

# RECOMMANDATIONS

## RECOMMANDATION (UE) 2020/518 DE LA COMMISSION

du 8 avril 2020

**concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées**

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

- (1) La crise de santé publique causée par l'actuelle pandémie de COVID-19 (ci-après dénommée la «crise de la COVID-19») oblige l'Union et les États membres à faire face à un défi sans précédent pour ses systèmes de soins de santé, son mode de vie, sa stabilité économique et ses valeurs. Aucun État membre ne peut réussir seul à lutter contre la crise de la COVID-19. Une crise exceptionnelle d'une telle ampleur requiert une action résolue de l'ensemble des États membres et des institutions et organes de l'UE, collaborant dans un véritable esprit de solidarité.
- (2) Les technologies et données numériques ont un rôle précieux à jouer dans la lutte contre la crise de la COVID-19, puisque de nombreuses personnes en Europe sont connectées à l'internet au moyen d'appareils mobiles. Ces technologies et données peuvent offrir un outil important pour informer le public et aider les autorités publiques concernées dans leurs efforts en vue d'endiguer la propagation du virus ou pour permettre aux organismes de soins de santé d'échanger des données de santé. Toutefois, une approche fragmentée et non coordonnée risque d'entraver l'efficacité des mesures visant à lutter contre la crise de la COVID-19, tout en causant un préjudice grave pour le marché unique et pour les droits et libertés fondamentaux.
- (3) Il est donc nécessaire d'élaborer une approche commune concernant l'utilisation des technologies et données numériques en réaction à la crise actuelle. Cette approche devrait être efficace pour soutenir les autorités nationales compétentes, en particulier les autorités sanitaires et les décideurs politiques, en leur fournissant des données précises suffisantes pour comprendre l'évolution et la propagation du virus COVID-19 ainsi que ses effets. De même, ces technologies peuvent donner aux citoyens les moyens de prendre des mesures efficaces et mieux ciblées en matière de distanciation sociale. Dans le même temps, l'approche proposée vise à préserver l'intégrité du marché unique et à protéger les droits et libertés fondamentaux, notamment les droits au respect de la vie privée et à la protection des données à caractère personnel.
- (4) Les applications mobiles peuvent aider les autorités sanitaires, tant au niveau national qu'au niveau de l'UE, à surveiller et à maîtriser la pandémie de COVID-19 en cours. Elles peuvent fournir des orientations aux citoyens et faciliter l'organisation du suivi médical des patients. Les applications d'alerte et de traçage peuvent jouer un rôle important pour retracer les contacts, limiter la propagation de la maladie et interrompre les chaînes de transmission. Par conséquent, en combinaison avec des stratégies adéquates de dépistage et un traçage approprié des contacts, les applications peuvent être particulièrement utiles pour fournir des informations sur le niveau de circulation du virus, pour évaluer l'efficacité des mesures de distanciation physique et de confinement et pour éclairer les stratégies de relâchement des mesures de confinement.

