leurs obligations en matière de données de santé et doivent être en mesure de démontrer à une autorité de surveillance compétente que tous les traitements de données respectifs sont effectivement menés à bien conformément aux obligations applicables[17]. Cette exigence fait en outre écho à l'appel lancé aux États en faveur de la mise en place d'autorités de surveillance indépendantes et capables de contrôler la mise en œuvre des mesures de surveillance nécessaires, même à orientation épidémiologique, comme nous l'expliquerons plus loin. Un comptage très approximatif effectué par le titulaire du mandat suggère que, dans le meilleur des cas, moins de 60 États respectent partiellement les normes minimales énoncées dans la Recommandation. En d'autres termes, plus de 70 % des États membres de l'Organisation des Nations Unies sont bien loin de respecter ces normes. Toute personne désireuse d'en savoir plus doit donc se poser une question essentielle : dans quelle mesure, le cas échéant, mon pays applique-t-il effectivement les normes énoncées dans la Recommandation sur la protection et l'utilisation des données de santé ?

[15] Privacy International, « Extraordinary powers need extraordinary protections », 20 mars 2020.
[16] A/74/277, annexe, par. 2.1.
[17] Ibid., par. 4.5.

39. Il convient de noter que la Convention 108+ exige que, « même dans des situations particulièrement difficiles, les principes de protection des données soient respectés [18] ». Il importe d'être conscient que les États sont tenus de protéger la santé de leur population, mais également de protéger leur droit à la vie privée, tant dans les mesures prises à court terme que dans la planification à long terme. Ces deux éléments ne sont pas contradictoires et les États sont encouragés à envisager la Recommandation comme un modèle de règles et de législation qui fournirait la base juridique appropriée pour le traitement des données relatives à la santé, même si celui-ci peut exceptionnellement comporter une composante surveillance.

40. Un an après la soumission officielle de la Recommandation à l'Assemblée générale, et compte tenu de la crise sanitaire actuelle de la COVID-19, il est nécessaire de prendre des mesures urgentes pour remédier aux faibles niveaux actuels de conformité aux normes énoncées dans la Recommandation.

C. Surveillance et données relatives à la santé

Surveillance par les services de répression, de renseignement et de sécurité

41. Le mandat du Rapporteur spécial sur le droit à la vie privée a été créé en 2015 en réaction directe aux révélations d'Edward Snowden sur la surveillance exercée par l'État. Après plus de deux ans de vastes consultations, en mars 2018, le Rapporteur spécial a soumis au Conseil des droits de l'homme un projet d'instrument juridique sur la surveillance exercée par les services répressifs et les services de sécurité et de renseignement[19].

42. Le document décrit un grand nombre de principes de base et de mesures minimales (garanties et recours) qu'un État devrait respecter ou introduire pour se conformer à l'article 11 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques. Comme l'ont souligné les principaux tribunaux régionaux, à l'heure actuelle, un mécanisme de surveillance est autorisé à condition que les mesures de surveillance soient prévues par la loi et qu'elles soient nécessaires et proportionnées à la vie dans une société démocratique[20]. Si une telle surveillance doit être mise en œuvre, il apparaît clairement que la principale garantie réside dans un contrôle efficace et opportun de celle-ci.

43. Au nombre des normes minimales recommandées comme étant essentielles figure l'existence d'une autorité indépendante chargée du contrôle *ex ante* et *ex post* de toutes les mesures de surveillance prises tant par les services répressifs que par les services de renseignement. Le droit national de chaque État devrait donc garantir un contrôle efficace des services répressifs et des services de sécurité et de renseignement, exercé par des autorités de surveillance indépendantes et dotées de

---

[18] Conseil de l'Europe, « Déclaration conjointe sur le droit à la protection de données dans le contexte de la pandémie à COVID-19 par Alessandra Pierucci, Présidente du Comité de la Convention 108 et Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe », 30 mars 2020. Disponible à l'adresse suivante : https://rm.coe.int/covid19-declaration-conjointe/16809e0a17.

[19] Voir le projet d'instrument juridique sur les activités de surveillance menées par les États et sur la vie privée. Disponible à l'adresse suivante : www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

[20] Voir Cour européenne des droits de l'homme, *Big Brother Watch et autres c. Royaume-Uni* (requêtes nos 58170/13, 62322/14 et 24960/15), arrêt du 13 septembre 2018.

ressources suffisantes. Comme le confirme la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice européenne, la surveillance doit être de préférence ciblée et toujours menée de manière appropriée, avec l'autorisation préalable d'une autorité extérieure indépendante, comprenant de préférence, mais pas nécessairement, au moins une personne habilitée à ester en justice.

