Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG

Rapport explicatif concernant l'ordonnance sur le système de traçage de proximité pour le coronavirus SARS-CoV-2 (OSTP)

Juin 2020

Table des matières

1 Remarques générales

1.1 Contexte

Suite au recul continu du nombre de nouvelles infections au coronavirus, la Suisse se trouve depuis le 11 mai 2020 dans la phase dite d'endiguement. Il s'agit dès lors, à l'aide du traçage ciblé et systématique des contacts effectué par les cantons, de retracer de manière cohérente les chaînes de transmission, d'isoler les personnes infectées et de placer leurs contacts étroits en quarantaine. Ainsi, un contrôle à long terme de l'épidémie deviendra possible.

Un système de traçage de proximité, c'est-à-dire l'application SwissCovid avec les autres composants nécessaires, ne peut pas remplacer le traçage classique des contacts ; il peut être utilisé toutefois comme un outil de soutien. Ces systèmes sont particulièrement efficaces quand ils sont utilisés par des personnes à forte mobilité et qui se trouvent régulièrement dans des endroits fréquentés par de nombreuses personnes qui leur sont inconnues.

Deux motions de même teneur (CIP-N 20.3144 du 22 avril 2020 et CIP-E 20.3168 du 30 avril 2020 « Bases juridiques nécessaires à l'introduction des applications d'alerte Corona [application Corona Proximity Tracing] ») ont chargé le Conseil fédéral de présenter au Parlement la base légale nécessaire à l'introduction d'applications d'alerte sur le coronavirus (application « Corona Proximity Tracing »). Avec le message concernant la modification urgente du 20 mai 2020 de la loi sur les épidémies (LEp)[1] en lien avec le coronavirus (système de traçage de proximité) (FF 2020 4361), le Conseil fédéral a soumis au Parlement une telle proposition de réglementation. Celle-ci prévoyait, en réponse à ces deux motions, une solution technique qui ne stocke pas les données personnelles de manière centralisée et un emploi de l'application en question sur une base volontaire. Au cours des débats parlementaires, le Conseil national et le Conseil des États ont complété le projet du Conseil fédéral, d'une part, par un droit de se soumettre gratuitement à un test d'identification du coronavirus et à un test sérologique de mise en évidence des anticorps au coronavirus, sur présentation de la notification d'une exposition potentielle au coronavirus (voir à ce sujet le ch. 1.2.1 ci-après). D'autre part, le Parlement a recommandé au Conseil fédéral d'examiner en parallèle une solution qui prévoit aussi, pour les personnes informées par le système et se mettant volontairement en quarantaine, un droit à une allocation pour perte de gain si elles ne peuvent pas poursuivre leur activité professionnelle en quarantaine (voir à ce sujet le ch. 1.2.2 ci-après). Les deux chambres de l'Assemblée fédérale suisse ont déclaré le projet urgent et l'ont accepté en votation finale le 19 juin 2020.

L'essai pilote relatif au système suisse de traçage de proximité s'est déroulé à partir du 25 mai 2020. L'application SwissCovid remplace l'application testée dans ce cadre, mais le système est globalement maintenu.

1.2 Liens avec d'autres réglementations

1.2.1 Gratuité des tests

Toute personne qui a été informée par le système de traçage de proximité pour le coronavirus SARS-CoV-2 au sens de l'art. 60*a* LEp (système TP) de son exposition potentielle au coronavirus peut, sur présentation du message du système TP, se soumettre gratuitement à un test d'identification du coronavirus et à un test sérologique de mise en évidence des anticorps au coronavirus (art. 60*a*, al. 4, LEp). Le Conseil fédéral n'a pas précisé ce droit de se soumettre gratuitement à un test et la prise en charge des coûts correspondants dans la présente ordonnance. Il règle les critères et la procédure de prise en charge de ces coûts par la Confédération aux art. 26 et 26*a* de l'Ordonnance 3 COVID-19 du 19 juin 2020 (RS 818.101.24). Le droit de se soumettre gratuitement à un test après avoir reçu une notification par l'application SwissCovid fait partie des critères de suspicion, de prélèvement d'échantillons et de déclaration de l'OFSP du 24 juin 2020[2] qui sont pertinents pour la prise en charge.

[1] Loi du 28 septembre 2012 sur les épidémies (RS **818.101**).

[2] L'état actuel peut être consulté en tout temps sous www.ofsp.admin.ch > Maladies > Lutter contre les maladies infectieuses > Systèmes de déclaration pour maladies infectieuses > Maladies infectieuses à déclaration obligatoire > Formulaires de déclaration.