- (5) La décision n° 1082/2013/UE du Parlement européen et du Conseil <sup>(1)</sup> établit des règles spécifiques en matière de surveillance épidémiologique, de surveillance des menaces transfrontières graves sur la santé, d'alerte précoce en cas de telles menaces et de lutte contre celles-ci. Conformément à l'article 2, paragraphe 5, de cette décision, la Commission doit veiller, en liaison avec les États membres, à ce que la coordination et l'échange d'informations soient assurés entre les mécanismes et les structures établis au titre de ladite décision et des mécanismes et structures similaires établis au niveau de l'Union ou au titre du traité Euratom dont les activités sont utiles à la planification de la préparation et de la réaction, à la surveillance des menaces transfrontières graves sur la santé, à l'alerte précoce en cas de telles menaces et à la lutte contre celles-ci. Le forum chargé de la coordination des efforts dans le contexte de menaces transfrontières graves sur la santé est le comité de sécurité sanitaire institué par l'article 17 de la décision précitée. Dans le même temps, l'article 6, paragraphe 1, de la décision institue un réseau de surveillance épidémiologique des maladies transmissibles, exploité et coordonné par le Centre européen de contrôle des maladies.
- (6) La directive 2011/24/UE du Parlement européen et du Conseil <sup>(2)</sup> relative à l'application des droits des patients en matière de soins de santé transfrontaliers dispose que le réseau «Santé en ligne» doit œuvrer à la mise en place de systèmes et de services européens de santé en ligne offrant des avantages économiques et sociaux durables ainsi que des applications interopérables, de manière à atteindre un niveau élevé de confiance et de sécurité, à renforcer la continuité des soins et à garantir l'accès à des soins de santé de qualité élevée et sûrs.
- (7) Le règlement (UE) 2016/679 du Parlement européen et du Conseil <sup>(3)</sup> 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 définit les conditions pour le traitement des données à caractère personnel, y compris les données relatives à la santé. Ces données peuvent être traitées notamment lorsqu'une personne concernée donne son consentement explicite ou lorsque le traitement est dans l'intérêt public, conformément au droit de l'État membre ou au droit de l'Union, en particulier à des fins de surveillance et d'alerte, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé.
- (8) Plusieurs États membres ont introduit des dispositions législatives spécifiques leur permettant de traiter les données relatives à la santé, sur la base de l'intérêt public [article 6, paragraphe 1, points c) ou e), et article 9, paragraphe 2, point i), du règlement (UE) 2016/679]. En tout état de cause, il convient de spécifier clairement les finalités et les moyens du traitement des données, ainsi que les données à traiter et les personnes chargées du traitement.
- (9) La Commission peut consulter le Contrôleur européen de la protection des données et le comité européen de la protection des données, conformément à l'article 42 du règlement (UE) 2018/1725 du Parlement européen et du Conseil <sup>(4)</sup> et à l'article 70 du règlement (UE) 2016/679.
- (10) La directive 2002/58/CE du Parlement européen et du Conseil <sup>(5)</sup> fixe les règles applicables aux données relatives au trafic et aux données de localisation, ainsi qu'au stockage des informations et à l'accès aux informations stockées dans l'équipement terminal, tel qu'un appareil mobile, d'un utilisateur ou d'un abonné. Conformément à l'article 5, paragraphe 3, de la directive, ce stockage ou cet accès ne sont permis que dans des circonstances strictement définies ou à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect du règlement 2016/679, une information claire et complète. En outre, l'article 15, paragraphe 1, de la directive autorise les États membres à adopter des mesures législatives visant à limiter la portée de certains droits et obligations établis par la directive, y compris ceux visés à l'article 5, lorsqu'une telle restriction constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique pour atteindre certains objectifs.

<sup>(1)</sup> Décision n° 1082/2013/UE du Parlement européen et du Conseil du 22 octobre 2013 relative aux menaces transfrontières graves sur la santé et abrogeant la décision n° 2119/98/CE (JO L 293 du 5.11.2013, p. 1).

<sup>(2)</sup> Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

<sup>(3)</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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) (JO L 119 du 4.5.2016, p. 1).