44. La grande majorité des États sont très loin d'atteindre ces normes. En juillet 2020, sur les 193 États Membres de l'Organisation des Nations Unies, seule une infime minorité (moins de 10 %) était en passe de satisfaire aux normes nécessaires pour qu'un gouvernement puisse garantir la protection et le respect de la vie privée de sa population lorsqu'il s'agit de surveillance exercée par l'État.

45. La crise de la COVID-19 se complique encore lorsque des appareils de surveillance traditionnellement utilisés pour garantir la sécurité de l'État sont proposés ou déployés à la hâte dans un but de santé publique tel que la lutte contre la COVID-19.

46. Afin que chaque personne soit protégée de toute ingérence dans la jouissance de son droit à la vie privée, les États doivent être soumis aux procédures réglementaires prévues par les lois nationales. La législation des États doit prévoir des mesures de précaution visant à garantir qu'une surveillance ne peut être mise en place tant qu'il n'a pas été prouvé, devant une autorité indépendante et compétente qu'une telle mesure est légale, nécessaire et proportionnée à l'objectif recherché, c'est-à-dire « exclusivement en vue d'assurer la reconnaissance et le respect des droits et libertés d'autrui et afin de satisfaire aux justes exigences de la morale, de l'ordre public et du bien-être général dans une société démocratique[21] ».

47. Le Rapporteur spécial recommande également que les États complètent ces mesures en incorporant dans leur système juridique interne les normes et garanties énoncées dans la Convention 108+, en particulier l'article 11, et que toute information à caractère personnel échangée entre les services de renseignement et les services répressifs aux niveaux national et international soit soumise à la surveillance de leurs autorités nationales indépendantes.

48. Tous les États sont encouragés à introduire ou à actualiser, dans leur système juridique interne, une loi détaillée sur la surveillance par les services de répression et les services de sécurité et de renseignement qui soit assortie de garanties de contrôle, de manière à fournir une base juridique aux mesures de surveillance qui sont nécessaires et proportionnées dans une société démocratique, ainsi que pleinement conformes à l'article 9 de la Convention 108 et à l'article 11 de la Convention 108+. Le Rapporteur spécial s'est employé à encourager le renforcement de la sensibilisation et l'échange de bonnes pratiques en matière de contrôle de la surveillance par la création du Forum international de contrôle des services de renseignement, qui se réunit chaque année depuis 2016. Les États sont invités à s'engager auprès de leurs pairs et à participer activement au Forum.

La surveillance en épidémiologie – un outil pour lutter contre la propagation des maladies

49. Au cours de leurs études, les étudiants en épidémiologie, par opposition aux juristes spécialisés dans la protection de la vie privée, apprendraient que la surveillance est définie comme « l'examen continu de tous les aspects liés à l'apparition et à la propagation d'une maladie qui sont utiles à des fins de contrôle

[21] Déclaration universelle des droits de l'homme, art. 29 2).

efficace », et qu'elle implique «la collecte, l'analyse, l'interprétation et la diffusion systématiques de données relatives à la santé ». La détection et le diagnostic des maladies est « l'acte visant à découvrir une nouvelle maladie ou un nouvel événement pathologique, émergent ou réémergent, et à en identifier la cause ». Le diagnostic est «la pierre angulaire des mesures efficaces de contrôle et de prévention des maladies, y compris la surveillance[22] ».

50. La surveillance, en matière d'épidémiologie, a toujours été considérée comme la clé du contrôle efficace de la propagation d'une maladie. Cette surveillance porte notamment sur les informations relatives aux données médicales, telles que les diagnostics cliniques, les taux de mortalité, ainsi que sur d'autres informations pertinentes nécessaires pour détecter et suivre la maladie, en termes de personnes, de lieu et de temps. Cette approche[23] a été particulièrement renforcée avec la propagation du VIH/sida, de l'hépatite C et de la dengue hémorragique.

51. Chaque pays jouant un rôle dans la propagation des épidémies, les systèmes nationaux de notification relatifs à la propagation des maladies infectieuses sont établis conformément aux cadres juridiques des différents pays, généralement comme indiqué ci-dessus.

52. L'OMS a pour mandat de diriger et de coordonner la surveillance mondiale de ces notifications. Le Règlement sanitaire international (2005) constitue un accord juridiquement contraignant avec 196 pays, à savoir tous les États membres de l'OMS et certains États non membres. Les États signataires sont tenus de signaler tout événement susceptible de constituer « une urgence de santé publique de portée internationale ». Une telle urgence « s'entend d'un événement extraordinaire dont il est déterminé ... i) qu'il constitue un risque pour la santé publique dans d'autres États en raison du risque de propagation internationale de maladies et ii) qu'il peut requérir une action internationale coordonnée ».