1.2.2 Allocations pour perte de gain en cas de quarantaine

Par courrier, la CSSS-N et la CSSS-E ont recommandé au Conseil fédéral d'examiner une solution qui prévoit aussi, pour les personnes averties par le système TP et se mettant volontairement en quarantaine, un droit à une allocation pour perte de gain si elles ne peuvent pas poursuivre leur activité professionnelle en quarantaine. Il est toutefois important de souligner que la seule notification ne donne pas droit à la poursuite du versement du salaire ou à une allocation pour perte de gain. L'*infoline SwissCovid* (consultation gratuite, utilisée sur mandat de l'Office fédéral de la santé publique [OFSP] comme hotline nationale) conseillera plutôt aux personnes averties par l'application et qui ne peuvent pas travailler à la maison de contacter le service cantonal compétent. Celui-ci décidera, sur la base d'un entretien, s'il ordonne une quarantaine à la personne concernée. Si une quarantaine est ordonnée ou décidée, la personne concernée a droit à la poursuite du versement du salaire selon l'opinion qui prévaut (en vertu de l'art. 324 ou 324*a* CO). Mais en l'état actuel des choses, cette question n'a pas encore été tranchée par un tribunal. Le droit à une allocation pour perte de gain est réglé actuellement dans l'ordonnance sur les pertes de gain COVID-19 (RS 830.31) et devrait être précisé sur la base de la future loi COVID-19, eu égard à l'abrogation de cette ordonnance le 16 septembre 2020.

1.2.3 Ordonnance COVID-19 essai pilote traçage de proximité

Entre le 25 mai et le 25 juin 2020, le système TP suisse a été testé dans le cadre d'un essai pilote en s'appuyant sur l'art. 17*a* de la loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1) et l'ordonnance du 13 mai 2020 COVID-19 essai pilote traçage de proximité (RO 2020 1589). Cet essai pilote a fait place à l'exploitation régulière du système TP dès l'entrée en vigueur de la base légale (art. 60*a* LEp) et de la présente ordonnance. L'ordonnance COVID-19 essai pilote traçage de proximité est abrogée par l'art. 16 de la présente ordonnance.

2 Interopérabilité internationale

La compatibilité de l'application SwissCovid avec des applications étrangères similaires est un objectif majeur du système TP. Mais pour l'heure, l'application SwissCovid ne peut pas informer les participants s'il y a eu une situation de rapprochement pertinente du point de vue épidémiologique avec un utilisateur infecté d'une application étrangère. L'application SwissCovid n'est pas reliée à des systèmes étrangers. La loi prévoit, s'agissant de l'interopérabilité internationale de l'application SwissCovid, qu'un échange transfrontalier n'est envisagé que si un niveau de protection des données comparable à la Suisse est assuré (art. 62*a* LEp). En outre, les principes de base du système TP doivent être pris en compte. En l'absence d'un concept technique définitif et d'accords juridiques, la question ne peut pas être réglée dans la présente ordonnance. À l'heure actuelle, l'interopérabilité est notamment visée avec des systèmes en principe compatibles en Allemagne, en Italie et en Autriche. Une fois les conditions-cadres clarifiées, le Conseil fédéral adaptera le cas échéant l'ordonnance en conséquence.

3 Commentaire des dispositions

Art. 1 Objet

Les détails de l'organisation, de l'exploitation et du traitement des données du système TP font l'objet de la présente ordonnance. Le Conseil fédéral remplit ainsi son mandat de régler ces modalités au niveau de l'ordonnance (art. 60*a*, al. 7, LEp).

Art. 2 Structure

D'un point de vue technique, le système TP se base sur le projet DP-3T (*Decentralized Privacy Preserving Proximity Tracing*) développé notamment par l'École polytechnique fédérale de Lausanne et, partant, sur le principe de protection des données dès la conception (*privacy by design*). Grâce à des méthodes cryptographiques innovantes et à son traitement décentralisé des données, il ne contient pratiquement aucune donnée permettant d'identifier des personnes (données personnelles). Par conséquent, tous les composants du système TP et leur exploitation sont conçus de manière à ce que les données personnelles ne soient traitées que si cela est nécessaire au fonctionnement du système. Lors du traitement des données, toutes les mesures techniques et organisationnelles appropriées doivent donc être prises pour éviter que les participants ne puissent être identifiés (art. 60*a*, al. 5, let. a, LEp).

En même temps, le système TP prévoit que dans la mesure du possible, les données sont traitées sur des composants décentralisés que les participants installent sur leur téléphone portable ; en particulier, les données enregistrées sur le téléphone portable d'un participant concernant d'autres participants sont traitées et enregistrées exclusivement sur ce téléphone (art. 60*a*, al. 5, let. b, LEp). La structure du système TP visée à l'art. 2 garantit le respect de ces exigences.