<sup>(4)</sup> Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

<sup>(5)</sup> Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

- (11) Dans sa communication intitulée «Une stratégie européenne pour les données»<sup>(6)</sup>, la Commission européenne a annoncé que l'UE créerait un marché unique dans lequel les données pourront circuler à l'intérieur de l'UE et entre les secteurs, au bénéfice de tous les citoyens, où les règles européennes, en particulier en matière de protection de la vie privée et des données à caractère personnel, ainsi que le droit de la concurrence, seront pleinement respectées et où les règles relatives à l'accès et à l'utilisation des données seront équitables, pratiques et claires. En particulier, la Commission a indiqué qu'elle examinerait la nécessité d'une action législative visant à promouvoir le partage des données des entreprises vers les pouvoirs publics dans l'intérêt public.
- (12) Depuis le début de la crise liée au COVID-19, diverses applications mobiles ont été mises au point, par des autorités publiques dans certains cas, et tant les États membres que le secteur privé ont appelé à une coordination au niveau de l'Union, notamment pour répondre aux préoccupations en matière de cybersécurité, de sécurité et de protection de la vie privée. Ces applications remplissent trois fonctions générales: i) informer et conseiller les citoyens et faciliter l'organisation du suivi médical des personnes présentant des symptômes, souvent en combinaison avec un questionnaire d'autodiagnostic; ii) avertir les personnes qui se sont trouvées à proximité d'une personne infectée afin d'interrompre la chaîne de transmission de l'infection et d'empêcher une augmentation des cas d'infection à la sortie du confinement; et iii) contrôler et faire respecter la quarantaine des personnes infectées, éventuellement en combinaison avec des fonctionnalités évaluant leur état de santé au cours de la période de quarantaine. Certaines applications sont à la disposition du grand public, tandis que d'autres ne sont accessibles qu'à des groupes fermés d'utilisateurs, en vue d'assurer un traçage des contacts sur le lieu de travail. L'efficacité de ces applications n'a généralement pas été évaluée. Les applications d'information et d'analyse des symptômes pourraient se révéler utiles pour sensibiliser les citoyens. Toutefois, de l'avis des experts, les applications visant à informer et à alerter les utilisateurs semblent les plus prometteuses pour empêcher la propagation du virus, compte tenu également de leur incidence plus limitée sur la protection de la vie privée, et plusieurs États membres étudient actuellement la possibilité d'y avoir recours.
- (13) Certaines de ces applications mobiles pourraient être considérées comme des dispositifs médicaux lorsqu'elles sont destinées par le fabricant à être utilisées, notamment, à des fins de diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation d'une maladie, et relèveraient donc du champ d'application du règlement (UE) 2017/745 du Parlement européen et du Conseil<sup>(7)</sup> ou de la directive 93/42/CEE du Conseil<sup>(8)</sup>. En ce qui concerne les applications d'autodiagnostic et d'analyse des symptômes, il convient, lorsqu'elles fournissent des informations liées à la prévention, au contrôle, à la prédiction ou au pronostic, d'évaluer leur qualification comme dispositifs médicaux conformément au cadre réglementaire relatif aux dispositifs médicaux [directive 93/42/CEE ou règlement (UE) 2017/745].
- (14) L'efficacité de ces applications mobiles dépend d'un certain nombre de facteurs. Parmi ceux-ci, citons le taux de pénétration auprès des utilisateurs, c'est-à-dire, sur le pourcentage de la population utilisant un appareil mobile, le pourcentage de personnes qui a téléchargé l'application et qui a donné son consentement au traitement de données à caractère personnel les concernant et ne l'a pas retiré. Au rang des autres facteurs importants figurent la confiance du public dans le fait que les données seront protégées par des mesures de sécurité appropriées, utilisées exclusivement pour prévenir les personnes susceptibles d'avoir été exposées au virus; l'aval des autorités de santé publique; la capacité des autorités sanitaires à prendre des mesures en fonction des données générées par l'application; l'intégration et le partage de données avec d'autres systèmes et applications, ou encore l'interopérabilité transfrontalière et interrégionale avec d'autres systèmes.
- (15) Les applications d'alerte et de traçage sont utiles pour les États membres à des fins de traçage des contacts et elles peuvent jouer un rôle important dans l'endigement dans les scénarios de relâchement des mesures de confinement. Elles peuvent également constituer un outil précieux pour permettre aux citoyens d'exercer une distanciation sociale effective et mieux ciblée. Leur efficacité peut être renforcée par une stratégie en faveur d'une généralisation des tests. Le traçage des contacts signifie que les autorités de santé publique identifient rapidement tous les contacts d'un cas confirmé de COVID-19, leur demandent de se confiner et les testent et les placent à l'isolement rapidement s'ils présentent des symptômes. En outre, les données anonymisées et agrégées issues de ces applications, combinées à des informations sur l'incidence de la maladie, pourraient être utilisées pour évaluer l'efficacité des mesures de distanciation sociale. Si ces applications présentent une utilité évidente pour les États membres, elles peuvent également apporter une valeur ajoutée aux travaux de l'ECDC.

<sup>(6)</sup> Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions intitulée «Une stratégie européenne pour les données», COM (2020) 66 final.

<sup>(7)</sup> Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1).

<sup>(8)</sup> Directive 93/42/CEE du Conseil du 14 juin 1993 relative aux dispositifs médicaux (JO L 169 du 12.7.1993, p. 1).