53. L'obligation générale de notification étend donc le champ d'application au-delà des maladies à déclaration obligatoire ou transmissibles, et vise spécifiquement à permettre la détection précoce de tous les événements de santé publique susceptibles d'avoir de graves conséquences internationales. Le Règlement identifie notamment des maladies spécifiques qui sont considérées comme particulièrement préoccupantes et oblige les signataires à notifier immédiatement à l'OMS tout cas isolé de certaines maladies, notamment le syndrome respiratoire aigu sévère (SRAS), quel que soit le contexte dans lequel il survient.

54. Le partage des données de l'OMS lors d'une urgence de santé publique « donne la possibilité de mener des analyses qui permettent de comprendre l'urgence de la manière la plus détaillée possible, en vue de faire en sorte que les décisions soient fondées sur les meilleures données factuelles disponibles ». Chacune des trois catégories ci-après doit tenir compte de différents facteurs :

a) surveillance, épidémiologie et interventions d'urgence, notamment dans les établissements de santé ;

---

[22] Institute of Medicine, Global Infectious Disease Surveillance and Detection : Assessing the Challenges-Finding Solutions, résumé de l'atelier (Washington D.C., National Academies Press, 2007).

[23] On estime que la pandémie de « grippe espagnole », qui a fait rage entre 1918 et 1919, a tué quelque 40 millions de personnes dans le monde. Elle a fait ressortir la nécessité d'une surveillance efficace de la santé publique visant à détecter et à prévenir de telles pandémies.

b) séquences génétiques ;

c) études observationnelles et essais cliniques.[24].

55. Les États parties au Règlement sanitaire international sont encouragés à partager les données dans le but de prévenir la propagation d'une éventuelle pandémie mondiale, et l'OMS s'engage à ne publier que des données anonymes. Les données publiées incluraient les données issues de la surveillance et du contrôle, telles que communiquées par les États parties, ainsi que celles résultant de l'intervention d'urgence menée par l'État concerné. Une telle intervention pourrait par exemple se traduire par la recherche de contacts et des informations relatives au traitement. Les données publiées peuvent également inclure des informations sur les installations médicales, y compris leur emplacement et leurs ressources. L'article 45 du Règlement énonce les exigences de protection de ces données, y compris la suppression de tout identifiant personnel et de toute donnée liée à la géolocalisation.

56. Le rapport de l'OMS sur la surveillance mondiale des maladies infectieuses à tendance épidémique énumère les types de données de surveillance qui sont généralement collectées et communiquées en ce qui concerne les maladies infectieuses. L'une des méthodes de surveillance consiste à communiquer des informations relatives à la confirmation des cas observés dans les services de santé. C'est ce qu'on appelle la surveillance passive, car elle revient à signaler les cas qui n'ont pas été activement recherchés. Une autre méthode consiste à surveiller des souches pathogènes. Certaines maladies, telles que la grippe, présentent de nouvelles souches, qui apparaissent fréquemment. Enfin, une dernière méthode consiste à effectuer un dépistage actif et systématique de la maladie auprès de la population afin de recenser les cas à l'échelle locale.

57. Par conséquent, les pratiques de surveillance, de contrôle et de recherche des contacts ne sont pas des concepts nouveaux dans le cadre de la recherche épidémiologique. L'OMS fait référence à ces mesures en vue de protéger les populations contre la propagation des éventuelles épidémies.

58. L'OMS a énuméré certains des objectifs liés à la surveillance de la COVID-19, à savoir :

a) Permettre la détection, l'isolement, le dépistage et la gestion rapides des cas suspects ;

b) Identifier et suivre les contacts ;

c) Orienter la mise en œuvre des mesures de contrôle ;

d) Détecter et contenir les foyers épidémiques au sein des populations vulnérables ;

e) Évaluer l'incidence de la pandémie sur les systèmes de santé et la société ;

f) Surveiller les tendances épidémiologiques à long terme et l'évolution du virus de la COVID-19 ;

g) Comprendre la co-circulation du virus de la COVID-19, de la grippe et d'autres virus respiratoires[25].

---

[24] OMS, « Déclaration de principe sur la communication de données par l'OMS lors des urgences de santé publique », 13 avril 2016.

[25] OMS, « Stratégies de surveillance de l'infection humaine à coronavirus 2019 (COVID-19) », point nº 29, 5 juin 2020.

59. Les objectifs décrits ci-dessus peuvent potentiellement être justifiés par des impératifs de santé publique ou d'intérêt général, et sont susceptibles de fournir un motif légal et justifiable de traiter des données relatives à la santé, mais uniquement si et dans la mesure où celles-ci sont traitées conformément à la législation sur la protection des données adoptée conformément à la Recommandation du Rapporteur spécial sur la protection et l'utilisation des données de santé.