En vertu de l'*al. 1*, le système TP s'articule en plusieurs éléments dans lesquels seules sont enregistrées les données nécessaires à l'exploitation du système global. Il comprend, d'une part, un système de gestion de données relatives aux situations de rapprochement (système GR), composé d'un logiciel que les participants installent sur leur téléphone portable (application SwissCovid) et d'un *back-end* (*back-end* GR) et, d'autre part, un système permettant de gérer les codes pour autoriser les notifications (système de gestion des codes), composé d'un *front-end* en ligne et d'un *back-end*. Le contenu, le fonctionnement et la combinaison des différents éléments sont précisés aux art. 5, 6 et 9 (voir les commentaires correspondants).

L'*al. 2* précise que le *back-end* GR et le système de gestion des codes sont administrés comme des serveurs centraux par l'OFSP. Ces derniers, des éléments indispensables au fonctionnement de l'application SwissCovid, sont développés et administrés par l'Office fédéral de l'informatique et de la télécommunication (OFIT) sur mandat de l'OFSP. L'utilisation des éléments centraux nécessaires ne change rien au fait que les données enregistrées sur le téléphone portable d'un participant concernant d'autres participants sont traitées et enregistrées exclusivement sur ce téléphone (art. 60*a*, al. 5, let. b, LEp).

Art. 3 Caractère volontaire

L'*al. 1* précise l'exigence légale du caractère volontaire de la participation au système TP (art. 60*a*, al. 3, phrase 1, LEp) en ce sens qu'aussi bien l'installation que l'utilisation (c.-à-d. notamment l'activation de la fonction Bluetooth) de l'application SwissCovid s'effectuent sur une base volontaire.

À noter par ailleurs que de par la loi, les autorités, les entreprises et les particuliers ne peuvent pas favoriser ou désavantager une personne en raison de sa participation ou de sa non-participation au système TP ; les conventions contraires sont sans effet (art. 60*a*, al. 3, phrase 2, LEp).

L'*al. 2* précise en outre qu'en cas d'infection, la saisie du code d'autorisation pour informer les autres participants qu'ils ont potentiellement été exposés au coronavirus est également volontaire et nécessite le consentement exprès de la personne infectée. L'information des personnes potentiellement exposées au coronavirus se fait sans indication de données personnelles ; malgré tout, une personne avertie peut découvrir le cas échéant, à l'aide des contacts sociaux des derniers jours, quelle est la personne infectée avec laquelle elle a été en contact pertinent d'un point de vue épidémiologique. Comme la personne avertie sait alors la personne concernée a attrapé le coronavirus, il s'agit de communication de données personnelles sensibles, qui nécessite le consentement exprès de la personne concernée (cf. art. 3, let. c, ch. 2 et art. 4, al. 5, phrase 2, LPD). L'application en informe la personne infectée. Les autres personnes ne sont informées qu'à la suite de la confirmation, dans l'application SwissCovid, que la personne infectée l'a compris et souhaite malgré tout la notification des autres personnes.

Art. 4 Organe fédéral responsable

La législation fédérale sur la protection des données est applicable au système TP (art. 60*a*, al. 6, LEp). Le système global avec tous les composants (y compris l'application SwissCovid) est intégralement soumis à la responsabilité de l'OFSP, l'exploitant du système, au niveau du droit de la protection des données. Le *back-end* GR et le système de gestion des codes sont ainsi administrés par l'OFIT sur mandat de l'OFSP (voir le commentaire de l'art. 2, al. 2). Cela ne change rien à la possibilité de faire valoir le cas échéant les droits relevant de la protection des données (en particulier les droits d'accès et à la rectification des données ; cf. art. 5, al. 2 et art. 8 LPD) auprès de l'OFSP. Ces droits ne sont applicables que s'il y a effectivement des données personnelles (art. 3, let. a, LPD) et si l'OFSP y a accès. Les principes déterminants de la protection des données dès la conception l'empêchent dans la mesure du possible (en particulier l'art. 60*a*, al. 5, let. a et b, LEp ; voir à ce sujet le commentaire de l'art. 2). L'OFSP ne peut par exemple pas donner des renseignements sur les situations de rapprochement pour une certaine personne ou corriger ces données. Il ne peut pas consulter de telles données,

car elles sont uniquement enregistrées de manière décentralisée sur les téléphones portables.

Art. 5 Fonctionnement de base

L'*al. 1* décrit le contenu des données qui sont enregistrées dans le *back-end* GR et auxquelles celui-ci donne aux applications SwissCovid un accès en ligne. Il s'agit des clés privées (*private keys*) des participants dont l'infection est avérée pendant la période où il y a une forte probabilité, d'un point de vue épidémiologique, que la personne infectée ait déjà été contagieuse (voir en particulier le commentaire de l'art. 6, al. 3). Le *back-end* GR contient en outre la date de chaque clé.