- (16) Les applications d'autodiagnostic et d'analyse des symptômes pourraient fournir des informations pertinentes sur le nombre de personnes présentant des symptômes compatibles avec la COVID-19, par âge et par semaine, pour des zones bien définies dans lesquelles la couverture de l'application est élevée. Si les résultats sont concluants, les autorités nationales de santé publique peuvent décider d'utiliser les données de l'application pour la surveillance syndromique de la COVID-19 dans le cadre des soins de santé primaires. Ces données pourraient être communiquées à l'ECDC chaque semaine, sous une forme agrégée [par exemple, le nombre de syndromes de type grippal (ILI) ou d'infections respiratoires aiguës (IRA) enregistrés par semaine, par groupe d'âge, sur la population totale couverte par les médecins sentinelles]. Les autorités nationales et l'ECDC seraient alors en mesure d'estimer la valeur prédictive positive des symptômes respiratoires dans une communauté donnée, ce qui fournirait, à partir des données issues de l'application, des informations sur le niveau de circulation du virus.
- (17) L'utilisation des fonctionnalités des applications pour smartphones décrites ci-dessus est susceptible de porter atteinte à l'exercice de certains droits fondamentaux tels que le droit au respect de la vie privée et familiale. Toute ingérence dans ces droits devant être conforme aux exigences prévues par la loi, les législations des États membres qui établiraient ou autoriseraient des restrictions à l'exercice de certains droits fondamentaux devraient respecter les principes généraux du droit de l'Union énoncés à l'article 6 du traité sur l'Union européenne, les traditions constitutionnelles de ces États membres et leurs obligations en vertu du droit international.
- (18) Afin de favoriser l'acceptation de différents types d'applications (et des systèmes d'information sur les chaînes de transmission de l'infection qui les sous-tendent) et de faire en sorte qu'elles servent l'objectif déclaré en matière de surveillance épidémiologique, les politiques, exigences et contrôles sous-jacents doivent être alignés et mis en œuvre de manière coordonnée par les autorités sanitaires nationales compétentes. L'expérience de plusieurs États membres qui ont commencé à introduire des applications de traçage des contacts montre que, pour améliorer l'acceptation, il est judicieux de recourir à une gouvernance intégrée pour préparer et mettre en œuvre les mesures, en faisant intervenir non seulement les autorités sanitaires, mais aussi d'autres autorités (telles que celles chargées de la protection des données), ainsi que le secteur privé, des experts, des universitaires et des parties intéressées telles que des groupes de patients. Une vaste opération de communication sur l'application est également essentielle pour assurer l'adoption et le succès de celle-ci.
- (19) Afin de détecter les contacts rapprochés entre utilisateurs de différentes applications de traçage des contacts (un scénario très probable entre les personnes circulant par-delà les frontières nationales/régionales), il convient d'envisager l'interopérabilité entre les applications. Les autorités sanitaires nationales chargées de la surveillance des chaînes de transmission de l'infection devraient être en mesure d'échanger avec d'autres États membres ou régions des informations interopérables sur les utilisateurs qui ont été testés positifs afin de rompre les chaînes de transmission transfrontalières.
- (20) Certaines entreprises, notamment les fournisseurs de télécommunications et les principales plates-formes technologiques, ont publié ou mis à disposition des autorités publiques des données de localisation agrégées et anonymisées. Ces données sont nécessaires à la recherche pour lutter contre le virus et aux travaux de modélisation qui permettront de comprendre comment le virus va se propager et de prévoir les effets économiques de la crise. En particulier, les données permettront de comprendre et de modéliser la dynamique spatiale de l'épidémie et d'évaluer l'impact des mesures de distanciation sociale (restrictions de déplacement, fermetures d'activités non essentielles, confinement total, etc.) sur la mobilité. Cela est essentiel, d'une part, pour endiguer les effets du virus et pour évaluer les besoins, notamment en termes d'équipements de protection individuelle et d'unités de soins intensifs, et, d'autre part, pour soutenir la stratégie de sortie avec des modèles axés sur les données indiquant les effets potentiels de l'assouplissement des mesures de distanciation sociale.
- (21) La crise actuelle a montré le bénéfice que pourraient tirer les autorités de santé publique et les instituts de recherche d'un plus grand accès à des informations essentielles pour analyser l'évolution du virus et évaluer l'efficacité des mesures de santé publique.
- (22) Certains États membres ont pris des mesures pour simplifier l'accès aux données nécessaires. Toutefois, les efforts communs de l'UE pour combattre le virus pâtissent de l'hétérogénéité actuelle des approches.