60. La surveillance à des fins épidémiologiques, telle que susmentionnée, peut prendre de nombreuses formes, mais doit être nécessaire et proportionnée aux objectifs à atteindre. Les objectifs énumérés ci-dessus pourraient servir de guide aux États qui cherchent à définir leurs objectifs.

D. Technologie et données relatives à la santé – considérations relatives à la vie privée et à la santé publique

Base juridique applicable aux mesures ordinaires/extraordinaires et nécessité d'une intervention proportionnée et mesurée

61. Comme mentionné ci-dessus, les traités internationaux et la plupart des constitutions nationales contiennent des dispositions qui permettent aux États d'accroître temporairement leurs pouvoirs en période de crise. Les gouvernements peuvent faire usage de pouvoirs spéciaux, qui seraient normalement considérés comme des atteintes aux droits et libertés fondamentaux de l'homme ou des violations de ceux-ci, pendant une période limitée et dans un but précis – généralement pour combattre ou prévenir une menace imminente (dans le cas présent, pour empêcher la propagation de la COVID-19).

62. Les États disposent de différents moyens de faire usage de ces pouvoirs renforcés, en fonction des dispositions de leur Constitution et/ou des traités internationaux qu'ils ont ratifiés. Certains États parlent « d'état d'urgence », d'autres, « d'état de nécessité », tandis que, surtout pendant la crise actuelle de la COVID-19, d'autres encore font état d'une « urgence de santé publique ». Chaque régime juridique spécial temporaire confère des pouvoirs différents aux autorités. Par exemple, les recherches menées à ce jour indiquent qu'au moins 15 États du Nord ont réagi à la crise actuelle en déclarant l'état d'urgence[26].

63. Dans une déclaration[27] publiée au début de la crise, un groupe d'experts des procédures spéciales a affirmé que les États devaient trouver le bon équilibre entre les mesures extraordinaires mises en place pour lutter contre la propagation de la COVID-19 et la protection des droits de l'homme. Les mesures extraordinaires sont – ou devraient être – strictement définies par les lois et les constitutions nationales en tant qu'ordres juridiques revêtant une forme spécifique, émis par des autorités dotées

---

[26] Le délai imparti pour la présentation du présent rapport n'a permis qu'une analyse sommaire de quelques pays pour lesquels des données fiables étaient plus facilement disponibles. Au cours de la période allant de juin 2020 à juin 2021, le Rapporteur spécial s'emploiera à rassembler et à trianguler des données, de manière à obtenir un tableau plus précis et plus fiable des mesures juridiques et opérationnelles liées à la COVID-19 disponibles et déployées dans les pays du Sud. En Asie, en Afrique et en Amérique du Sud, par exemple, la crise de la COVID-19 est encore très récente et fait l'objet d'un suivi constant de la part du titulaire du mandat, qui entend en rendre compte dans son prochain rapport annuel.

[27] HCDH, « COVID-19 : les États ne doivent pas abuser des mesures d'urgence pour réprimer les droits de l'homme – Experts de l'ONU », communiqué de presse, 16 mars 2020. Disponible à l'adresse suivante : www.ohchr.org/fr/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=f.

de pouvoirs spéciaux en cas d'état d'urgence. Elles sont également reconnues dans les instruments juridiques internationaux, notamment le Pacte international relatif aux droits civils et politiques (article 4) et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (article 15)[28].

64. La nécessité de coordonner de manière adéquate les mesures prises pour prévenir la contagion à grande échelle de la COVID-19, dans le respect des droits fondamentaux de l'homme, y compris le droit à la protection des données, est très bien abordée dans la déclaration conjointe publiée le 30 mars 2020 par la Présidente du Comité de la Convention 108 et le Commissaire à la protection des données du Conseil de l'Europe[29]. La surveillance, les mesures de suivi et les restrictions similaires aux libertés fondamentales ont été appliquées pour des motifs de sécurité publique. Par conséquent, on dispose d'un corpus d'expérience non négligeable concernant les mesures prises pour concilier sécurité nationale et droits fondamentaux, tout en veillant à ce que les mesures portant atteinte à la vie privée soient prévues par la loi et soient nécessaires et proportionnées dans une société démocratique. Toutefois, transposer cette expérience dans le domaine de la santé publique pourrait se révéler plus compliqué, et certains ajustements pourraient être nécessaires en vue de définir une approche appropriée et sensible à la protection de la vie privée et des données.