Al. 2 à 4 : l'*al. 2* définit les fonctions que remplit l'application SwissCovid selon la *phrase d'introduction* « à l'aide d'une interface avec le système d'exploitation du téléphone portable ». Concrètement, l'interface en question est exploitable dans l'*Exposure Notificiation Framework* développé conjointement par Google et Apple. Elle est disponible avec les dernières versions iOS et Android d'Apple et de Google (à partir de la version 13.5 pour iOS et de la version 6 des derniers services Google Play pour Android). L'application SwissCovid, qui s'appuie sur cette interface, est donc en principe opérationnelle sur les versions du système d'exploitation qui contiennent l'interface en question. L'utilisation de l'interface permet notamment d'augmenter la précision des mesures Bluetooth et de réduire la consommation d'électricité supplémentaire au strict minimum. Par ailleurs, l'interface permet à l'application de fonctionner en arrière-plan si elle est activée. D'un point de vue technique, le système d'exploitation sous-jacent ou l'interface concernée avec le système d'exploitation du téléphone portable soutient l'application SwissCovid de manière déterminante dans l'exécution de ses fonctions, même si le système d'exploitation et l'interface ne sont pas véritablement des éléments de l'application SwissCovid (ni, à cet égard, des composants du système TP au sens de l'art. 2).

D'un point de vue juridique, les prescriptions de l'art. 60*a* LEp et de la présente ordonnance sont une nouvelle fois déterminantes pour le système TP et ses composants. À ce titre, elles ne couvrent pas les fonctions des systèmes d'exploitation de Google et d'Apple utilisées par l'application SwissCovid. Dans ce cadre, l'ordonnance attribue juridiquement les fonctions déterminantes fournies par le système d'exploitation à l'application SwissCovid. Concrètement, cela signifie en particulier :

- L'*al. 3* précise que les *fonctions des systèmes d'exploitation utilisées via l'interface* doivent satisfaire aux prescriptions de l'art. 60*a* LEp et de la présente ordonnance, même si les systèmes d'exploitation de Google et d'Apple ne sont pas soumis à la présente ordonnance comme tels. En d'autres termes, en cas de modification du logiciel Android ou iOS dans le domaine pertinent pour l'application à la suite de laquelle les dispositions de l'ordonnance ne seraient plus remplies, le Conseil fédéral devrait adapter l'ordonnance dans le cadre des prescriptions légales ou – si ce n'est pas possible – mettre un terme à la collaboration (utilisation de l'interface avec le système d'exploitation).
- En vertu de l'*al. 3*, l'OFSP, l'exploitant du système, est tenu de s'assurer que les fonctions des systèmes d'exploitation utilisées via l'interface respectent les prescriptions correspondantes, notamment en se procurant les garanties appropriées de Google et d'Apple.
- À noter à cet égard que l'art. 60*a*, al. 5, let. e, LEp fixe la publicité du code source et des spécifications techniques de tous les composants du système TP, alors qu'Apple et Google ne publient pas les codes sources de leurs systèmes d'exploitation (et de l'interface utilisée) en tant qu'entreprises commerciales. Le législateur en était conscient en adoptant les dispositions en question. L'al. 3 précise donc clairement que les fonctions des systèmes d'exploitation utilisées via l'interface ne doivent pas satisfaire à la réglementation concernant le code source au sens de l'art. 60*a*, al. 5, let. e, LEp. Cela n'affecte pas la publication des spécifications techniques (et les obligations de l'OFSP qui en découlent).

Dans le détail, l'application SwissCovid fonctionne comme suit avec le système d'exploitation :

- *Let. a :* le système d'exploitation génère chaque jour une nouvelle clé privée qui ne permet pas d'identifier l'application SwissCovid, le téléphone portable ou le participant.
- *Let. b :* l'enregistrement des situations de rapprochement entre les participants se fonde sur la technologie sans fil Bluetooth ; aucune donnée de géolocalisation n'est collectée ni traitée de quelque façon que ce soit par le système TP (art. 60*a*, al. 5, let. c, LEp). La localisation doit être ainsi activée sur les appareils équipés de systèmes d'exploitation Android pour que Bluetooth fonctionne. Mais

l'application SwissCovid n'a accès à aucun moment à la position des participants. À portée de Bluetooth, le système d'exploitation échange alors un code d'identification, modifié au moins toutes les demi-heures (*random ID*), avec tous les autres systèmes d'exploitation qui ont également installé une application autorisée par Google ou Apple et compatible. Ce code est généré à partir de la clé privée actuelle au sens de la let. a, mais ne permet ni de remonter à la clé, ni d'identifier l'application SwissCovid, le téléphone portable ou le participant.