- (23) Une approche commune de l'Union face à la crise de la COVID-19 est également devenue nécessaire parce que les mesures prises dans certains pays, telles que le traçage des personnes au moyen de la géolocalisation, le recours à la technologie pour évaluer le niveau de risque sanitaire attaché à un individu et la centralisation de données sensibles, posent question du point de vue de plusieurs droits et libertés fondamentaux garantis dans l'ordre juridique de l'Union, notamment le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. En tout état de cause, la charte des droits fondamentaux de l'Union européenne prévoit que les restrictions à l'exercice des libertés et droits fondamentaux qu'elle consacre doivent être justifiées et proportionnées. En particulier, de telles restrictions doivent être temporaires, c'est-à-dire rester strictement limitées à ce qui est nécessaire pour combattre la crise et ne pas perdurer, sans raison valable, une fois la crise passée.
- (24) En outre, l'Organisation mondiale de la santé et d'autres organismes ont mis en garde contre le risque que des applications et des données inexactes n'entraînent une stigmatisation des personnes qui présentent certaines caractéristiques perçues comme liées à la maladie.
- (25) Conformément au principe de minimisation des données, les autorités de santé publique et les instituts de recherche ne devraient traiter des données à caractère personnel que si cela est adéquat, pertinent et limité à ce qui est nécessaire, et elles devraient mettre en œuvre des garanties appropriées telles que la pseudonymisation, l'agrégation, le chiffrement et la décentralisation.
- (26) Des mesures efficaces en matière de cybersécurité et de sécurité des données sont essentielles pour préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données.
- (27) Pour veiller à ce que les données à caractère personnel soient traitées de manière licite et que les droits des personnes concernées soient respectés, il est essentiel de consulter les autorités chargées de la protection des données, conformément aux exigences du droit de l'Union en matière de protection des données à caractère personnel.
- (28) En vertu de l'article 14 de la directive 2011/24/UE, l'Union est chargée de soutenir et faciliter la coopération et l'échange d'informations entre les États membres dans le cadre d'un réseau volontaire reliant les autorités nationales chargées de la santé en ligne désignées par les États membres (le réseau «Santé en ligne»). Les objectifs de ce réseau consistent notamment à œuvrer à la mise en place de systèmes et de services européens de santé en ligne offrant des avantages économiques et sociaux durables ainsi que des applications interopérables, de manière à atteindre un niveau élevé de confiance et de sécurité, à renforcer la continuité des soins et à garantir l'accès à des soins de santé de qualité élevée et sûrs. La décision d'exécution (UE) 2019/1765 de la Commission <sup>(9)</sup> arrête les règles relatives à la création, à la gestion et au fonctionnement du réseau «Santé en ligne». Compte tenu de sa composition et de son domaine d'expertise, le réseau «Santé en ligne» devrait être le principal forum pour débattre des données dont ont besoin les autorités de santé publique et les instituts de recherche, avec la participation également de responsables des autorités nationales de régulation des communications électroniques, des ministères nationaux chargés du numérique et des autorités nationales compétentes en matière de protection des données.
- (29) Le réseau «Santé en ligne» et la Commission devraient également coopérer étroitement avec d'autres organismes et réseaux en mesure d'apporter les contributions nécessaires pour donner effet à la présente recommandation, notamment avec le comité de sécurité sanitaire, le réseau de surveillance épidémiologique des maladies transmissibles, l'ECDC, le comité européen de la protection des données, l'organe des régulateurs européens des communications électroniques et le groupe de coopération en matière de réseaux et de systèmes d'information.
- (30) Dans le cadre de la lutte contre la crise de la COVID-19, faire preuve de transparence, communiquer de façon claire et régulière, et prendre en compte les contributions des personnes et des communautés les plus touchées sera primordial pour maintenir la confiance du public.
- (31) Compte tenu de l'évolution rapide de la situation dans les différents États membres en ce qui concerne la crise de la COVID-19, il est essentiel que l'approche exposée dans la présente recommandation fasse l'objet de rapports des États membres et d'évaluations de la Commission, de façon rapide et régulière tant que la crise persiste.
- (32) La présente recommandation devrait, en tant que de besoin, être complétée par des orientations supplémentaires données par la Commission, notamment en ce qui concerne les implications, sur le plan de la protection des données et du respect de la vie privée, de l'utilisation d'applications mobiles d'alerte et de prévention,

<sup>(9)</sup> Décision d'exécution (UE) 2019/1765 de la Commission du 22 octobre 2019 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE (JO L 270 du 24.10.2019, p. 83).

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

### OBJET DE LA PRÉSENTE RECOMMANDATION

1. La présente recommandation établit un processus en vue de l'élaboration d'une approche commune, appelée «boîte à outils», afin de recourir à des moyens numériques pour faire face la crise. Cette «boîte à outils» consistera en des mesures concrètes permettant une utilisation efficace des technologies et des données, en mettant particulièrement l'accent sur deux domaines:
  - 1) une approche paneuropéenne, coordonnée au niveau de l'Union, de l'utilisation d'applications mobiles permettant aux citoyens de prendre des mesures efficaces et plus ciblées de distanciation sociale, et servant à l'alerte, à la prévention et au traçage des contacts, afin de limiter la propagation de la COVID-19. Cette approche comprendra un suivi des méthodes et un partage des évaluations de l'efficacité de ces applications, de leur interopérabilité et de leurs implications transfrontières, ainsi que de leur conformité aux exigences en matière de sécurité, de respect de la vie privée et de protection des données; et
  - 2) un dispositif commun pour l'utilisation de données anonymisées et agrégées sur la mobilité des populations afin i) de modéliser et de prévoir l'évolution de la maladie, ii) de contrôler l'efficacité de la prise de décision des autorités des États membres en ce qui concerne les mesures telles que la distanciation sociale et le confinement, et iii) de servir de base à l'élaboration d'une stratégie coordonnée de sortie de la crise de la COVID-19.
2. Les États membres devraient prendre ces mesures d'urgence et en étroite coordination avec les autres États membres, la Commission et les autres parties intéressées, et sans préjudice des compétences des États membres dans le domaine de la santé publique. Ils devraient veiller à ce que toutes les mesures soient prises en conformité avec le droit de l'Union, en particulier avec la législation relative aux dispositifs médicaux et au droit au respect de la vie privée et à la protection des données à caractère personnel, ainsi qu'aux autres droits et libertés consacrés par la charte des droits fondamentaux de l'Union européenne. La «boîte à outils» sera complétée par des orientations de la Commission, notamment concernant les implications, sur le plan de la protection des données et du respect de la vie privée, de l'utilisation d'applications mobiles d'alerte et de prévention.