65. Près de 30 % des États Membres de l'Organisation des Nations Unies se sont déjà formellement engagés, en vertu du droit international, à respecter les principes de nécessité et de proportionnalité : les 55 États qui ont ratifié la Convention 108 ou la Convention 108+ du Conseil de l'Europe sont déjà liés par l'article 9 de la Convention 108 ou l'article 11 de la Convention 108+. Ils doivent être bien conscients que les mesures prises pour des motifs de la santé publique doivent répondre aux mêmes critères de légalité, de nécessité et de proportionnalité dans une société démocratique que ceux prévus dans les articles susmentionnés. Aux fins du présent rapport, la crise de la COVID-19 s'entend comme étant couverte par l'alinéa a) du paragraphe 1 de l'article 11 de la Convention 108+, sous la rubrique « autres objectifs essentiels d'intérêt public général ». Les 70 % d'États Membres restants qui ne sont pas parties à la Convention pourraient donc commencer par se prévaloir de la recommandation antérieure du Rapporteur spécial et adhérer à la Convention 108+ dans les meilleurs délais, puis mettre en place tous les mécanismes identifiés dans le présent document et ailleurs, et appliquer les principes qui y figurent dans leurs dispositifs de gouvernance au quotidien, y compris ceux relatifs à la protection des données relatives à la santé.

66. Ainsi, lorsqu'un État s'est doté d'une loi qui prévoit des pouvoirs extraordinaires, et lorsque les mesures déployées dans l'exercice de ces pouvoirs semblent porter atteinte à la vie privée, y compris toute forme de surveillance (par exemple, géolocalisation, surveillance de proximité, logiciels malveillants, écoutes téléphoniques, profilage), ces mesures doivent faire l'objet d'une surveillance *ex ante*

---

[28] Voir également, Cour européenne des droits de l'homme, Lawless c. Irlande (n° 3), arrêt du 1er juillet 1961, par. 3 ; et Danemark, Norvège, Suède et Pays-Bas c. Grèce (requêtes n° 3321, 3322, 3323, 3324/67, Rapport de la Commission européenne des droits de l'homme du 5 novembre 1969.

[29] Conseil de l'Europe, « Déclaration conjointe sur le droit à la protection de données dans le contexte de la pandémie à COVID-19 par Alessandra Pierucci, Présidente du Comité de la Convention 108 et Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe », Strasbourg, 30 mars 2020. Disponible à l'adresse suivante : https://rm.coe.int/covid19-declaration-conjointe/16809e0a17.

et *ex post* afin de démontrer qu'elles sont nécessaires et proportionnées à l'objectif recherché. Ainsi, on pourrait garantir que seule la méthode de surveillance appropriée est appliquée, par les personnes appropriées, dans le but approprié et pour une durée appropriée.

E. Technologie et autres réalités

67. De tous les moyens technologiques auxquels les gouvernements ont eu recours pour faire face à la pandémie de COVID-19, les applications pour smartphones comptent parmi les méthodes les plus discutées et les plus déployées par les États pour surveiller la propagation du virus. Jusqu'à présent, de nombreux pays semblent avoir pris la décision de développer leurs propres applications de recherche de contacts. L'interopérabilité transfrontalière demeure donc toujours au stade embryonnaire et n'est qu'une recommandation pour l'avenir[30].

68. Lorsqu'il s'agit de développer des applications de recherche de contacts, il convient de tenir compte de certains aspects, à savoir :

a) Comment l'application recueille des informations sur la géolocalisation/proximité des personnes (par exemple, certaines applications identifient les contacts d'une personne en suivant les mouvements du smartphone, en utilisant le système GPS ou la triangulation à partir d'antennes-relais situées à proximité), et recherche d'autres smartphones qui se sont trouvés au même endroit au même moment ;

b) L'utilisation du suivi de proximité, selon lequel les smartphones échangent des codes cryptés avec d'autres smartphones proches par le truchement de la technologie Bluetooth, qui gère les informations recueillies et leur stockage (c'est-à-dire des approches centralisées ou décentralisées) ;

c) Si l'installation et l'utilisation de l'application sont volontaires ou obligatoires (c'est-à-dire déploiement consensuel ou non).

69. De nombreuses applications reposent sur les interfaces de programmation d'applications communes développées par Apple et Google. L'interface permet aux smartphones iOS et Android de communiquer entre eux via Bluetooth, ce qui a permis aux développeurs de créer une application de recherche de contacts qui fonctionne pour les deux systèmes. Les deux sociétés prévoient d'intégrer cette fonctionnalité directement dans leurs systèmes d'exploitation.