- *Let. c :* le système d'exploitation enregistre sur le téléphone portable les codes d'identification reçus, la force du signal, la date et la durée approximative du rapprochement. L'échange fonctionne, comme cela a été dit, à portée de la technologie sans fil Bluetooth. En d'autres termes, tous les codes d'identification sont échangés et enregistrés dans un rayon potentiel de 50 mètres. L'échange et l'enregistrement ne sont pas limités aux téléphones portables équipés d'applications SwissCovid suisses ; l'un et l'autre sont en principe possibles sur tous les téléphones portables qui utilisent l'*Exposure Notification Framework* pour leurs applications de traçage de proximité (compatibles entre elles). Du point de vue aussi bien de la technique que du droit de la protection des données, cela est nécessaire pour les raisons suivantes :
  D'un point de vue technique, des signaux Bluetooth de force différente sont utilisés en fonction du type de téléphone portable. Le cryptage des paquets de données diffusés comprend aussi l'indication de la force du signal envoyé par le module d'émission de ce téléphone, ce qui est nécessaire pour l'estimation de la distance (à l'aide de la force du signal reçu) par le téléphone portable récepteur. Le système d'exploitation peut également ne pas reconnaître, à l'aide des codes d'identification envoyés, si l'application de traçage de proximité utilisée est l'application suisse ou une application étrangère compatible. Pour la protection des participants sous l'angle de la protection des données, un décryptage de la force du signal enregistrée (et donc, déduite par l'application SwissCovid, la détermination des rapprochements définis comme pertinents d'un point de vue épidémiologique au sens de la let. e) n'est entrepris qu'*après* une notification d'infection (s'agissant d'une information). En d'autres termes, le code d'identification ne peut pas être décrypté sans la clé privée de la personne infectée. Ce qui veut dire que le système TP peut le cas échéant aussi décrypter les codes d'identification des personnes utilisant des applications étrangères (et vice versa) s'il a été relié à un système étranger correspondant au sens de l'art. 62*a* LEp (c.-à-d. sous réserve d'un niveau adéquat de protection de la personnalité).
- *Let. d :* l'application SwissCovid extrait à intervalles réguliers une liste des clés privées des participants infectés et laisse le système d'exploitation vérifier si au moins un code d'identification enregistré localement a été généré avec une clé privée de la liste.
- *Let. e :* si tel est le cas et que les conditions relatives au rapprochement définies comme pertinentes d'un point de vue épidémiologique sont remplies, l'application SwissCovid émet une information. À l'heure actuelle, ces conditions épidémiologiques relatives au rapprochement sont remplies selon l'*annexe* quand il y a au moins une situation de rapprochement d'une distance de 1,5 mètre ou moins (estimée à l'aide de la force des signaux reçus) avec un téléphone portable d'un participant infecté et que la somme de la durée de tous ces rapprochements atteint quinze minutes en un jour. En vertu de l'*al. 4*, le Département fédéral de l'intérieur (DFI) gère ces conditions relatives au rapprochement et l'annexe correspondante en fonction de l'état actuel des connaissances scientifiques.

Art. 6 Fonctionnement après une infection

L'*al. 1* prévoit qu'en cas d'infection avérée (par un test positif au SARS-CoV-2), le professionnel disposant des droits d'accès (voir à ce sujet le commentaire de l'art. 9) génère dans le *front-end* en ligne du système de gestion des codes un code d'autorisation unique et valable pendant 24 heures (cf. art. 13, al. 2) (*Covidcode*). En outre, il saisit dans le système la date où les premiers symptômes sont apparus ou, si la personne infectée ne présente aucun symptôme, la date du test.

En vertu de l'*al. 2*, le professionnel disposant des droits d'accès communique le code d'autorisation à la personne infectée. Celle-ci peut saisir le code d'autorisation dans son application SwissCovid avec un délai de réflexion de 24 heures (durée de validité du code d'autorisation) et confirmer sa volonté de le notifier aux participants concernés. La saisie du code d'autorisation et l'information des autres participants ne se font ainsi que si la personne infectée y a expressément consenti (art. 3, al. 2).

En vertu de l'*al. 3*, le *back-end* du système de gestion des codes confirme à l'application SwissCovid la validité du code d'autorisation saisi. Il retranche deux jours de la date d'apparition des premiers symptômes ou du test positif et communique cette nouvelle date à l'application SwissCovid. Ces deux jours précédant l'apparition des symptômes correspondent à la période où il y a une grande probabilité, d'un point de vue épidémiologique, que la personne infectée ait déjà été contagieuse alors qu'elle n'avait pas encore de symptômes. Il est ainsi possible d'avertir les personnes qui étaient contact avec la personne infectée avant même qu'elle ne soit au courant de son infection, mais alors qu'était parfois déjà contagieuse.

En vertu de l'*al. 4*, l'application SwissCovid transmet au *back-end* GR, après confirmation de la validité du code d'autorisation, les données suivantes : les clés privées pour chaque jour dès le moment où une infection était possible ainsi que la date de la clé correspondante.