### DÉFINITIONS

3. Aux fins de la présente recommandation, on entend par:
  - a) «applications mobiles», des applications logicielles fonctionnant sur des appareils intelligents, en particulier sur des smartphones, destinées généralement à des interactions variées et ciblées avec des ressources web, qui traitent des données de proximité et d'autres informations contextuelles recueillies par de nombreux capteurs installés dans tout appareil intelligent et qui sont en mesure d'échanger des informations par l'intermédiaire de nombreuses interfaces réseau avec d'autres appareils connectés;
  - b) «réseau "Santé en ligne"», le réseau établi par l'article 14 de la directive 2011/24/UE et dont les tâches ont été précisées par la décision d'exécution (UE) 2019/1765;
  - c) «comité de sécurité sanitaire», l'organe composé de représentants des États membres, institué en vertu de l'article 17 de la décision n° 1082/2013/UE;
  - d) «réseau de surveillance épidémiologique», le réseau de surveillance épidémiologique des maladies transmissibles et des problèmes sanitaires particuliers connexes, géré et coordonné par l'ECDC et assurant la mise en communication permanente de la Commission, de l'ECDC et des autorités compétentes chargées, à l'échelle nationale, de la surveillance épidémiologique, créé en vertu de l'article 6 de la décision n° 1082/2013/UE.

### PROCESSUS D'ÉLABORATION D'UNE BOÎTE À OUTILS POUR L'UTILISATION DE LA TECHNOLOGIE ET DES DONNÉES

4. Ce processus devrait faciliter l'élaboration et l'adoption urgentes, par les États membres et la Commission, d'une boîte à outils prévoyant des mesures pratiques, y compris une approche européenne pour les applications mobiles COVID-19 et pour l'utilisation des données de mobilité en vue de modéliser et de prévoir l'évolution du virus.

5. Aux fins de l'élaboration de la boîte à outils, les États membres, représentés au sein du réseau «Santé en ligne», devraient se réunir immédiatement, et fréquemment par la suite, avec des représentants de la Commission et du Centre européen de prévention et de contrôle des maladies. Ils devraient échanger leurs points de vue sur la manière d'utiliser au mieux des données provenant de diverses sources pour faire face à la crise de la COVID-19 tout en garantissant un niveau élevé de confiance et de sécurité selon des modalités compatibles avec le droit de l'Union, en particulier en ce qui concerne la protection des données à caractère personnel et de la vie privée, et sur la meilleure manière de partager les meilleures pratiques et de favoriser des approches communes à cet égard.
6. Le réseau «Santé en ligne» devrait se réunir immédiatement pour définir les modalités de mise en œuvre de la présente recommandation.
7. Les États membres, représentés au sein du réseau «Santé en ligne», devraient, s'il y a lieu, informer et solliciter pour contribution le comité de sécurité sanitaire, l'organe des régulateurs européens des communications électroniques, le groupe de coopération SRI, les agences compétentes de la Commission, y compris l'ENISA et Europol, et les groupes de travail du Conseil, lorsqu'ils donneront effet à la présente recommandation.
8. Le comité européen de la protection des données et le Contrôleur européen de la protection des données devraient également être étroitement associés aux discussions, afin que la boîte à outils intègre les principes de protection des données et de respect de la vie privée dès la conception.
9. Les autorités des États membres et la Commission devraient assurer une communication régulière, claire et complète à destination du public sur les mesures prises en application de la présente recommandation et offrir au public des possibilités d'interagir et de participer aux discussions.
10. Il devrait être primordial de veiller, tout au long du processus, à respecter l'ensemble des droits fondamentaux, notamment la protection de la vie privée et la protection des données, ainsi qu'à empêcher toute surveillance et stigmatisation. En ce qui concerne ces questions spécifiques, la boîte à outils devrait donc:
  - 1) limiter strictement le traitement de données à caractère personnel aux fins de la lutte contre la pandémie de COVID-19 et faire en sorte que les données à caractère personnel ne soient pas utilisées à d'autres fins, telles que des fins répressives ou commerciales;
  - 2) prévoir un réexamen régulier de la nécessité de maintenir le traitement de données à caractère personnel pour surmonter la crise de la COVID-19 et fixer des clauses appropriées de limitation dans le temps, de manière à garantir que le traitement n'excède pas ce qui est strictement nécessaire à ces fins;
  - 3) prendre des mesures pour faire en sorte que, dès que le traitement n'est plus strictement nécessaire, celui-ci soit effectivement arrêté et que les données à caractère personnel concernées soient irréversiblement détruites, à moins que, selon l'avis de comités d'éthique et d'autorités chargées de la protection des données, leur valeur scientifique pour servir l'intérêt public l'emporte sur les conséquences pour les droits concernés, sous réserve de garanties appropriées.
11. La boîte à outils devrait être élaborée progressivement en tenant compte des discussions menées avec toutes les parties intéressées et du suivi de la situation, des meilleures pratiques, des problèmes et de la solution concernant les sources et types de données dont les autorités de santé publique et les instituts de recherche en matière de santé publique ont besoin et dont ils disposent pour combattre la pandémie de COVID-19.
12. Il convient que la boîte à outils soit partagée avec les partenaires internationaux de l'Union européenne pour échanger les meilleures pratiques et contribuer à endiguer la propagation du virus dans le monde entier.