70. De manière générale, l'un des problèmes les plus graves réside dans le fait que la sous-discipline de l'ingénierie de la protection de la vie privée ne reçoit pas l'importance qu'elle mérite. Les grandes entreprises technologiques (telles qu'Apple) ont été parmi les premières à faire de l'ingénierie de la protection de la vie privée une discipline à part entière. Il importe de souligner que le seul fait de s'appuyer sur des garanties juridiques n'est pas suffisant. La protection de la vie privée doit être prise en compte dès le début, en commençant par la conception de l'application. Bien que

[30] Il convient de souligner que même si tous les efforts ont été déployés pour garantir l'exactitude des informations fournies, la crise de la COVID-19 a sérieusement limité la capacité du Rapporteur spécial à trianguler les données, en particulier les données recueillies dans les médias. Les informations contenues dans le présent rapport concernant les pratiques ou les interventions actuellement mises en place dans les différents États sont donc proposées à titre indicatif, et ne sont pas nécessairement définitives. Si la crise de la COVID-19 le permet, ces informations devraient être vérifiées de manière adéquate et faire l'objet d'un rapport en 2021.

cela soit pris en compte dans l'esprit de l'approche « confidentialité programmée » préconisée dans le règlement général de l'Union européenne sur la protection des données, la réalité de l'ingénierie de la protection de la vie privée est loin de ces nobles idéaux. En pratique, la grande majorité des pays du monde sont dotés d'équipes d'ingénieurs en technologies de l'information et des communications pour lesquelles la performance ou la fonctionnalité – et non la confidentialité – est au cœur du processus d'ingénierie. Le manque de formation et de recherche en matière d'ingénierie de la protection de la vie privée dans les universités signifie qu'il faudra plusieurs années, voire des décennies, pour que la situation évolue de manière à ce que la protection de la vie privée dès la conception devienne une réalité.

71. L'action concertée menée par de petits groupes de personnes motivées suscite toutefois un certain espoir. Face à la crise de la COVID-19, une méthode prometteuse a été mise au point, à savoir le « traçage de proximité décentralisé préservant la vie privée », un protocole ouvert développé par un groupe d'écoles d'ingénieurs aux fins du traçage basé sur la technologie Bluetooth, en vertu duquel les contacts détectés par le smartphone d'une personne ne sont stockés que localement, de sorte qu'aucune autorité centrale ne peut savoir qui a été exposé[31]. Un certain nombre d'États (tels que l'Autriche, l'Estonie, l'Allemagne et la Suisse) ont annoncé que les applications qu'ils ont déployées au niveau national sont basées sur ce protocole. En comparaison, le « traçage de proximité paneuropéen préservant la confidentialité » – un autre protocole développé par un consortium d'universitaires et d'entrepreneurs pour faire face à la pandémie de COVID-19 – est dépourvu de certaines caractéristiques liées à la transparence et à la protection de la vie privée (par exemple, les données des utilisateurs sont stockées sur un serveur, tandis que le traçage de proximité décentralisé préservant la vie privée repose sur la décentralisation, de sorte que les données ne quittent jamais le smartphone de l'utilisateur).

72. En fonction de la conception de l'application, les responsables de la santé sont parfois dans l'impossibilité d'avoir accès aux données sur les personnes qui se sont trouvées à proximité d'une personne contaminée. Certaines applications [par exemple COVIDSafe (Australie) et StopCovid (France)] reposent sur un modèle centralisé, ce qui signifie que la personne contaminée doit transmettre l'identification de son smartphone et celle des smartphones de ses contacts récents à un serveur central. Bien que les identifications soient anonymes, les fonctionnaires peuvent accéder à l'ensemble du réseau de contacts.

73. D'autres applications (par exemple, en Allemagne) sont décentralisées, ce qui signifie que les données sur les contacts récents d'une personne restent sur son smartphone. Une personne contaminée ne télécharge que sa propre identification anonymisée dans une base de données centrale ; toute personne qui a téléchargé l'application sur son smartphone peut régulièrement télécharger la liste des utilisateurs contaminés et vérifier les smartphones qui se sont trouvés à proximité de ces derniers. Les défenseurs de la protection de la vie privée voient de réels avantages dans cette conception et affirment que celle-ci ne permet pas de rendre les données relatives aux réseaux sociaux des utilisateurs vulnérables au piratage ou à l'exploitation.

74. Il convient également de prendre en considération le rôle essentiel que jouent les données des smartphones dans la recherche médicale, dans la mesure où il s'agit

[31] École Polytechnique Fédérale de Lausanne, ETH Zurich, KU Leuven, Delft University of Technology, University College London, Helmholtz Centre for Information Security, University of Torino et ISI Foundation.

d'un motif largement invoqué par les États qui choisissent la conception centralisée. Dans le cas des applications décentralisées, les services nationaux de santé publique et les chercheurs ne prennent connaissance que des personnes qui les contactent effectivement pour signaler qu'elles ont reçu une notification. Étant donné que les acteurs de la santé publique n'ont pas accès aux numéros de téléphone des personnes qui ont été notifiées et qui ne l'ont pas signalé, il pourrait être plus difficile d'évaluer l'exactitude et la précision des données saisies par l'application.