En vertu de l'*al. 5*, le *back-end* GR inscrit ces clés privées et les dates correspondantes dans sa liste pour l'interrogation par les autres applications SwissCovid qui, à l'aide des clés privées de cette liste, font vérifier par le système d'exploitation si elles étaient en contact étroit avec la personne infectée.

En vertu de l'*al. 6*, l'application SwissCovid génère, après la transmission des clés privées, une nouvelle clé privée qui ne permet pas de remonter à d'anciennes clés privées. Pour l'heure, toutes les clés privées sont générées de telle sorte qu'elles ne permettent pas de remonter à d'anciennes clés privées, raison pour laquelle l'application génère d'ordinaire le lendemain une nouvelle clé privée. L'al. 6 reste cependant nécessaire dans la mesure où il fixe le principe selon lequel, avant la notification d'une infection, les clés privées (enregistrées dans le *back-end* GR) ne permettent pas de déduire les clés privées après la notification. Et ce afin d'empêcher, par exemple, qu'il soit possible de surveiller l'isolement d'une personne concernée à l'aide de cette clé privée (voir aussi l'art. 60*a*, al. 2, phrase 2, LEp).

Art. 7 Contenu de l'information

L'*al. 1* fixe le contenu de l'information que les participants reçoivent le cas échéant en vertu de l'art. 5, al. 2, let. e. Une personne informée est avisée par l'application SwissCovid du fait qu'elle a potentiellement été exposée au coronavirus (*let. a*) et du jour où cela s'est produit la dernière fois (*let. b*). Elle n'apprend pas en revanche qui est infecté et a déclenché l'information. Seuls le médecin traitant et le professionnel disposant des droits d'accès au sens de l'art. 9 connaissent l'identité de la personne infectée qui saisit le code d'autorisation. Il se peut toutefois que la personne informée puisse découvrir, à l'aide des contacts sociaux des derniers jours, quelle peut être la personne infectée. Mais rien ne permet de l'éviter et il n'en va pas autrement dans le traçage classique des contacts. En outre, l'information comprend la mention que l'OFSP gère une ligne info SwissCovid offrant des conseils sans frais (*let. c*) ainsi que des règles de conduite recommandées par l'OFSP qui visent à briser les chaînes de transmission conformément aux données épidémiologiques actuelles (*let. d*).

L'*al. 2* précise que le système TP ne donne aucune consigne aux participants. Il ne peut ni procéder à une évaluation médicale, ni ordonner des mesures relevant du droit des épidémies à la place des autorités compétentes (comme p. ex. une quarantaine). Le système TP et les données qu'il traite ne peuvent pas servir aux autorités cantonales compétentes à ordonner ou à mettre en œuvre des mesures au sens des art. 33 à 38 LEp (art. 60*a*, al. 2, phrase 2, LEp). Il ne permet notamment pas de surveiller une quarantaine imposée. Le système TP et les données qu'il traite servent en fin de compte (sous réserve d'évaluations statistiques rudimentaires) « uniquement » à informer les personnes potentiellement exposées au coronavirus (art. 60*a*, al. 2, phrase 1, LEp).

Art. 8 Contenu du système de gestion des codes

En vertu de l'*al. 1*, le système de gestion des codes contient les données suivantes : les codes d'autorisation (*let. a*) ; la date à laquelle les premiers symptômes sont apparus ou, si la personne infectée ne présente aucun symptôme, la date du test (*let. b*) ; enfin, la date de la destruction de ces données, qui intervient 24 heures après la génération du code en vertu de l'art. 13, al. 2 (*let. c*).

L'*al. 2* précise que ces données ne permettent pas de remonter aux participants. Seul le professionnel disposant des droits d'accès au sens de l'art. 9 sait pour qui il génère le code d'autorisation. Cette information n'est cependant saisie nulle part dans le système TP. Le système de gestion des codes

confirme uniquement à l'application SwissCovid la validité du code d'autorisation ; à aucun moment il ne dispose d'informations sur la personne à qui est attribué ce code d'autorisation.

Art. 9 Droits d'accès au système de gestion des codes

L'*al. 1* définit les personnes disposant des droits d'accès qui peuvent émettre le code d'autorisation. Le code d'autorisation est généré et édité par les personnes chargées du traçage classique des contacts par le canton ou, pour les militaires, au service du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Le canton ou le DDPS peut alors utiliser sa propre structure organisationnelle ou charger des organisations privées du traçage classique des contacts. Le médecin traitant et son personnel assistant peuvent le cas échéant aussi entrer en ligne de compte comme personnes disposant potentiellement des droits d'accès. Les droits d'accès sont toujours limités à la génération d'un code après une infection avérée ; il n'y a pas d'accès aux données du système TP en mode lecture ou traitement.

L'*al. 2* précise que les professionnels disposant des droits d'accès s'inscrivent par le biais du système central de gestion des accès et des autorisations de l'administration fédérale pour les applications Web (système eIAM) (ce pour quoi ils ont besoin d'une identité électronique).