#### UNE APPROCHE PANEUROPÉENNE POUR LES APPLICATIONS MOBILES COVID-19

13. La première priorité de la boîte à outils devrait consister en une approche paneuropéenne pour les applications mobiles COVID-19, devant être élaborée conjointement par les États membres et la Commission, pour le 15 avril 2020 au plus tard. Le comité européen de la protection des données et le Contrôleur européen de la protection des données seront associés au processus. Cette approche devrait comprendre:
  - 1) des spécifications pour garantir l'efficacité des applications mobiles d'information, d'alerte et de traçage visant à combattre la pandémie de COVID-19 du point de vue médical et technique;
  - 2) des mesures visant à prévenir la prolifération d'applications non compatibles avec le droit de l'Union, à soutenir l'imposition d'obligations en matière d'accessibilité pour les personnes handicapées, d'interopérabilité et de promotion de solutions communes, sans exclure une éventuelle application paneuropéenne;

- 3) des mécanismes de gouvernance devant être appliqués par les autorités de santé publique et une coopération avec l'ECDC;
  - 4) l'identification de bonnes pratiques et de mécanismes d'échange d'informations sur le fonctionnement des applications; et
  - 5) un échange de données avec les organismes publics de surveillance épidémiologique et les instituts de recherche en matière de santé publique concernés, y compris les données agrégées à l'ECDC.
14. Les autorités des États membres, représentées au sein du réseau «Santé en ligne», devraient établir un processus pour échanger des informations et assurer l'interopérabilité des applications lorsque des scénarios transfrontières sont envisagés.

#### **ASPECTS RELATIFS AU RESPECT DE LA VIE PRIVÉE ET À LA PROTECTION DES DONNÉES DANS L'UTILISATION DES APPLICATIONS MOBILES**

15. Les principes de respect de la vie privée et de protection des données devraient guider l'élaboration de la boîte à outils.
16. En ce qui concerne spécifiquement l'utilisation des applications mobiles d'alerte et de prévention COVID-19, il convient de respecter les principes suivants:
- 1) des garanties, telles que les règles applicables en matière de protection des données à caractère personnel et de confidentialité des communications, assurant le respect des droits fondamentaux et empêchant la stigmatisation;
  - 2) la préférence donnée aux mesures efficaces les moins intrusives, telles que l'utilisation de données de proximité, et à l'utilisation de données anonymisées et agrégées dans la mesure du possible; on évitera en revanche le traitement des données relatives à la localisation ou aux déplacements de personnes;
  - 3) les exigences techniques concernant les technologies appropriées (par exemple Bluetooth à basse consommation) pour établir la proximité des appareils, le chiffrement, la sécurité des données, le stockage des données sur les appareils mobiles, la possibilité pour les autorités sanitaires d'avoir accès aux données et de les stocker;
  - 4) des exigences en matière de cybersécurité efficaces pour préserver la disponibilité, l'authenticité, l'intégrité et la confidentialité des données;
  - 5) l'expiration des mesures prises et l'effacement des données à caractère personnel obtenues grâce à ces mesures au plus tard lorsque la pandémie sera déclarée maîtrisée;
  - 6) le téléchargement montant de données de proximité en cas d'infection confirmée et des méthodes appropriées pour alerter les personnes qui ont été en contact étroit avec la personne infectée, qui doit rester anonyme; enfin,
  - 7) des exigences de transparence concernant les paramètres de confidentialité, afin de susciter la confiance dans les applications.
17. La Commission publiera des orientations précisant les principes en matière de respect de la vie privée et de protection des données, à la lumière des constatations pratiques résultant de l'élaboration de la boîte à outils et de sa mise en œuvre.