75. Il existe une différence essentielle dans la manière de promouvoir et de faire fonctionner les applications. La plupart des États encouragent les populations à télécharger l'application volontairement, avec le libre consentement de l'utilisateur ; L'Inde est la seule démocratie qui a rendu le téléchargement de l'application obligatoire pour des millions de personnes. Dans certains cas rares mais importants, le déploiement de l'application a été jugé obligatoire pour certaines catégories de personnes, par exemple en République de Corée, ou même pour toute personne jouissant d'une vie normale, comme dans le cas de la Chine.

76. Même lorsque l'installation de l'application est « volontaire », la saisie obligatoire des données varie et il importe donc d'évaluer le niveau de protection des données en s'assurant que seules les informations nécessaires sont collectées par l'application, que le stockage des données respecte les normes internationales de protection des données et que ce stockage est limité dans le temps et utilisé uniquement pour des motifs appropriés.

Systèmes de surveillance hybrides

77. La méthode de surveillance employée en République de Corée repose sur l'utilisation d'une application pour smartphone, mais pas uniquement ; en effet, le pays a plutôt adopté une approche hybride rassemblant des technologies traditionnellement utilisées dans les domaines de la répression et de la lutte contre le terrorisme, et combinant plusieurs sources de données personnelles pour dresser un tableau des déplacements d'une personne, notamment :

– Les transactions par carte de crédit et de débit – qui peuvent indiquer les lieux dans lesquels une personne a fait ses achats ou pris ses repas, et comment elle s'est déplacée sur un réseau de transport ;

– Les relevés de localisation téléphonique obtenus auprès des opérateurs de téléphonie mobile – qui donnent une idée approximative du quartier dans lequel se trouve une personne lorsqu'elle se connecte à différentes antennes-relais ;

– Les informations capturées par le vaste réseau de caméras de surveillance[32].

78. Le système adopté en Israël n'est pas seulement inspiré des technologies antiterroristes ; il les utilise directement. Selon certaines sources, depuis la mi-mars, l'Organisme de sécurité israélien aide le Gouvernement d'Israël à mener des enquêtes épidémiologiques en fournissant au Ministère de la Santé les itinéraires des personnes contaminées par le coronavirus et les listes des personnes avec lesquelles elles ont été en contact étroit[33]. Ces informations sont disponibles dans la base de données

[32] Rory Cellan-Jones, « Tech Tent: Can we learn about coronavirus-tracing from South Korea? » BBC News, 15 mai 2020. Disponible à l'adresse suivante : www.bbc.com/news/technology-52681464.

[33] Amir Cahane, « Israel reauthorizes Shin Bet's coronavirus location tracking », Lawfare, 3 juillet 2020. Disponible à l'adresse suivante : www.lawfareblog.com/israel-reauthorizes-shin-bets-coronavirus-location-tracking.

consacrée aux métadonnées de communication de l'Organisme. La méthode de surveillance utilisée en Israël est particulièrement intéressante étant donné que la Cour suprême a invalidé son utilisation en avril 2020, obligeant le Gouvernement à adopter une nouvelle loi pour fournir la base juridique appropriée de cette surveillance. Bien que, depuis mars, le Gouvernement d'Israël ait essayé de renforcer le niveau de contrôle parlementaire de ses opérations de renseignement, à la différence des Pays-Bas, du Royaume-Uni ou d'autres pays, il ne possède pas « d'organe expert » statutaire indépendant capable d'agir en qualité d'autorité de surveillance totalement indépendante chargée de compléter le travail de la Commission parlementaire.

III. Conclusions

79. **La surveillance et la recherche des contacts liées à la COVID-19 peuvent prendre différentes formes, et peuvent être manuelles ou technologiques, anonymes ou non, consensuelles ou non.**

80. **Afin d'évaluer correctement les mesures de lutte contre la COVID-19, il importe de s'assurer qu'elles sont modérément utiles ou indispensables, ou de déterminer qu'elles ne sont pas du tout utiles. Cette évaluation contribuerait à déterminer si la mesure est nécessaire et proportionnée dans une société démocratique, et donc admissible au titre du droit international relatif à la protection de la vie privée.**

81. **Il est beaucoup trop tôt pour déterminer avec certitude si certaines mesures de lutte contre la COVID-19 pourraient se révéler inutiles ou disproportionnées. Le Rapporteur spécial continuera de surveiller l'incidence de la surveillance épidémiologique sur le droit à la vie privée et fera rapport à l'Assemblée générale en 2021**[34]**. Le principal risque pour la vie privée réside dans l'utilisation de méthodes non consensuelles, telles que celles décrites dans la section sur les systèmes de surveillance hybrides, qui pourraient entraîner des dérives et être utilisées à d'autres fins susceptibles de porter atteinte à la vie privée.**