En vertu de l'*al. 3*, l'OFSP attribue et gère les droits d'accès. Il peut autoriser les médecins cantonaux, le médecin en chef de l'armée ou certains membres de leur personnel assistant à attribuer des droits d'accès à du personnel assistant. À noter que l'OFSP peut également, sur la base de l'art. 10, al. 2, déléguer à des tiers l'attribution des droits d'accès.

Art. 10 Prestations de tiers

L'*al. 1* permet à l'OFSP, l'exploitant du système, de charger des tiers de fournir aux applications SwissCovid la liste des données requises pour accéder en ligne aux informations. Concrètement, l'OFSP (ou l'OFIT sur mandat de sa part) utilise actuellement Amazon Web Services pour distribuer la liste avec les clés privées par le biais de leur Content Delivery Network (CDN). L'utilisation de ce service est nécessaire, parce que les applications SwissCovid (potentiellement des millions) demandent des mises à jour de la liste à une fréquence élevée, ce qui implique le traitement d'un nombre considérable de requêtes. Les tiers mandatés ne peuvent associer à personne les clés privées anonymes des personnes infectées qui sont enregistrées sur la liste.

Par ailleurs, l'OFSP peut, en vertu de l'*al. 2*, déléguer à des organisations appropriées de droit privé ou public l'attribution (et donc la gestion) des droits d'accès au système de gestion des codes. Le tiers désigné le cas échéant doit garantir une vérification fiable et juridiquement correcte des droits accordés aux professionnels.

L'*al. 3* prévoit que les tiers ainsi mandatés doivent être contractuellement tenus de respecter les prescriptions de l'art. 60*a* LEp et de la présente ordonnance. Pour ce faire, l'OFSP (ou le cas échéant l'OFIT sur mandat de sa part) doit conclure des contrats correspondants et contrôler le respect de ces prescriptions. La disposition précise par ailleurs que la réglementation concernant le code source au sens de l'art. 60*a*, al. 5, let. e, LEp fait exception. Le législateur a adopté cette prescription, en vertu de laquelle le code source de tous les composants du système TP est public, sachant que le CDN d'Amazon Web Services est utilisé pour la distribution de la liste avec les clés privées et que le code source n'est pas public à cet égard.

Art. 11 Journaux des accès

L'*al. 1* règle les dispositions applicables à l'enregistrement et à l'analyse des données journalisées. Les accès des professionnels disposant des droits d'accès pour générer le code d'autorisation sont ainsi journalisés à des fins de sécurité des données. Quant à l'utilisation du système GR, les données secondaires relatives à ces données de communication sont journalisées par ailleurs lors de l'accès du flux de données au réseau fédéral à des fins de protection de l'infrastructure électronique. Pour éviter une analyse des données personnelles lors de la transmission des données d'un participant infecté, un flux de données supplémentaire est généré. Les autorités fédérales ne peuvent pas associer une infection à une personne donnée, à un téléphone portable donné ou à une application SwissCovid donnée. L'enregistrement et l'analyse des journaux des accès concernés sont soumis aux art. 57*i* à 57*q* de la loi

du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA ; RS 172.010) et à l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS 172.010.442). Par ailleurs, les accès à la liste au sens de l'art. 10, al. 1 sont journalisés (c.-à-d. dans le CDN d'Amazon Web Services). Le tiers actuellement mandaté, Amazon Web Services, est contractuellement tenu de les enregistrer dans la région « UE (Francfort) » et de ne pas les utiliser lui-même. L'OFIT dispose d'un accès à ces données journalisées. Les dispositions précitées sont aussi déclarées applicables à l'enregistrement et à l'analyse de ces journaux d'accès par l'OFIT.

L'*al. 2* précise qu'hormis ces journaux des accès et l'enregistrement des rapprochements, le système TP n'enregistre aucun journal des activités des *front-ends* du système de gestion des codes et des applications SwissCovid.

Art. 12 Communication à des fins statistiques

L'OFSP met régulièrement à la disposition de l'Office fédéral de la statistique (OFS) les données actuelles disponibles dans les deux *back-ends* à des fins statistiques (cf. art. 60*a*, al. 2, phrase 1, LEp). Ces données sont mises à la disposition de l'OFS sous une forme entièrement anonymisée afin de permettre des évaluations statistiques rudimentaires (en particulier le nombre de codes d'autorisation générés par les professionnels disposant des droits d'accès et de codes d'autorisation saisis par les participants dans l'application SwissCovid). À noter à cet égard que l'OFS est aussi tenu, en vertu de l'art. 13, al. 5, de détruire ces données dans les délais prévus à l'art. 13. Il est ainsi exclu de pouvoir conserver des données à des fins statistiques plus longtemps que ne l'exigerait l'information au sens de l'art. 5, al. 2, let. e (cf. art. 60*a*, al. 5, let. d, LEp).