#### **UTILISATION DES DONNÉES DE MOBILITÉ POUR ÉCLAIRER LES MESURES À PRENDRE ET LA STRATÉGIE DE SORTIE**

18. La seconde priorité assignée à la boîte à outils devrait être une approche commune pour l'utilisation des données de mobilité anonymisées et agrégées, nécessaires pour:
- 1) les travaux de modélisation permettant de cartographier et prévoir la propagation de la maladie et son incidence sur les besoins des systèmes de santé des États membres, par exemple en matière d'unités de soins intensifs dans les hôpitaux et d'équipements de protection individuelle; et
  - 2) l'optimisation de l'efficacité des mesures visant à endiguer la propagation du virus COVID-19 et à en traiter les effets, y compris le confinement (et le déconfinement), et à obtenir et utiliser ces données.
19. Pour élaborer cette approche, les États membres (représentés au sein du réseau «Santé en ligne», qui coordonnera ses travaux avec le comité de sécurité sanitaire, le réseau de surveillance épidémiologique, l'ECDC et, si nécessaire, l'ENISA) devraient échanger les meilleures pratiques sur l'utilisation des données de mobilité, partager et comparer leurs modélisations et prévisions sur la propagation du virus, et surveiller les effets des mesures destinées à limiter cette propagation.



20. L'approche visée devrait comprendre les éléments suivants:

- 1) l'utilisation appropriée de données de mobilité anonymisées et agrégées à des fins de modélisation, pour comprendre comment le virus va se propager et modéliser les effets économiques de la crise;
- 2) des conseils aux autorités publiques afin qu'elles vérifient auprès des fournisseurs de données la méthode appliquée pour anonymiser les données et qu'elles procèdent à un contrôle de plausibilité sur l'emploi de cette méthode;
- 3) la mise en place de garanties afin d'empêcher la désanonymisation et d'éviter la ré-identification des personnes, notamment des garanties quant à un niveau suffisant de sécurité des données et de l'infrastructure informatique, et une évaluation des risques de ré-identification en cas de mise en corrélation des données anonymisées avec d'autres données;
- 4) la suppression immédiate et irréversible de toutes les données traitées accidentellement qui permettraient d'identifier des personnes, et la communication aux fournisseurs de données ainsi qu'aux autorités compétentes de ce traitement accidentel et de la suppression des données;
- 5) la suppression des données en principe après 90 jours ou, en tout état de cause, au plus tard lorsque la pandémie sera déclarée maîtrisée; et
- 6) la limitation du traitement des données aux seules fins indiquées ci-dessus et l'exclusion du partage des données avec des tiers.

#### RAPPORTS ET EXAMEN

21. L'approche paneuropéenne pour les applications mobiles COVID-19 sera publiée le 15 avril et sera complétée par des orientations de la Commission sur le respect de la vie privée et la protection des données.
22. Les États membres devraient, au plus tard le 31 mai 2020, faire rapport à la Commission sur les mesures prises en application de la présente recommandation. Par la suite, des rapports devraient être présentés régulièrement aussi longtemps que la crise du COVID-19 persistera.
23. À compter du 8 avril 2020, les États membres devraient permettre à la Commission et aux autres États membres de prendre connaissance des mesures qu'ils auront appliquées dans les domaines couverts par la présente recommandation, en vue d'un examen réciproque. Les États membres et la Commission auront une semaine pour présenter leurs observations éventuelles sur ces mesures. L'État membre concerné devrait tenir le plus grand compte de ces observations.
24. À partir de juin 2020, sur la base de ces rapports des États membres, la Commission évaluera les progrès accomplis et les effets de la présente recommandation. La Commission pourra adresser d'autres recommandations aux États membres, notamment sur le calendrier des mesures appliquées dans les domaines couverts par la présente recommandation.

Fait à Bruxelles, le 8 avril 2020.

*Par la Commission*  
Thierry BRETON  
*Membre de la Commission*

---