82. **La surveillance technologique intensive et omniprésente est loin d'être la panacée en cas de pandémies telles que la COVID-19. Cette constatation s'est particulièrement vérifiée dans les pays où l'utilisation des méthodes conventionnelles de recherche des contacts, sans recours aux applications des smartphones, à la géolocalisation ou à d'autres technologies, s'est avérée la plus efficace pour contrer la propagation de la COVID-19.**

83. **Lorsqu'un État décide qu'une surveillance technologique est nécessaire pour faire face à la pandémie mondiale de COVID-19, il doit s'assurer, après avoir démontré qu'une telle mesure est à la fois nécessaire et proportionnée, qu'il a adopté une loi qui prévoit explicitement de telles mesures de surveillance (comme dans le cas d'Israël).**

---

[34] Le Rapporteur spécial a entrepris de compiler des tableaux contenant des données de base sur l'utilisation de la technologie en lien avec la COVID-19, qui seront mis à jour pour proposer les informations les plus précises possibles. Les tableaux seront publiés en annexe au présent rapport de 2020 à l'Assemblée générale sur le site web du titulaire du mandat (www.ohchr.org/EN/Issues/Privacy/SR/Pages/ AnnualReports.aspx) et mis à jour selon que de besoin.

84. **Un État souhaitant instaurer une mesure de surveillance aux fins de la lutte contre la COVID-19 ne devrait pas avoir la possibilité de s'appuyer sur une disposition législative générale, telle que celle disposant que le responsable de l'autorité de santé publique peut « ordonner toute autre mesure qu'il [ou elle] juge appropriée ». En effet, une telle disposition ne prévoit pas les garanties explicites et spécifiques ayant été rendues obligatoires à la fois au titre des dispositions de la Convention 108 et de la Convention 108+, et fondées sur la jurisprudence de la Cour européenne des droits de l'homme. En effet, si la garantie n'est pas suffisamment détaillée, elle ne peut pas être considérée comme une garantie adéquate.**

85. **L'OMS tient une liste des cas de COVID-19 (et du nombre de décès y relatifs) par région de l'OMS[35]. Cette liste sert à rappeler constamment qu'il faut donner la priorité à l'adoption de mesures devant permettre de réduire considérablement le nombre de décès. En bref, si un État souhaite adopter une mesure portant atteinte à la vie privée, en particulier une mesure pouvant facilement donner lieu à des dérives, telle que la surveillance technologique, il doit démontrer que la mesure est nécessaire et proportionnée pour atteindre l'objectif recherché. L'État concerné doit mettre la mesure à l'épreuve en posant les questions suivantes : existe-t-il une autre méthode qui aurait pu être utilisée et qui aurait permis d'éviter les décès dans la même mesure ou mieux que la technologie portant atteinte à la vie privée déployée ou envisagée ? La technologie déployée était-elle/est-elle « une solution de facilité » ? Quel est le coût – financier et en termes de protection de la vie privée – du déploiement de la technologie en question ? C'est seulement à ce moment-là que la nécessité et le coût des mesures respectueuses de la vie privée pourront être correctement évalués, et que leur proportionnalité pourra être appréciée.**

86. **On peut comprendre que certains des États ayant adopté des technologies portant atteinte à la vie privée pour lutter contre la COVID-19 affirment avoir enregistré un certain nombre de cas ou avoir évité un certain nombre de décès. Toutefois, ces affirmations n'ont pas encore été vérifiées. Il est encore trop tôt pour évaluer correctement l'efficacité des mesures prises dans le cadre de la lutte contre la COVID-19 et apporter des réponses aux questions suivantes :**

a) **Qu'est-ce qui fonctionne ?**

b) **Qu'est-ce qui fonctionne le mieux ?**

c) **Qu'est-ce qui fonctionne le mieux et pour qui ?**

d) **Qu'est-ce qui fonctionne le mieux et où ?**

87. **Une fois la mesure identifiée, la question suivante est de savoir pourquoi cette mesure a fonctionné au mieux, pour qui a-t-elle fonctionné et où ? On espère que les données qui seront collectées au cours des 12 prochains mois permettront de mieux comprendre ces variables et d'autres éléments, de manière à aider les experts en protection de la vie privée à évaluer correctement les mesures de lutte**

[35] OMS, maladie à coronavirus (COVID-19), Rapport de situation. Disponible à l'adresse suivante : www.who.int/docs/default-source/coronaviruse/situation-reports/20200712-covid-19-sitrep-174.pdf?sfvrsn=5d1c1b2c_2. Il convient de souligner qu'à ce stade, la question de savoir si l'objectif de réduction des décès doit être le seul ou le principal critère d'évaluation d'une mesure de lutte contre la COVID-19 est loin d'être tranchée. Il convient de poursuivre les consultations à cet égard.

contre la COVID-19 ayant été déployées et à déterminer si les mesures non consensuelles répondent aux critères stricts de proportionnalité et de nécessité.