Art. 13 Destruction des données

Les données traitées avec le système TP doivent être supprimées dès qu'elles ne sont plus nécessaires aux messages d'information des participants (art. 60*a*, al. 5, let. d, LEp). Cela implique des moments différents pour la destruction :

- *Al. 1* : les données relatives au rapprochement, qui ne sont pertinentes que pour la période d'une possible infection, sont détruites en continu après quatorze jours.
- *Al. 2* : le code d'autorisation est détruit 24 heures après sa saisie par le professionnel de la santé, indépendamment de son utilisation ou de sa non-utilisation.
- *Al. 3* : les données journalisées par des tiers mandatés au sens de l'art. 10, al. 1 sont détruites sept jours après leur saisie.
- *Al. 4* : pour le reste, les données journalisées sont détruites conformément à l'art. 4, al. 1, let. b, de l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS 172.010.442).

En vertu de l'*al. 5*, les données mises à la disposition de l'OFS pour des évaluations statistiques sont également détruites conformément à ces prescriptions.

Art. 14 Vérification du code source

Les programmes du système TP lisibles par une machine doivent avoir été élaborés, de manière avérée, au moyen du code source public (art. 60*a*, al. 5, let. e, LEp). En vertu de l'*al. 1*, l'OFSP publie les données qui servent à vérifier si, pour tous les éléments du système TP, les programmes lisibles par une machine ont été créés à partir du code source publié. Par conséquent, la preuve correspondante est fournie en premier lieu par le fait que les personnes intéressées par la technique peuvent en principe vérifier, à l'aide des données publiées par l'OFSP, si les programmes lisibles par une machine ont effectivement été élaborés à partir du code source publié.

En vertu de l'*al. 2*, l'OFSP effectue la vérification lui-même. Cette exigence découle déjà pour l'OFSP, l'exploitant du système, de l'obligation de publier le code source (art. 60*a*, al. 5, let. e, phrase 1, LEp).

À noter encore une fois que les codes sources ne sont pas publics pour les fonctions des systèmes d'exploitation utilisées via l'interface (art. 5, al. 3) ni pour les tiers mandatés au sens de l'art. 10, al. 3.

Art. 15 Désactivation de l'application SwissCovid et rapport

Lors de l'abrogation de la présente ordonnance ou de l'arrêt du système, l'OFSP procède à la désactivation et à la désinstallation de ses composants. En supprimant les deux *back-ends*, les applications SwissCovid sont désactivées. Mais l'OFSP ne peut pas désinstaller lui-même les applications SwissCovid sur les téléphones portables des participants. C'est pourquoi l'*al. 1* précise que l'OFSP, en plus de la désactivation de l'application, incite aussi les participants à la désinstaller de leur téléphone portable.

Le système TP a été développé pour la première fois de la sorte et la Confédération s'est aventurée à cette occasion en terrain inconnu. Pour pouvoir évaluer la pertinence d'un tel système et au regard d'éventuelles épidémies comparables, l'*al. 2* précise que l'OFSP fait rapport au Conseil fédéral au plus tard six mois après l'abrogation de la présente ordonnance.

Art. 16 Abrogation d'un autre acte

L'essai pilote s'achève avec l'introduction définitive du système TP, raison pour laquelle l'ordonnance COVID-19 essai pilote traçage de proximité devient caduque. Elle est abrogée avec l'entrée en vigueur de la présente ordonnance.

Art. 17 Entrée en vigueur et durée de validité

La modification urgente de la LEp en lien avec le coronavirus (système de traçage de proximité), adoptée le 19 juin 2020, a effet jusqu'au 30 juin 2022 ; dès le jour suivant, toutes les modifications qu'elle contient sont caduques. En se fondant directement sur l'art. 60*a*, al. 8, LEp, le Conseil fédéral est tenu d'arrêter le système TP auparavant, dès qu'il n'est plus requis ou qu'il ne se révèle pas suffisamment efficace. En conséquence, l'art. 17 précise que l'ordonnance a effet au plus tard jusqu'au 30 juin 2022.

Eu égard à l'art. 60*a*, al. 8, LEp, le Conseil fédéral doit donc s'assurer en permanence que l'exploitation du système TP est requise et suffisamment efficace. Si tel n'est plus le cas, il doit en ordonner l'arrêt (par une modification ou l'abrogation de la présente ordonnance). À noter à cet égard que l'OFSP, l'exploitant du système, est également chargé de soumettre au DFI les propositions nécessaires à l'intention du Conseil fédéral (art. 9, al. 3, let. a, ch. 1, de l'ordonnance du 28 juin 2000 sur l'organisation du Département fédéral de l'intérieur ; RS 172.212.1).